|  |
| --- |
| WorD598 |
|  |
| Certification & Accreditation Program  Provider Resource Name  (Environment)  Resource Security Plan |
| Month 01, 2017 |
|  |
|  |
|  |

Revisions

|  |  |
| --- | --- |
| Version | Changes |
| 1.0 | Document Creation |

**Table of Contents**

Executive Summary 4

1 Security Plan 6

1.1 Resource Personnel Contacts 6

1.1.1 Capability Architecture 7

1.1.2 Core Applications 7

1.1.3 Minor Applications 7

2 Security Plan Controls 7

2.1.1 Access Control Policy Family (AC) 7

2.1.2 Awareness and Training Control Family (AT) 23

2.1.3 Audit and Accountability Policy Family (AU) 27

2.1.4 Security Assessment & Authorization Policy Family (CA) 36

2.1.5 Configuration Management Policy Family (CM) 41

2.1.6 Contingency Planning Policy Family (CP) 51

2.1.7 Facilities Security (FS) 58

2.1.8 Identification and Authentication Policy Family (IA) 67

2.1.9 Incident Response Policy Family (IR) 74

2.1.10 Maintenance Policy Family (MA) 81

2.1.11 Media Protection Policy Family (MP) 85

2.1.12 Physical and Environmental Protection Control Family (PE) 90

2.1.13 Planning Control Family (PL) 100

2.1.14 Personnel Security Policy Family 104

2.1.15 Risk Assessment Policy Family (RA) 110

2.1.16 Resource and Services Acquisition Policy Family (SA) 115

2.1.17 Resource and Communications Protection Policy Family (SC) 124

2.1.18 Resource and Data Integrity Policy Family (SI) 134

2.1.19 Program Management Policy Family (PM) 143

2.1.20 Data Warehouse Security Requirements – FTI Only 144

# Executive Summary

Introduction

The purpose of this Security Plan is to provide an overview of the North Carolina Department of Revenue (Agency) and <Vendor> (Provider) security requirements for a particular Capability and to describe the controls in place or planned to meet those requirements. Each Security Plan is developed in accordance with the guidelines contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Resources, IRS Publication 1075 and applicable risk mitigation guidance and standards.

<Resource> Security Plan Summary – For NCDOR use only

This document details the security controls for <Resource> characterized as:

|  |  |  |
| --- | --- | --- |
| Lifecycle Category | Scope | Data Classification |
| Under Development  Under Major Revision  Operational | Minor or subset of  Major Capability | Public  Confidential  Federal Tax Information |

Compliance with Security Controls by Family

The following table provides a summary (by control family) of how the Capability complies with the security controls articulated in the North Carolina Department of Revenue Security Policy Manual.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control Family** | **Total Controls** | **Met** | **Partially Met** | **Not Met** | **N/A** |
| Access Control (AC) | 16 |  |  |  |  |
| Awareness & Training (AT) | 4 |  |  |  |  |
| Audit & Accountability (AU) | 12 |  |  |  |  |
| Certification, Accreditation, & Security Assessments (CA) | 6 |  |  |  |  |
| Configuration Management (CM) | 11 |  |  |  |  |
| Contingency Planning (CP) | 8 |  |  |  |  |
| Facilities Security (FS) | 10 |  |  |  |  |
| Identification and Authentication (IA) | 8 |  |  |  |  |
| Maintenance Policy Family (MA) | 5 |  |  |  |  |
| Media Protection (MP) | 6 |  |  |  |  |
| Physical and Environmental Protection (PE) | 17 |  |  |  |  |
| Planning (PL*)* | 4 |  |  |  |  |
| Risk Assessment (RA) | 2 |  |  |  |  |
| Personnel Security (PS) | 8 |  |  |  |  |
| Risk Assessment (RA) | 4 |  |  |  |  |
| Resource and Services Acquisition (SA) | 10 |  |  |  |  |
| Resource and Communications Protection (SC) | 15 |  |  |  |  |
| Resource and Data Integrity (SI) | 11 |  |  |  |  |
| Program Management (PM) | 1 |  |  |  |  |
| **Control Population Totals** | **158** |  |  |  |  |
| **Percentage** | |  |  |  |  |

Security Plan Approval

Capability Owner Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CIO Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Security Plan

## Resource Personnel Contacts

Resource personnel contacts include contact information for the authorizing official for the Provider and the authorizing official for the Resource.

Provider - Authorizing Official

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** |  | **Address:** |  |
| **Title:** |  | **Phone Number:** |  |
| **Agency:** |  | **E-mail Address:** |  |

Agency - Authorizing Official

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** | David Roseberry | **Address:** | 501 N. Wilmington St  Raleigh, NC 27602 |
| **Title:** | Chief Information Officer | **Phone Number:** | (919) 754-2002 |
| **Agency:** | North Carolina Department of Revenue | **E-mail Address:** | David.Roseberry@dornc.com |

### Capability Architecture

Architecture and description of Resource goes HERE

### Core Applications

|  |  |
| --- | --- |
| **Application** | **Version** |
|  |  |
|  |  |
|  |  |

### Minor Applications

|  |  |
| --- | --- |
| **Application** | **Version** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Instructions – Please read these first!**

It is important that you understand how to fill out this security plan correctly. See the example control below for how to format and where to place your response. If you have any questions please contact NCDOR.

Example Control:

|  |  |  |
| --- | --- | --- |
| Example control – Should be removed before finalizing the document and is provided as an example only | | |
| The purpose of this control is to provide an example.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | N/A | N/A | N/A |   The main body of the control is this part of the control. This is what you will respond to below in the provided sections.  a) This is a sub-section of the main control and also requires a response.  b) This is also part of the sub-section and again, requires a response.  CE1. This is a control enhancement section and also requires a response. See below. | | |
| **Do not check any of the boxes below**  **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  SAS | | |
| **Control implementation***: This is for the assessor’s use only. Do not write in this section.* | | |
| Provider Response | | |
| This should be left blank if it is here. | Response to the main control will go here. | |
| This should be left blank. | a. | Response to part a. will go here. |
| This should be left blank. | b. | Response to part b. will go here. |
| This should be left blank. | CE1 | This is where you respond to the enhancement. |
| NCDORResponse | | |
| This should be left blank. | NCDOR response will go here. Leave this blank. | |

# Security Plan Controls

### Access Control Policy Family (AC)

|  |  |
| --- | --- |
| (AC-1) Access Control Procedures | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the access control policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-1 | AC-1 | AC-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the access control processes must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| (AC-2) Account Management | | |
| The purpose of the policy is to ensure that the confidentiality and integrity of Data is protected by appropriately managing accounts.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-2 | AC-2 (CE1) (CE2) (CE3) (CE4) | AC-2 (CE-3) |   It is the policy of the Agency to restrict Staff access to Data and Resources appropriate to their duties and responsibilities.  The Provider:   1. Identifies and selects information system accounts to support organizational missions/business functions; and 2. Assigns account managers for information system accounts; and 3. Establishes conditions for group and role membership; and 4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; and 5. Must notify the NCDOR IT Service Desk when Staff that has access to components within the boundaries of this resource are separated or transferred to another department. Those supervising or sponsoring contractual Staff must notify NCDOR IT Service Desk when contractors that have access to components within the boundaries of this resource start, change work assignments, or end their assignment. Provider must then restrict access accordingly. Internal transfers will be treated as a separation from the originating department and a new hire in the department that the Staff transferred to; 6. Logs the use of accounts; and 7. Notify account managers:   1. When accounts are no longer required; and  2. When users are terminated or transferred; and  3. When individual information system usage or need-to-know changes.   1. Authorizes access to the information system based on:   1. A valid access authorization; and  2. Intended system usage; and  3. Other attributes as required by the organization or associated missions/business functions.   1. The Provider will review accounts for compliance with account management requirements annually, at a minimum, for accounts with general privileges and quarterly, at a minimum, for accounts with elevated privileges.   Control Enhancements  CE1. The Provider employs automated mechanisms to support the management of accounts.  CE2. The Resource automatically removes or disables temporary and emergency accounts after a defined time period for each type of account.  CE3. Accounts that are inactive for 120 days are disabled.  CE4. The Resource automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies Provider IT Security. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.* | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
|  | i. |  |
|  | CE1 | *The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.* |
|  | CE2 | *This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.* |
|  | CE3 |  |
|  | CE4 | *Related controls: AU-2, AU-12.* |
| NCDORResponse | | |
|  |  | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
|  | i. |  |
|  | CE1 |  |
|  | CE2 |  |
|  | CE3 |  |
|  | CE4 |  |

|  |  |  |
| --- | --- | --- |
| (AC-3, 4) Access & Information Flow Enforcement | | |
| The purpose of the policy is to establish requirements related to access control policies.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-3,4 | AC-3,4 | AC-3,4 |   It is the policy of the Agency that all Resources enforce Agency approved authorizations:  (AC-3) For logical access to Data in accordance with applicable access control policies; and  (AC-4) For controlling the flow of information within the Resource and between interconnected Resources based on applicable information flow control policies. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | AC-3 | *Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.* |
|  | AC-4 | *Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.*  *Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.* |
| NCDORResponse | | |
|  | AC-3 |  |
|  | AC-4 |  |

|  |  |  |
| --- | --- | --- |
| (AC-5) Separation of Duties | | |
| The purpose of the policy is to address the potential for abuse of privileges and the risk of malevolent activity without collusion.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | AC-5 | AC-5 |   It is the policy of the Agency that:   1. All duties of Staff are separated & documented to prevent harmful activity without collusion. For example:    * Dividing mission functions and Resource support functions among different individuals; and    * Conducting Resource support functions with different individuals such as Resource management, programming, configuration management, quality assurance & testing, and network security; and    * Ensuring security personnel administering access control functions do not also administer audit functions. 2. Resource access authorizations are defined to support separation of duties. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.* | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| (AC-6) Least Privilege | | | |
| The purpose of the policy is to establish the use of the principle of “least privilege”.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | AC-6 (CE1) (CE2) (CE5) (CE9) (CE10) | AC-6 (CE1) (CE2) (CE5) (CE9) (CE10) |   It is the policy of the Agency that Staff, or processes acting on behalf of Staff, is/are only authorized access necessary to accomplish assigned tasks in accordance with required business functions.  Control Enhancements  CE1. The Agency explicitly authorizes access to Data classified as Confidential or FTI.  CE2. The Agency requires that users of accounts, or roles, with access to Confidential Data or FTI use non-privileged accounts or roles when accessing non-security functions. (i.e. A system administrator account should not be used for non-security related work).  CE5. The Provider restricts privileged accounts on the Resource to a limited number of Staff with a need to perform security or administrative duties.  CE9. The Resource must log the execution of privileged functions.  CE10. The Resource must prevent non-privileged Staff from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.  CE11. A privileged account must be in addition to the non-privileged account which is used for day to day tasks. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
| *Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.* | | |
|  | CE1 | *Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.* |
|  | CE2 | *This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.* |
|  | CE5 | *Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.* |
|  | CE9 | *Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.* |
|  | CE10 | *Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.* |
|  | CE11 |  |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE2 |  |
|  | CE5 |  |
|  | CE9 |  |
|  | CE10 |  |
|  | CE11 |  |

|  |  |  |
| --- | --- | --- |
| (AC-7) Unsuccessful Logon Attempts | | |
| The purpose of the policy is to limit invalid logon attempts.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-7 | AC-7 | AC-7 (FTI1)(FTI2) |   The Resource must:   1. Enforce a limit of consecutive invalid logon attempts by a user during a defined time period; and 2. Automatically lock the account for a defined time period; locks the account until released by an administrator; delays next logon prompt when the maximum number of unsuccessful attempts is exceeded.   Control Enhancements  FTI1. Resources enforce a limit of three consecutive invalid logon attempts within a 120-minute period  FTI2. Resources automatically lock the account until released by the Resource administrator. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.* | |
|  | a. |  |
|  | b. |  |
|  | FTI1 |  |
|  | FTI2 |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | FTI1 |  |
|  | FTI2 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| (AC-8) Resource Use Notification | | | |
| The purpose of the policy is to establish the use of warning banners.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-8 | AC-8 | AC-8 |   It is the policy of the Agency that for all Resources:   1. Before granting access to Staff, the Resource must display a use notification message that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:    1. The Staff are accessing a restricted Resource; and    2. Usage may be monitored, recorded, and subject to audit; and    3. Unauthorized use of the Resource is prohibited and subject to criminal and civil penalties; and    4. Use of the Resource indicates consent to monitoring and recording. 2. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the Resource; and 3. For publicly accessible Resources:    1. Displays use information before granting further access; and    2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such Resources that generally prohibit those activities; and    3. And includes a description of the authorized uses of the Resource. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***: Note: NCDOR will provide an approved logon banner.* | | | |
| <Provider> Response | | | |
|  | *System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.* | |
|  | a. |  | |
|  | a.1 |  | |
|  | a.2 |  | |
|  | a.3 |  | |
|  | a.4 |  | |
|  | b. |  | |
|  | c. |  | |
|  | c.1 |  | |
|  | c.2 |  | |
|  | c.3 |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | a.1 |  | |
|  | a.2 |  | |
|  | a.3 |  | |
|  | a.4 |  | |
|  | b. |  | |
|  | c. |  | |
|  | c.1 |  | |
|  | c.2 |  | |
|  | c.3 |  | |

|  |  |
| --- | --- |
| (AC-11) Session Lock | |
| The purpose of the policy is to prevent unintended access.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | AC-11 | AC-11 |   It is the policy of the Agency that Resources prevent access by initiating a session lock after 15 minutes of inactivity and maintains the lock until Staff re-establishes access using established identification and authentication procedures. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| (AC-12) Session Termination | |
| The purpose of the policy is to prevent unintended access.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | AC-12 | AC-12 |   It is the policy of the Agency that Resources automatically terminate Staff-initiated logical sessions after 15 minutes of inactivity. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user’s logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| (AC-14) Permitted Actions without Identification or Authentication | |
| The purpose of the policy is to addresses situations in which it is determined that no identification or authentication is required for a Resource.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-14 | AC-14 | AC-14 |   It is the policy of the Agency that Data may not be disclosed without identification and authentication. For those Resources on which it is determined that no identification or authentication is required, the specific actions that can be performed must not include the disclosure of inappropriate Data. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| (AC-17) Remote Access | | |
| The purpose of the policy is to establish the requirements needed to access Resources and Data from a remote location.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-17 | AC-17 (CE1) (CE2) (CE3) (CE4) | AC-17 (CE1) (CE2) (CE3) (CE4) (FTI1) (FTI2) (FTI3) (FTI4) |   It is the policy of the Agency that for each type of remote access allowed, procedures must:   1. Document usage restrictions, configuration/connection requirements and implementation guidance, and 2. Authorizes remote access to the information system prior to allowing such connections   Control Enhancements  CE1. The Provider must monitor and control remote access methods.  CE2. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.  CE3. All remote access should be routed through the fewest number of managed network access control points as is practical.  CE4. There are no special restrictions to the use of privileged commands or access to security-relevant information based solely on the access being remote.  FTI1. Remote access requires identification and multifactor authorization prior to allowing access (IA-2, CE1, CE2, CE11);  FTI2. Multifactor authentication must be implemented such that one of the factors is provided by a device separate from the Resource gaining access. NIST SP 800-63 allows the use of software tokens (IA-2, CE11);  FTI3. Remote access is prohibited for Staff located outside of United States. Further, no Data may be received, processed, stored, transmitted or disposed of by Resources located outside of the United States;  FTI4. All remote access must be encrypted using a cryptographic module that is FIPS 140-2 compliant (CE2, IA-7); | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.* |
|  | CE2 | *The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.* |
|  | CE3 | *Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.* |
|  | CE4 | *Related control: AC-6.* |
|  | FTI1 |  |
|  | FTI2 |  |
|  | FTI3 |  |
|  | FTI4 |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |
|  | CE2 |  |
|  | CE3 |  |
|  | CE4 |  |
|  | FTI1 |  |
|  | FTI2 |  |
|  | FTI3 |  |
|  | FTI4 |  |

|  |  |  |
| --- | --- | --- |
| (AC-18) Wireless Access | | |
| The purpose of the policy is to prohibit the use of wireless technologies to directly access Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-18 | AC-18 (CE1) | AC-18 (CE1) (FTI1) (FTI2) |   It is the policy of the Agency to:   1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access. 2. Authorize wireless access to the Resource prior to allowing such connections.   Control Enhancements  CE1. The information system must protect wireless access to the system using authentication and encryption.  FTI1. To use FTI in an 802.11 WLAN the Provider must meet the following requirements:   1. The Provider should have WLAN management controls that include security policies and procedures, a complete inventory of Provider wireless network components, and standardized security configurations for all components. 2. WLAN hardware (access points, servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, Secure Storage—IRC 6103(p)(4)(B). 3. Each system within the Provider’s network that transmits FTI through the WLAN is hardened in accordance with the requirements in this publication. 4. The WLAN is architected to provide logical separation between WLANs with different security profiles and from the wired LAN. 5. WLAN infrastructure that receives, processes, stores, or transmits FTI must comply with the Institute of Electrical and Electronic Engineers 802.11i wireless security standard and perform mutual authentication for all access to FTI via 802.1X and extensible authentication protocol. 6. Vulnerability scanning should be conducted as part of periodic technical security assessments for the organization’s WLAN. 7. Wireless intrusion detection is deployed to monitor for unauthorized access, and security event logging is enabled on Provider WLAN components in accordance with IRS publication 1075 Section 9.3.3, Audit and Accountability. 8. Disposal of all WLAN hardware follows media sanitization and disposal procedures in IRS publication 1075 Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization.   FTI2. The Resource must employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential breaches to Resources. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Related controls: SC-8, SC-13.* |
|  | FTI1 |  |
|  | FTI1 a. |  |
|  | FTI1 b. |  |
|  | FTI1 c. |  |
|  | FTI1 d. |  |
|  | FTI1 e. |  |
|  | FTI1 f. |  |
|  | FTI1 g. |  |
|  | FTI1 h. |  |
|  | FTI2 |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |
|  | FTI1 |  |
|  | FTI1 a. |  |
|  | FTI1 b. |  |
|  | FTI1 c. |  |
|  | FTI1 d. |  |
|  | FTI1 e. |  |
|  | FTI1 f. |  |
|  | FTI1 g. |  |
|  | FTI1 h. |  |
|  | FTI2 |  |

|  |  |  |
| --- | --- | --- |
| **(AC-19) Access Control for Mobile Resources** | | |
| The purpose of the policy is to clarify the use of highly portable Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-19 | AC-19 (CE5) | AC-19 (CE2) (CE5) (FTI1) |   It is the policy of the Agency to:   1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and 2. Authorize the connection of mobile devices to organizational Resources.   Control Enhancements  CE2. Mobile Resources must automatically purge/wipe Data from mobile Resources based on 10 consecutive, unsuccessful logon attempts. Laptop computers are excluded from this specific requirement.  CE5. Mobile Resources must use a cryptographic module that is FIPS 140-2 compliant to protect confidentiality and integrity of local Data.  FTI1. In addition, Mobile Resources must also meet the following requirements (IRS 1075 September 2016- 9.4.8):   1. Mobile Resource management controls must be in place including security policies and procedures, inventory, and standardized security configurations for all Resources; and 2. An annual risk assessment must be conducted of the security controls in place on all Resources in the mobile environment; and 3. Protection mechanisms must be in place in case a mobile Resource is lost or stolen—all Data stored internally on the Resource or via removable media, including internal storage and   removable media storage, such as Micro Secure Digital (SD) cards, must be encrypted using a cryptographic module that is FIPS 140-2 compliant; and   1. All data communication with the agency’s internal network must be encrypted using a   cryptographic module that is FIPS 140-2 compliant; and   1. The Agency must control the ability to download only authorized applications to the Resource   and must limit the accessibility to FTI by applications to only authorized applications; and   1. All mobile device management servers that receive, store or transmit Data must be hardened in accordance to this policy manual; and 2. A centralized mobile Resource management solution must be used to authenticate Agency-issued and personally owned mobile Resources prior to allowing access to the internal network; and 3. Security events must be logged for all mobile Resource and related management Resources; and 4. The Agency must disable wireless personal area networks that allow a mobile Resource to connect to other Resources via Bluetooth or near field communication (NFC); and 5. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, must be disabled to the extent practical; and 6. Disposal of all mobile Resource component hardware follows media sanitization and disposal procedures. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <Vendor> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.* | | |
|  | a. |  |
|  | b. |  |
|  | CE2 |  |
|  | CE5 | *Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.* |
|  | FTI1 |  |
|  | FTI1 a. |  |
|  | FTI1 b. |  |
|  | FTI1 c. |  |
|  | FTI1 d. |  |
|  | FTI1 e. |  |
|  | FTI1 f. |  |
|  | FTI1 g. |  |
|  | FTI1 h. |  |
|  | FTI1 i. |  |
|  | FTI1 j. |  |
|  | FTI1 k. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | CE2 |  |
|  | CE5 |  |
|  | FTI1 |  |
|  | FTI1 a. |  |
|  | FTI1 b. |  |
|  | FTI1 c. |  |
|  | FTI1 d. |  |
|  | FTI1 e. |  |
|  | FTI1 f. |  |
|  | FTI1 g. |  |
|  | FTI1 h. |  |
|  | FTI1 i. |  |
|  | FTI1 j. |  |
|  | FTI1 k. |  |

|  |  |  |
| --- | --- | --- |
| **(AC-20) Use of External Resources** | | |
| This control addresses the use of external Resources for the processing, storage, or transmission of Data from external Resources. External Resources are outside of the authorization boundary established by Agency and which the Agency has no direct supervision and authority over the application of required security controls or the assessment of control effectiveness.  Both the Agency and Provider establishes terms and conditions (i.e. MOUs, contracts, etc.) for the use of external Resources in accordance with Agency security policies and procedures. If terms and conditions with the owners of external Resources cannot be established, the Agency may impose restrictions on Agency or Provider personnel using those external Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-20 | AC-20 (CE1) (CE2) | AC-20 (CE2) (CE3) |   The Agency establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external Resources, allowing authorized individuals to:   1. Access the Resource from external Resources; and 2. Process, store, or transmit organization-controlled Data using external Resources.   Control Enhancements  CE1. The Agency permits authorized Staff to use an external Resource to access the Resource or to process, store, or transmit organization-controlled Data only when the Agency:   1. Verifies, through internal inspections required by the IRS, the implementation of required security controls on the external Resource within 18 months, at a minimum (See IRS Publication 1075 section 6.4); or 2. Retains approved Resource connection or processing agreements with the organizational entity hosting the external Resource.   CE2. The Agency restricts the use of portable storage devices in external Resources to authorized individuals for Data classified as Public or Confidential. For Data classified as FTI, it is the policy of the Agency that unless approved by the IRS Office of Safeguards:   1. Access to FTI from external Resources is prohibited; and 2. Use of non-Agency owned Resources to receive, process, store or transmit FTI is prohibited.   CE3. Usage of any non-Agency owned Resource requires the Agency to notify the IRS Office of Safeguards 45 days prior to implementation (See Section 7.4 45-Day Notification Reporting Requirements). | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***: Note: Connecting to external sources for patching would be considered as the use of external resources.* | | |
| <Provider> Response | | |
| *External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.*  *For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.* |
|  | CE1 a. |  |
|  | CE1 b. |  |
|  | CE2 | *Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.* |
|  | CE2 a. |  |
|  | CE2 b. |  |
|  | CE3 | *Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |
|  | CE1 a. |  |
|  | CE1 b. |  |
|  | CE2 |  |
|  | CE2 a. |  |
|  | CE2 b. |  |
|  | CE3 |  |

|  |  |
| --- | --- |
| **(AC-21) Data Sharing** | |
| The purpose of the policy is to restrict inappropriate re-disclosure of information.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | AC-21 | AC-21 |   It is the policy of the Agency that sharing or re-disclosure of Data classified as Confidential or FTI is strictly prohibited to only those authorized.  For FTI, authorization is defined in Internal Revenue Code 26 U.S.C. § Section 6103 - Confidentiality and disclosure of returns and return information and approved by the IRS Office of Safeguards. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(AC-22) Publicly Accessible Content** | | |
| The purpose of the policy is to establish the requirements around making information available for the general public.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AC-22 | AC-22 | AC-22 |   It is the policy of the Agency that only the NCDOR Public Information Officer (PIO), or his authorized delegate, may post information onto a publicly accessible Resource.   1. The NCDOR PIO must ensure that publically accessible information does not contain Data; and 2. The NCDOR PIO must review the proposed content of Data prior to posting onto the publicly accessible Resource; and 3. The NCDOR PIO must review the information on any publically accessible Resource for Data, at least quarterly, and remove it if discovered. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

### Awareness and Training Control Family (AT)

|  |  |
| --- | --- |
| **(AT-1) Security Awareness and Training Policy & Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the awareness and training policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AT-1 | AT-1 | AT-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the awareness and training procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(AT-2) Security Awareness and Training** | | |
| The purpose of the policy is to establish the parameters for security awareness training.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AT-2 | AT-2 (CE2) | AT-2 (CE2) |   It is the policy of the Agency that prior to granting Staff access to Data and Resources they must certify their understanding of the Agency’s security policy and procedures for safeguarding information. Staff may not access Resources and Data unless certification, or recertification, has been completed. Security awareness and training is provided to Staff:   1. As part of initial training for new Staff; and 2. When required by changes to Resources; and 3. Annually thereafter.   Control Enhancement  CE2. Training and certification must include the following provisions:   1. Include security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat training should bring awareness of the potential for Staff to use insider knowledge of sensitive Agency information to perform malicious actions, which could include the unauthorized access or redisclosure of Data; and 2. If the Data is classified as FTI, then per IRS 1075 IRC 6103(p)(4)(D)(6.3): 3. Staff must be advised of the provisions of IRCs 7431, 7213, and 7213A; and 4. Training must also cover the incident response policy and procedure for reporting unauthorized disclosures and Data breaches; and 5. During this training, Staff must be made aware that disclosure restrictions and the penalties apply even after employment with the Agency has ended; and 6. Staff must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements; and 7. Training certification must be documented and placed in files for NCDOR review and retained for at least five years. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation:** *NCDOR Security Awareness Training through the NCDOR LMS should cover all requirements of this control. All contract staff requiring physical or logical access to NCDOR data or systems must complete this training prior to access being granted.* | | |
| <Provider> Response | | |
| *Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE2 | *Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.* |
|  | CE2 a. |  |
|  | CE2 b. |  |
|  | CE2 b.1 |  |
|  | CE2 b.2 |  |
|  | CE2 b.3 |  |
|  | CE2 b.4 |  |
|  | CE2 b.5 |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE2 |  |
|  | CE2 a. |  |
|  | CE2 b. |  |
|  | CE2 b.1 |  |
|  | CE2 b.2 |  |
|  | CE2 b.3 |  |
|  | CE2 b.4 |  |
|  | CE2 b.5 |  |

|  |  |  |
| --- | --- | --- |
| **(AT-3) Role-Based Security Training** | | |
| The purpose of the policy is to establish the need for training on the NCDOR Security Policy manual.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AT-3 | AT-3 | AT-3 |   It is the policy of the Agency that Staff must be provided training on the content of the Technical Policies Manual:   1. As part of initial training for new Staff; and 2. When required by changes to Resources; and 3. Annually thereafter. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***: Providers are required to ensure that all staff with a Technical IT role receive annual role-based security training. A list and brief explanation is provided in the NCDOR Security Policy Manual, Section AT-3, however, this list is not all-inclusive. If there is a question about rather specific personnel need this training, NCDOR IT Security (under the direction of the NCDOR CISO) should be consulted. Documentation does not have to be provided, but should be maintained and is subject to audit. Retention for all training records is outlined in AT-4.* | | |
| <Provider> Response | | |
| *Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role- based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |
| --- | --- |
| **(AT-4) Security Training Records** | |
| The purpose of the policy is to establish the requirements to maintain records related to security training.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AT-4 | AT-4 | AT-4 |   It is the policy of the Agency that Provider documents and monitors individual security training activities including general security training and training of their Staff related to specific Resources. Training records must be retained for five years. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.* |
| NCDORResponse | |
|  |  |

### Audit and Accountability Policy Family (AU)

|  |  |
| --- | --- |
| **(AU-1) Audit and Accountability Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the Audit and Accountability policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-1 | AU-1 | AU-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the audit and accountability procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(AU-2) Audit Events** | | |
| The purpose of the policy is to establish the procedure requirements for audit events.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-2 | AU-2 (CE3) | AU-2 (CE3) |   It is the policy of the Agency that security-relevant events must enable the detection of unauthorized access to Data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of Data by each unique Staff member.  For each Resource:   1. Determine that it is capable, at a minimum, of auditing the following event types: 2. Log onto system; and 3. Log off of system; and 4. Change of password; and 5. All Resource administrator commands, while logged on as Resource administrator; and 6. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS); and 7. Creation or modification of super-user groups; and 8. Subset of security administrator commands, while logged on in the security administrator role; and 9. Subset of Resource administrator commands, while logged on in the user role; and 10. Clearing of the audit log file; and 11. Startup and shutdown of audit functions; and 12. Use of identification and authentication mechanisms (e.g., user ID and password); and 13. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su); and 14. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the Resource; and 15. Changes made to an application or database by a batch file; and 16. Application-critical record changes; and 17. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); and 18. All Resource and Data interactions; and 19. Access to Data must be audited at the operating system, software, and database levels. Software and platforms have differing audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific Office of Safeguards SCSEM, which is available on the IRS Office of Safeguards website. 20. Coordinate the security audit function with other Agency entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; and 21. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.   Control Enhancement  CE3. Review and update the audited events at a minimum, every 18 months. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.* | | |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | a.5 |  |
|  | a.6 |  |
|  | a.7 |  |
|  | a.8 |  |
|  | a.9 |  |
|  | a.10 |  |
|  | a.11 |  |
|  | a.12 |  |
|  | a.13 |  |
|  | a.14 |  |
|  | a.15 |  |
|  | a.16 |  |
|  | a.17 |  |
|  | a.18 |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | a.5 |  |
|  | a.6 |  |
|  | a.7 |  |
|  | a.8 |  |
|  | a.9 |  |
|  | a.10 |  |
|  | a.11 |  |
|  | a.12 |  |
|  | a.13 |  |
|  | a.14 |  |
|  | a.15 |  |
|  | a.16 |  |
|  | a.17 |  |
|  | a.18 |  |
|  | b. |  |
|  | c. |  |

|  |  |  |
| --- | --- | --- |
| **(AU-3) Content of Audit Records** | | |
| The purpose of the policy is to establish the content for audit records.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-3 | AU-3 (CE1) | AU-3 (CE1) |   It is the policy of the Agency that each Resource must generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any accounts associated with the event.  Control Enhancement  CE1. Generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.* | | |
|  | CE1 | *Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |

|  |  |
| --- | --- |
| **(AU-4) Audit Storage Capacity** | |
| The purpose of the policy is to establish the requirements for retention of audit records.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-4 | AU-4 | AU-4 |   It is the policy of the Agency to allocate sufficient storage capacity in order to retain records for seven years. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(AU-5) Response to Audit Processing Failures** | | |
| The purpose of the policy is to ensure that the appropriate Staff knows when an auditing process fails.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-5 | AU-5 | AU-5 (CE1) |   It is the policy of the Agency that all Resources must:   1. Alert Provider IT Security in the event of an audit processing failure; and 2. Monitor Resource operational status using operating system or Resource audit logs and verify functions and performance of the Resource. Logs shall be able to identify where Resource process failures have taken place and provide information relative to corrective actions to be taken by the Resource administrator.   Control Enhancement  CE1. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.* |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(AU-6) Audit Review, Analysis and Reporting** | | | |
| The purpose of the policy is to ensure that audit logs are reviewed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-6 | AU-6 (CE1) | AU-6 |   It is the policy of the Agency that Provider IT Security Staff:   * 1. Review and analyze Resource audit records at least weekly for indications of unusual activity related to potential unauthorized access; and   2. Report findings according to the Agency security incident response policy. If the finding involves a potential unauthorized disclosure of Data classified as Federal Tax Information, the NCDOR Service Desk must be notified immediately so that the NCDOR can fulfill reporting obligations.   Control Enhancement  CE1. The Agency employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.* | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 | *Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(AU-7) Audit Reduction and Report Generation** | | | |
| The purpose of the policy is to ensure that audit logs can be easily reviewed and analyzed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | AU-7 (CE1) | AU-7 |   It is the policy of the Agency that the Security Event Information Management (SEIM) Resource used by the Agency must provide an audit reduction and report generation capability that:   1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and   b) Does not alter the original content or time ordering of audit records.  Control Enhancement  CE1. The SEIM provides the capability to process audit records for events of interest based on the content of specific audit record fields including, identities of individuals, event types, event times, event dates, Resources involved or IP addresses involved. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.* | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 | *Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. Related controls: AU-2, AU-12.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(AU-8) Time Stamps** | | | |
| The purpose of the policy is to ensure that audit logs have accurate time stamps.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-8 | AU-8 (CE1) | AU-8 (CE1) |   It is the policy of the Agency that all Resources:   1. Use internal Resource clocks to generate time stamps for audit records; and   b) Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).  Control Enhancement  CE1. All Resources compare and synchronize the internal Resource clocks to approved authoritative time sources (e.g., NIST, Naval Observatory) | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12.* | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 | *This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 |  | |

|  |  |  |
| --- | --- | --- |
| **(AU-9) Protection of Audit Information** | | |
| The purpose of the policy is to ensure that audit logs have accurate time stamps.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-9 | AU-9 (CE4) | AU-9 (CE4) |   It is the policy of the Agency that the Resources must protect audit information and audit tools from unauthorized access, modification, and deletion.  Control Enhancement  CE4. The Provider must authorize access to manage audit functionality only to IT Security Staff. Resource and network administrators must not have the ability to modify or delete audit log entries. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.* | | |
|  | CE4 | Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5. |
| NCDORResponse | | |
|  | | |
|  | CE4 |  |

|  |  |
| --- | --- |
| **(AU-11) Audit Record Retention** | |
| The purpose of the policy is to ensure that audit logs are kept for a sufficient amount of time.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-11 | AU-11 | AU-11 |   It is the policy of the Agency that audit records must be retained for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and Agency information retention requirements as identified in Section 9.3.3.2, Audit Event (AU-2). | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(AU-12) Audit Generation** | | | |
| The purpose of the policy is to ensure that audit logs capture particular events.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | AU-12 | AU-12 | AU-12 |   It is the policy of the Agency that Resources must:  a) Provide audit record generation capability for the auditable events defined in the policy Audit Events (AU-2); and  b) Allow Agency IT Security Staff to select which auditable events are to be audited by specific components of the Resource; and  c) Generate audit records for the events with the content defined in the policy Content of Audit Records (AU-3); and  d) These records should be offloaded to NCDOR. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |

|  |  |  |
| --- | --- | --- |
| **(AU-16) Cross Agency Auditing** | | |
| The purpose of the policy is to ensure that audit information is protected when working with service providers outside of the Agency.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | AU-16 |     It is the policy of the Agency to coordinate the access and protection of audit information among external organizations when audit information is transmitted across Agency boundaries:  a) For cloud computing environments see IRS 1075 section 9.4.1 Cloud Computing Environments for mandatory requirements; and  b) For consolidated data centers see IRS 1075 5.4.2 Contractor- or Agency-Shared Facility—Consolidated Data Centers for mandatory requirements. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***: Audit log events captured by <PROVIDER> as defined in control AU-12 will be sent to the NCDOR central logging repository and used for security purposes or qRadar will be installed on <PROVIDER> components within the Resource and Provider will protect audit logs.* | | |
| <Provider> Response | | |
| *When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.* | | |
|  | CE1 |  |
|  | CE2 |  |
|  | CE5 |  |
|  | CE9 |  |
|  | CE10 |  |
|  | CE11 |  |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE2 |  |
|  | CE5 |  |
|  | CE9 |  |
|  | CE10 |  |
|  | CE11 |  |

### Security Assessment & Authorization Policy Family (CA)

|  |  |
| --- | --- |
| **(CA-1) Security Assessments** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the security assessment and authorization policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CA-1 | CA-1 | CA-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the security assessment and authorization procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(CA-2) Security Assessments** | | | |
| The purpose of the policy is to establish the requirements for security assessments. Security assessments ensure that information security is built into organizational Resources; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions as part of security authorization processes; and ensure compliance to vulnerability mitigation procedures.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CA-2 | CA-2 (CE1) | CA-2 |   It is the policy of the Agency that the NCDOR IT Security Department must:   1. Develop a security assessment plan that describes the scope of the assessment, including:    1. Security controls and control enhancements under assessment; and    2. Assessment procedures to be used to determine security control effectiveness; and    3. Assessment environment, assessment team, and assessment roles and responsibilities. 2. Assess the security controls in the Resource and its environment, at a minimum, every 18 months to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; and 3. Produce a security assessment report that documents the results of the assessment; and 4. Provide the results of the security control assessment to the Agency Chief Information Officer and Chief Information Security Officer, as well as to the Provider CIO; and 5. Security assessments on Resources that store, process or transmit Data classified as Federal Tax Information are required immediately upon implementation and within 18 months thereafter for this Resource.   Control Enhancement  CE1. The Agency employs impartial assessors or assessment teams to conduct security control assessments. Impartiality is defined as assessors that are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* *Security assessments will be conducted by NCDOR as part of the Certification & Accreditation Process and as part of any contractual obligation outside of this process.* | | | |
| <Provider> Response | | | |
|  | *Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.*  *To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | CE1 | *Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | CE1 |  | |

|  |  |  |
| --- | --- | --- |
| **(CA-3) Resource Interconnections** | | |
| The purpose of the policy is to ensure that the Agency carefully consider the risks that may be introduced when Resources are connected to other Resources with different security requirements and security controls, both within organizations and external to organizations.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CA-3 | CA-3 (CE5) | CA-3 (CE5) |   It is the policy of the Agency that the NCDOR CIO must authorize connections from Resource to Resource.  a) To connect to an external Resource there must be an Interconnection Security Agreement. The agreement must document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. The Agency may also incorporate Interconnection Security Agreement information into Memorandums of Understanding (MOUs) for interconnections established between state agencies; and  b) If interconnecting systems are within the Agency, the Interconnection Security Agreement is not needed and may simply describe the interface characteristics between those interconnecting Resources in their respective security plans; and  c) IT Security must review and update the system interconnection or Resource security plan every 18 months and the NCDOR CIO must reauthorize the connection.  Control Enhancement  CE5. The connection must employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit Data classified as Federal Tax Information to connect to external information systems. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* *The NCDOR CIO will review the authorization package as part of the Certification & Accreditation process. During this process the Resource documentation will be reviewed by the CIO before an ATO is granted, including any interconnections to other components/systems/resources.* | | |
| <Provider> Response | | |
| *This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE5 | *Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE5 |  |

|  |  |  |
| --- | --- | --- |
| **(CA-5) Plan of Action and Milestones** | | |
| The purpose of the policy is to ensure that the Agency documents remedial actions.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CA-5 | CA-5 | CA-5 |   It is the policy of the Agency the Plan of Action and Milestones (POA&M) is reflected in the NCDOR IT tracking system to track vulnerabilities identified. The POA&M will be updated quarterly, at a minimum by the NCDOR IT Security Team.   1. Each issue will be identified by the portfolio segment type “Compliance” and be assigned a value based on the combination of Impact (Severity) and the level of effort that will be required to remediate the issue; and 2. All items in the tracking system will be processed according to the portfolio management procedures; and 3. Remediation plans will be documented as part of the Service Design process; and 4. Remediation and testing will be executed as defined by the Service Transition process; and 5. All remediation items will be audited by NCDOR IT Security once the item has been moved into Service Operations and results documented in the tool. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:*  **Planned Security Controls:** *A plan of actions and milestones will be developed, and the findings tracked by the NCDOR and remediated by the Provider as described in the NCDOR Security Policy manual.* | | |
| <Provider> Response | | |
| *Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |

|  |  |  |
| --- | --- | --- |
| **(CA-6) Security Authorization** | | |
| The purpose of the policy is to authorize all Resources prior to being implemented for use.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CA-6 | CA-6 | CA-6 |   It is the policy of the Agency that the Agency CIO is the authorizing official for all Resource component(s) and must provide authorization before commencing operations. In addition, all Resource authorizations must be approved again every three years or if there is a significant change to the Resource.  In order to submit for authorization the following information must be provided to the Agency’s CIO:  a) The Agency and Provider must approve that the architecture adheres to the established standards, or approve the exception; and  b) The Agency’s CISO must approve that the Resource meets all relevant security policies and controls or approves the exception. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control Implementation***:* | | |
| <Provider> Response | | |
| *Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.* | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |

|  |  |  |
| --- | --- | --- |
| **(CA-7) Continuous Monitoring** | | |
| The purpose of the policy is to ensure that Resources are monitored to protect confidentiality and integrity of Data appropriately.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CA-7 | CA-7 (CE1) | CA-7 |   It is the policy of the Agency that the Provider must implement a continuous monitoring strategy and implement a continuous monitoring program that includes defined metrics to be monitored annually, ongoing security control assessments and continual security status monitoring.  Control Enhancement  CE1. The organization employs impartial assessors or assessment teams that to monitor the security controls in the Resource on an ongoing basis. Impartiality is defined as assessors that are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.* | | |
|  | CE1 | *Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |

### Configuration Management Policy Family (CM)

|  |  |
| --- | --- |
| **(CM-1) Configuration Management Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the configuration management policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-1 | CM-1 | CM-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the configuration management procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(CM-2) Baseline Configuration** | | |
| The purpose of the policy is to ensure that baseline configurations are maintained.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-2 | CM-2 (CE1) (CE3)(CE7) | CM-2 (CE1) |   It is the policy of the Agency to develop, document, and maintain under configuration control, a current baseline configuration of the Resource.  Control Enhancements  CE1. The Provider must review and update the baseline configuration of the Resource:  a) At a minimum annually; and  b) When required due to system upgrades, patches, or other significant changes; and  c) As an integral part of Resource component installations and upgrades.  For Data classified as FTI, the Provider must use SCSEMs provided on the Office of Safeguards website for developing a Resource baseline configuration.  CE3. The Provider retains at least 1 previous configuration version to support rollback.  CE7. The Agency may choose to:  a) Issues mobile devices with special configurations to individuals traveling to locations that the Agency deems to be of significant risk; and  b) Applies standard configurations to the devices when the individuals return. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.* | | |
|  | CE1 | *Related control: CM-5.* |
|  | CE1 a. |  |
|  | CE1 b |  |
|  | CE1 c. |  |
|  |  | |
|  | CE3 | *Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.* |
|  | CE7 | *When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.* |
|  | CE7 a. |  |
|  | CE7 b. |  |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE1 a. |  |
|  | CE1 b |  |
|  | CE1 c. |  |
|  |  | |
|  | CE3 |  |
|  | CE7 |  |
|  | CE7 a. |  |
|  | CE7 b. |  |

|  |  |  |
| --- | --- | --- |
| **(CM-3) Configuration Change Control** | | |
| The purpose of the policy is to ensure that changes to Resources are controlled, documented and that security is properly considered.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | CM-3 (CE2) | CM-3 (CE2) |   It is the policy of the Agency that changes to Resources is methodical.   1. The Agency will determine the types of changes to Resources that are configuration controlled; and 2. The Agency will review proposed configuration-controlled changes and approve or disapprove such changes with explicit consideration for security impact analyses; and 3. The Provider will document configuration change decisions; and 4. The Provider will implement approved configuration-controlled changes; and 5. The Provider will retain records of configuration-controlled changes to the Resource for the life of the system; and 6. The Agency will audit and review activities associated with configuration-controlled changes; and   g) The Provider will coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur.  Control Enhancement  CE2. The Provider will also test, validate, and document changes to the Resource before implementing the changes on the operational system unless there is a major change to the Resource, in which case the Agency will assess the Resource before changes can be implemented into the operational system. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***: Proposed changes to the Resource must be submitted to the Agency’s CISO for review.* | | |
| <Provider> Response | | |
| *Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE2 | *Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE2 |  |

|  |  |
| --- | --- |
| **(CM-4) Security Impact Analysis** | |
| The purpose of the policy is to ensure that configuration changes to Resources must be reviewed to prevent negative impact to security.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-4 | CM-4 | CM-4 |   It is the policy of the Agency that prior to implementing changes being made to resources that the Agency must analyze the proposed changes for security impacts. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* *Proposed changes to the Resource must be submitted to the Agency’s CISO for review.* | |
| <Provider> Response | |
|  | *Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(CM-5) Access Restrictions for Change** | |
| The purpose of the policy is to ensure that the Staff who can make changes to Resources is limited.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | CM-5 | CM-5 |   It is the policy of the Agency that the Provider define, document, approve and enforce physical and logical access restriction associated with changes to Resources. The documented access restrictions must be submitted to the Agency when a major change to the Resource is proposed and will be audited by the Agency for minor changes. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(CM-6) Configuration Settings** | | |
| The purpose of the policy is to ensure that Resource configuration changes are properly documented.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-6 | CM-6 | CM-6 |   It is the policy of the Agency that for all Resources configuration settings must be documented by the Provider using IRS Office of Safeguards approved compliance requirements (e.g. SCSEMs, assessment tools) that reflect the most restrictive mode consistent with operational requirements.  The Provider must:  a) Implement approved configuration settings; and  b) Identify, document, and submit for review any deviations from established configuration settings; and  c) Monitor and control changes to the configuration settings. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.*  *Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |  |
| --- | --- | --- |
| **(CM-7) Least Functionality** | | |
| The purpose of the policy is to ensure that Resources are configured with only the functionality that is required, and no more.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-7 | CM-7 (CE1) (CE2) (CE4) | CM-7 |   It is the policy of the Agency for all Resources that they are configured with only essential capabilities.    a) Restrict or prohibit the use of functions, ports, protocols or services. For Data classified as FTI, restrict or prohibit the use of functions, ports, protocols or services as defined in the IRS Office of Safeguards-approved compliance requirement (e.g. IRS SCSEMs, assessment tools); and  b) Review the Resource as part of the vulnerability assessments to identify unnecessary or non-secure functions, ports, protocols, and services per Vulnerability Scanning (RA-5); and  c) Disable defined functions, ports, protocols, and services within the Resource deemed to be unnecessary or non-secure.  Control Enhancements  CE1. a) The Agency reviews the Resource at a minimum of every 18 months to identify unnecessary and/or non-secure functions, ports, protocols, and services; and  b) Disables defined functions, ports, protocols, and services within the Resource deemed to be unnecessary or non-secure.  CE4. a) The Agency identifies software programs not authorized to execute on Resources; and  b) The Provider an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the Resource; and  c) The Provider reviews and updates the list of unauthorized software programs annually. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control Implementation:** | | |
| <Provider> Response | | |
| *Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE1 | *The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.* |
|  | CE1 a. |  |
|  | CE1 b. |  |
|  | CE4 | *The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.* |
|  | CE4 a. |  |
|  | CE4 b. |  |
|  | CE4 c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE1 a. |  |
|  | CE1 b. |  |
|  | CE4 a. |  |
|  | CE4 b. |  |
|  | CE4 c. |  |

|  |  |  |
| --- | --- | --- |
| **(CM-8) Resource Component Inventory** | | |
| The purpose of the policy is to ensure that Resource component inventory is properly maintained.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-8 | CM-8 (CE1) (CE3) (CE5) | CM-8 (CE1) |   It is the policy of the Agency for this Resource:  a) That the Provider maintains an inventory of owned components that:  1. Accurately reflects the current state; and  2. Includes all components; and  3. Is at the level of granularity deemed necessary for tracking and reporting; and  4. Includes information deemed necessary to achieve effective Resource component accountability.  b) Review and update the component inventory through periodic manual inventory checks or network monitoring tool that automatically maintains inventory; and  c) All additional requirements for maintaining a Resource component inventory are provided in NIST SP 800-70 Rev 2 Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers.  Control Enhancements  CE1. That the Provider updates the inventory of owned Resource components as an integral part of component installations, removals and updates.  CE3. The Provider:  a) Employs automated mechanisms weekly to detect the presence of unauthorized hardware, software, and firmware components within the authorization boundary of the capability; and  b) Disables network access by such components; isolates the components; notifies the CISO and CIO.  CE5. The Provider verifies that all owned components within the authorization boundary of the Resource are not duplicated in other Resource component inventories. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.* | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | b. |  |
|  | c. |  |
|  | CE1 |  |
|  | CE3 | *This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.* |
|  | CE3 a. |  |
|  | CE3 b. |  |
|  | CE5 | *This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.* |
| NCDORResponse | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | b. |  |
|  | c. |  |
|  | CE1 |  |
|  | CE3 a. |  |
|  | CE3 b. |  |
|  | CE5 |  |

|  |  |  |
| --- | --- | --- |
| **(CM-9) Configuration Management** | | |
| The purpose of the policy is to set forth the requirements for a configuration management plan.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | CM-9 | CM-9 |   It is the policy of the Agency to develop, document and implement a configuration management plan for all Resources that:  a) Addresses roles, responsibilities, and configuration management processes and procedures; and  b) Establishes a process for identifying configuration items throughout the system development lifecycle (SDLC) and for managing the configuration of the configuration items; and  c) Defines the configuration items for the information system and places the configuration items under configuration management; and  d) Protects the configuration management plan from unauthorized disclosure and modification. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |

|  |  |  |
| --- | --- | --- |
| **(CM-10) Software Usage Restrictions** | | |
| The purpose of the policy is to make sure that software is licensed properly.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-10 | CM-10 | CM-10 (CE1) |   It is the policy of the Agency that all software must be used in accordance with contract agreements and copyright laws.    a) All software usage must be tracked and improper copying or distribution is strictly prohibited; and  b) Peer-to-peer file sharing technology is prohibited in order to prevent unauthorized distribution, display, performance or reproduction of copyrighted work.  Control Enhancement  CE1. Open source software must be legally licensed, approved for use by the Agency’s CISO and adheres to a secure configuration baseline checklist from the U.S. Government or industry. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |

|  |  |
| --- | --- |
| **(CM-11) User Installed Software** | |
| The purpose of the policy is to make sure that software installed by non-IT Staff does not violate contracts, copyright laws or create security issues.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CM-11 | CM-11 | CM-11 |     It is the policy of the Agency that software may not be installed by non-IT Staff unless specifically authorized by the Provider’s CIO. Software installation must be prohibited, and compliance monitored, through automated methods when practical. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.* |
| NCDORResponse | |
|  |  |

### Contingency Planning Policy Family (CP)

|  |  |
| --- | --- |
| **(CP-1) Contingency Planning Process** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the contingency planning policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CP-1 | CP-1 | CP-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the contingency planning procedures must be documented and disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(CP-2) Contingency Plan** | | |
| The purpose of the policy is to develop plans to ensure that Data and Resources are available, based on the risk assessment.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CP-2 | CP-2 (CE1)(CE3)(CE8) | CP-2 |   It is the policy of the Agency that each Resource:  a) The Provider must have a contingency plan that:  1. Identifies essential missions and business functions and associated contingency requirements; and  2. Provides recovery objectives, restoration priorities, and metrics; and  3. Addresses contingency roles, responsibilities, assigned individuals with contact information; and  4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and  5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and  6. Is reviewed and approved by the respective Provider’s CIO.  b) Distributes copies of the contingency plan to key contingency personnel (including the Agency’s CISO), at a minimum; and  c) The Provider coordinates contingency planning activities with incident handling activities; and  d) The Provider reviews the contingency plan for the Resource annually; and  e) The Provider updates the contingency plan to address changes to the organization, Resources, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and  f) The Provider communicates contingency plan changes to key contingency personnel and to the Agency’s CISO, at a minimum; and  g) The Provider protects the contingency plan from unauthorized disclosure and modification.  Control Enhancements  CE1. The Agency coordinates contingency plan development with organizational elements responsible for related plans.  CE3. The Provider plans for the resumption of essential missions and business functions within the stated recovery objective of each capability after contingency plan activation.  CE8. The Provider identifies critical information system assets supporting essential missions and business functions. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.* | | |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | a.5 |  |
|  | a.6 |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE1 | *Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.* |
|  | CE3 | *Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.* |
|  | CE8 | *Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information* |
| NCDORResponse | | |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | a.5 |  |
|  | a.6 |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE1 |  |
|  | CE3 |  |
|  | CE8 |  |

|  |  |
| --- | --- |
| **(CP-3) Contingency Training** | |
| The purpose of the policy is to make sure that Staff who could be involved in the recovery of Resources is trained to execute contingency plans.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CP-3 | CP-3 | CP-3 |   It is the policy of the Agency that contingency training is provided to Resource users consistent with assigned roles and responsibilities prior to assuming a contingency role or responsibility. Training should be refreshed in the event of a major change to the Resource and annually thereafter. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(CP-4) Contingency Plan Testing** | | |
| The purpose of the policy is to make sure that contingency plans are tested.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CP-4 | CP-4 (CE1) | CP-4 |   It is the policy of the Agency that prior to any Resource being released into production for general use that the contingency plan is tested and then, at a minimum, annually thereafter.  a) The plan should be tested for effectiveness to ensure that the Provider and/or the Agency are ready to execute it if needed; and  b) Contingency plan testing results should be reviewed and corrective actions implemented if needed.  Control Enhancement  CE1. The Agency coordinates contingency plan testing with organizational elements responsible for related plans. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.* | | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 | *Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.* | |
| NCDORResponse | | | |
|  | | | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 |  | |

|  |  |  |
| --- | --- | --- |
| **(CP-6) Alternate Storage Site** | | |
| The purpose of the policy is to endure the recovery of backup information in the event of a disaster.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | CP-6 (CE1)(CE3) | CP-6 |   It is the policy of the Agency that the Provider:  a) Establish an alternative storage site, including necessary agreements to permit the storage and retrieval of Resource backup information; and  b) Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site. If the Resource backup information contains Data classified as Federal Tax Information, the Provider must ensure that the alternative storage site provides information security safeguards that meet the IRS Publication 1075 revision October 2015 Section 4.2 – Minimum Protection Standards and the disclosure provisions of Internal Revenue Code § 6103 Confidentiality and disclosure of returns.  Control Enhancements  CE1. The Provider identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.  CE3. The Provider identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.* |
|  | CE3 | *Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.* |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |
|  | CE3 |  |

|  |  |  |
| --- | --- | --- |
| **(CP-7) Alternate Processing Site** | | |
| The purpose of the policy is to make sure that normal operations are resumed in the event of a disaster.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | CP-7 (CE1)(CE2)(CE3) | CP-7 |     It is the policy of the Agency to establish an alternative processing site including necessary agreements to permit the transfer and resumption of Resources for essential missions/business functions within the recovery period identified for the Resource (See CP-2).  a) Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the time period defined in the contingency plan for transfer/resumption; and  b) Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site. In the event that the Resource stores, processes or transmits Data classified as Federal Tax Information, the alternate processing site must provide information security safeguards that meet the minimum protection standards and the disclosure provisions of Internal Revenue Code § 6103 Confidentiality and disclosure of returns.  Control Enhancements  CE1. The Provider identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.  CE2. The Provider identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.  CE3. The Provider develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.* |
|  | CE2 | *Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.* |
|  | CE3 | *Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |
|  | CE2 |  |
|  | CE3 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(CP-9) Resource Backup** | | | |
| The purpose of the policy is to ensure the backup of Agency information.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CP-9 | CP-9 (CE2) | CP-9 |   It is the policy of the Agency to conduct backups of user-level information, system-level information, and security-related documentation consistent with the defined frequency in the Resource contingency plan. In the event that the backup contains Data classified as Federal Tax Information, the confidentiality of backup information at storage locations will be protected pursuant to Internal Revenue Code § 6103 Confidentiality and disclosure of returns requirements. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.* | | |
|  | CE2 | *Related control: CP-4.* |
| NCDORResponse | | | |
|  |  | | |

|  |  |  |
| --- | --- | --- |
| **(CP-10) Resource Recovery and Reconstitution** | | |
| The purpose of the policy is to ensure the Agency can recover from a disaster.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | CP-10 | CP-10 (CE2) | CP-10 |   It is the policy of the Agency to provide for the recovery and reconstitution of the Resource to a known state after a disruption, compromise, or failure.  Control Enhancement  CE2. The Resource implements transaction recovery if it is transaction-based. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.* | | |
|  | CE2 | *Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.* |
| NCDORResponse | | |
|  | | |
|  | CE2 |  |

### Facilities Security (FS)

|  |  |  |
| --- | --- | --- |
| **(FS-1) Staff Responsibilities** | | |
| The purpose of the policy is to establish the responsibilities of all Staff as it relates to the security of  Facilities.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-1 | FS-1 | FS-1 |   All Staff must:  a) Observe surroundings.  b) Report to Security Guards any unusual activity.  c) Report any threats (actual or perceived) against the Agency or any Agency staff.  d) Safeguard their badge at all times, and wear it between the neck and waist.  e) Report a lost or stolen badge immediately to the Service Desk or Security Guard.  f) Not allow another individual to “piggyback” or “tailgate” through security checkpoints (e.g. doors with badge access).  g) Never share their badge. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |

|  |  |  |
| --- | --- | --- |
| **(FS-2) Management Responsibilities** | | |
| The purpose of the policy is to establish the responsibilities of managers as it relates to the security of  Facilities.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-2 | FS-2 | FS-2 |   It is the policy of the Agency that managers actively participate in ensuring the security of Facilities.  a) Notify the badge authorization personnel of Staff termination, so access badges can be immediately revoked.  b) Facility access must be terminated immediately and the manager can later submit approved access request form to remove all other system access of employee or contractor. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |

|  |  |
| --- | --- |
| **(FS-3) Threats** | |
| The purpose of the policy is to ensure that threats are promptly and appropriately reported.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-3 | FS-3 | FS-3 |   It is the policy that Staff is required to immediately report any threat, actual or perceived, against the  Agency, Staff, or any other criminal threat to the Security Guards. Only Security Guards should attempt to deal with a physical threat. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  |  |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(FS-4) Visitors** | | |
| The purpose of the policy is to ensure that visitors are properly controlled while in a Facility.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-4 | FS-4 | FS-4 |   It is the policy of the Agency that access to Facilities is controlled.  a) Visitors must provide proof of identity before being granted access to areas where Resources reside or Data is transmitted, stored or processed. Visitors must be escorted at all times while in such areas. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | | |
|  | a. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |

|  |  |  |
| --- | --- | --- |
| **(FS-5) Staff Background Screening** | | |
| The purpose of the policy is to ensure that background screens are performed and the screening process is administered consistently, equally and fairly to all Provider Staff and prospective Staff who have access to Agency Resource components.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-5 | FS-5 | FS-5 |   Background screening of Agency employees, contractors and prospective employees shall have the  objective and focus on the following:  a) Compliance with IRS Publication 1075 requirements (and protection of Data classified as Federal Taxpayer Information).  b) Compliance with PCI Data Security Standard requirements.  c) Compliance with all regulatory mandates and laws enforced by state and federal agencies.  d) Fulfilling other legal or contractual obligations.  e) Providing a safe work environment.  f) Protecting Agency assets.  g) Reducing risk of legal liabilities. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |

|  |  |  |
| --- | --- | --- |
| **(FS-6) Minimum Protection of Data Classified as Federal Tax Information (FTI)** | | |
| The purpose of the policy is to ensure that Providers establish a uniform method of physically protecting Data and Resources as well as non-electronic forms of FTI.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-6 | FS-6 | FS-6 |   It is the policy of the Agency that a minimum protection standard be established and maintained to inform Agency Staff as to what constitutes minimum protection of FTI per IRS regulations (IRS 1075, section 4.2).  IT Security Staff will:  a) Document, disseminate and review, at minimum, every 18 months a Minimum Protection Standard for safeguarding FTI. The Minimum Protection Standards should cover the following subjects:  1. Secured Perimeter  2. Security Room  3. Badged Staff  4. Security Contain | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |

|  |  |  |
| --- | --- | --- |
| **(FS-7) Restricted Area Access** | | |
| The purpose of the policy is to ensure that there are appropriate measures in place to prevent unauthorized access to Data by creating restricted areas where such Data resides.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-7 | FS-7 | FS-7 |   It is the policy of the Agency to have procedures that ensure Data is protected by restricting physical access to areas (i.e. restricted areas) where such Data resides.  a) All restricted areas shall have at least two barriers of protection to deter, delay, or detect illegal or unauthorized entry.  b) Data must be containerized in areas where other than authorized Staff may have access afterhours.  c) Access to Restricted Areas must be monitored and records maintained of all persons entering these areas.  d) The Agency must establish procedures for restricted area access including:  1. Protection of Data after normal business hours.  2. Appropriate storage containers.  3. Signs should be prominently posted.  4. Visitor access log that complies with IRS 1075, section 4.3 “Restricted Area Access”.  5. Visitor sign-in and validation of visitor’s identity.  6. Use Authorized Access List.  7. Control Access to Areas.  8. Control and Safeguard Keys and Combinations  9. Keep to a minimum physical keys (or knowledge of combination) to restricted areas  10. Protect Data in Transit  e) Restrict physical access to Data or Resources that house cardholder data (“PCI data”).  1. Including limiting and monitoring physical access to Resources in the cardholder data environment, developing procedures regarding badge access, and controlling access to restricted areas.  2. Procedures should comply with PCI DSS v3.0, Requirement 9. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | d.1 |  |
|  | d.2 |  |
|  | d.3 |  |
|  | d.4 |  |
|  | d.5 |  |
|  | d.6 |  |
|  | d.7 |  |
|  | d.8 |  |
|  | d.9 |  |
|  | d.10 |  |
|  | e. |  |
|  | e.1 |  |
|  | e.2 |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | d.1 |  |
|  | d.2 |  |
|  | d.3 |  |
|  | d.4 |  |
|  | d.5 |  |
|  | d.6 |  |
|  | d.7 |  |
|  | d.8 |  |
|  | d.9 |  |
|  | d.10 |  |
|  | e. |  |
|  | e.1 |  |
|  | e.2 |  |

|  |  |  |
| --- | --- | --- |
| **(FS-8) Physical Security of Resources and Data** | | |
| The purpose of the policy is to ensure that the Agency protects its Resources and Data.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-8 | FS-8 | FS-8 |   It is the policy of the Agency to have procedures that ensure basic security requirements are met for keeping Data protected.  The Provider must:  a) Keep in a secure area with restricted access Data and Resources that receive, process, store, or transmit Data.  b) In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, Resources must receive the highest level of protection practical, including full disk encryption.  c) All Resources that contain Data and are resident in an alternate work site must employ encryption mechanisms to ensure that the Data may not be accessed. If the computer is lost or stolen, it must be reported immediately to the employee’s manager and to the IT Service Desk.  d) Basic security requirements must be met, such as keeping Resources and Media locked up when not in use.  e) When removable media contains FTI, it must be labeled as such.  f) All Resources and media containing Data must be kept in a secured area under the immediate protection and control of an authorized Staff or locked up. When not in use, the Media must be promptly returned to a proper storage area/container.  g) Inventory records of electronic Media must be maintained and reviewed semi-annually for control and accountability.  h) Physical access to transmission medium (e.g., cabling), should be protected and access restricted. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |

|  |  |  |
| --- | --- | --- |
| **(FS-9) Media Off-site Storage Requirements** | | |
| The purpose of the policy is to ensure that the Agency protects its Media that contains Data.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-9 | FS-9 | FS-9 |   It is the policy of the Agency that when using off-site storage Facilities, if the following conditions are met that no additional IRS safeguarding controls related to physical access will apply:  a) The Media is encrypted.  b) The Media is locked in a turtle case.  c) The Agency retains the key to the turtle case. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |
| --- | --- |
| **(FS-10) Alternative Work Locations** | |
| The purpose of the policy is to ensure that the confidentiality and integrity of Data is protected.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | FS-10 | FS-10 | FS-10 |   It is the policy of the Agency that all policies apply at telework sites (e.g. Staff homes).  The Agency must conduct periodic inspections of alternative work sites during the year to ensure compliance with all policies. The results of each inspection shall be fully documented. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  |  |
| NCDORResponse | |
|  |  |

### Identification and Authentication Policy Family (IA)

|  |  |
| --- | --- |
| **(IA-1) Identification and Authentication Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the identification and authentication policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-1 | IA-1 | IA-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the identification and authentication procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(IA-2) Identification and Authentication** | | |
| The purpose of the policy is to make sure that Staff can be uniquely identified and authenticated prior to accessing a Resource.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-2 (CE1)(CE12) | IA-2 (CE1) (CE2) (CE3) (CE8) (CE11) (CE12) | IA-2 (CE1)(CE2) (CE11) |   It is the policy of the Agency that each Resource must be able to uniquely identify and authenticate Staff or processes acting on behalf of Staff (i.e. Staff may not share accounts).  Control Enhancements  CE1. The Resource implements multifactor authentication for network access to privileged accounts.  CE2. The Resource implements multifactor authentication for network access to non-privileged accounts.  CE3. The information system implements multifactor authentication for local access to privileged accounts.  CE8. The Resource implements replay-resistant authentication mechanisms for network access to privileged accounts.  CE11. The Resource implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. Note: NIST SP 800-63-2 allows the use of software tokens.  CE12. The Resource accepts and electronically verifies Personal Identity Verification (PIV) credentials. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.*  *Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.* | | |
|  | CE1 | *Related control: AC-6.* |
|  | CE2 |  |
|  | CE3 | *Related control: AC-6.* |
|  | CE8 | *Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.* |
|  | CE11 | *For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.* |
|  | CE12 | *This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE2 |  |
|  | CE3 |  |
|  | CE8 |  |
|  | CE11 |  |
|  | CE12 |  |

|  |  |
| --- | --- |
| **(IA-3) Identification and Authentication (Devices)** | |
| The purpose of the policy is to make sure that devices are uniquely identified.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | IA-3 | IA-3 |     It is the policy of the Agency that each Resource must be able to uniquely identify and authenticate devices before establishing a connection.  Organizational devices requiring unique device to device identification and authentication may be defined by type, device, or a combination. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(IA-4) Identifier Management** | | | |
| The purpose of the policy is to make sure that Resource identifiers are properly managed. Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-4 | IA-4 | IA-4 |     It is the policy of the Agency that Resource identifiers must be managed by:  a) Receiving authorization from the Agency’s CIO to assign an individual, group, role, or Resource identifiers; and  b) Selecting an identifier that identifies Staff, group, role, or Resource; and  c) Assigning the identifier to the intended Staff, group, role, or Resource; and  d) Preventing reuse of identifiers; and  e) Disabling the identifier after 120 days. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(IA-5) Authenticator Management** | | | |
| The purpose of the policy is to make sure that authenticators are properly managed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-5 (CE1) (CE11) | IA-5 (CE1) (CE2) (CE3) (CE11) | IA-5 (CE1) |   It is the policy of the Agency that the Provider manage Resource authenticators by:  a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; and  b) Establishing initial authenticator content for authenticators defined by the Agency. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length); and  c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; and  d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; and  e) Changing default content (e.g., the initial password) of authenticators prior to information system installation; and  f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; and  g) Changing/refreshing authenticators; and  h) Protecting authenticator content from unauthorized disclosure and modification; and  i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and  j) Changing authenticators for group/role accounts when membership to those accounts changes.  Control Enhancements  CE1. For password-based authentication the Resource must:  a) Enforce minimum password complexity of:  1. Eight characters; and  2. At least one numeric and at least one special character; and  3. A mixture of at least one uppercase and at least one lowercase letter; and  4. Storing and transmitting only encrypted representations of passwords.  b) Enforce password minimum lifetime restriction of one day; and  c) Enforce non-privileged account passwords to be changed at least every 90 days; and  d) Enforce privileged account passwords to be changed at least every 60 days; and  e) Prohibit password reuse for 24 generations; and  f) Allow the use of a temporary password for system logons requiring an immediate change to a permanent password; and  g) Password-protect system initialization (boot) settings.  CE2. The information system, for PKI-based authentication:  a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; and  b) Enforces authorized access to the corresponding private key; and  c) Maps the authenticated identity to the account of the individual or group; and  d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.  CE5. The Agency requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.  CE11. For hardware token-based authentication, the Resource employs mechanisms that satisfy Agency specifics such as working with a particular PKI. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | f. |  | |
|  | g. |  | |
|  | h. |  | |
|  | i. |  | |
|  | j. |  | |
|  | CE1 | *This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.* | |
|  | CE1 a.1 |  | |
|  | CE1 a.2 |  | |
|  | CE1 a.3 |  | |
|  | CE1 a.4 |  | |
|  | CE1 b. |  | |
|  | CE1 c. |  | |
|  | CE1 d. |  | |
|  | CE1 e. |  | |
|  | CE1 f. |  | |
|  | CE1 g. |  | |
|  | CE2 | *Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing. Related control: IA-6.* | |
|  | CE2 a. |  | |
|  | CE2 b. |  | |
|  | CE2 c. |  | |
|  | CE2 d. |  | |
|  | CE5 | *This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.* | |
|  | CE11 | *Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | f. |  | |
|  | g. |  | |
|  | h. |  | |
|  | i. |  | |
|  | j. |  | |
|  | CE1 a.1 |  | |
|  | CE1 a.2 |  | |
|  | CE1 a.3 |  | |
|  | CE1 a.4 |  | |
|  | CE1 b. |  | |
|  | CE1 c. |  | |
|  | CE1 d. |  | |
|  | CE1 e. |  | |
|  | CE1 f. |  | |
|  | CE1 g. |  | |
|  | CE2 a. |  | |
|  | CE2 b. |  | |
|  | CE2 c. |  | |
|  | CE2 d. |  | |
|  | CE5 |  | |
|  | CE11 |  | |

|  |  |
| --- | --- |
| **(IA-6) Authenticator Feedback** | |
| The purpose of the policy is to make sure that passwords aren’t seen by others.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-6 | IA-6 | IA-6 |   It is the policy of the Agency that the Resource obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(IA-7) Cryptographic Module Authentication** | |
| The purpose of the policy is to make sure that encryption is strong enough.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-7 | IA-7 | IA-7 |   It is the policy of the Agency that all Resources must implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.  Validation provides assurance that when the Provider implements cryptography to protect FTI, the encryption functions have been examined in detail and will operate as intended.  All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(IA-8) Identification and Authentication (non-Staff)** | | |
| The purpose of the policy is to make sure that non-Staff can be uniquely identified and authenticated prior to accessing a Resource.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IA-8(CE2)(CE3)(CE4) | IA-8(CE1)(CE2)(CE3)(CE4) | IA-8 |   It is the policy of the Agency that each Resource must be able to uniquely identify and authenticate non-Staff or processes acting on behalf of non-Staff (i.e. Staff is strictly prohibited from sharing accounts).  Control Enhancements  CE1. The Resource accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.  CE2. The Resource accepts only FICAM-approved third-party credentials.  CE3. The Agency employs only FICAM-approved Resource components to accept third-party credentials.  CE4. The Resource conforms to FICAM-issued profiles. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.* | | |
|  | CE1 | *This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.* |
|  | CE2 | *This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.* |
|  | CE3 | *This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.* |
|  | CE4 | *This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE2 |  |
|  | CE3 |  |
|  | CE4 |  |

### Incident Response Policy Family (IR)

|  |  |  |
| --- | --- | --- |
| **(IR-1) Major Incident Response Procedures** | | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the Major Incident response policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-1 | IR-1 | IR-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the Major Incident response procedures must be SC-7ed, disseminated and reviewed at least annually.  a) The procedures must also include a definition and examples of what a Major Incident; and  b) The NIST Special Publication 800-61 Revision 2 should be used as a guide for incident response procedures. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |

|  |  |
| --- | --- |
| **(IR-2) Incident Response Training** | |
| The purpose of the policy is to ensure that Staff are trained in Major Incident response processes.     |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-2 | IR-2 | IR-2 |   It is the policy of the Agency that Staff are trained in their Major Incident response roles prior to assuming a Major Incident response role or responsibility, when a change occurs in a Major Incident response process for a Resource and annually thereafter. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* *<PROVIDER> will train employees to immediately report suspected incidents to the NCDOR Service Desk and to work with the NCDOR and the IRS (if required) throughout the incident handling process.* | |
| <Provider> Response | |
|  | *Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(IR-3) Incident Response Testing** | | |
| The purpose of the policy is to ensure that Major Incident responses are tested annually.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | IR-3(CE2) | IR-3 |   It is the policy of the Agency that Major Incident response processes are tested annually.   1. The Provider must perform a tabletop exercise using scenarios that would be classified as a Major Incident including a breach of Data classified as Federal Tax Information (FTI); and 2. All Staff with significant Major Incident response capabilities must be included in the tabletop exercise along with NCDOR personnel identified by the CIO; and 3. Each exercise must produce and after-action report to improve the process. 4. For Major Incidents where FTI is involved:    1. The Provider must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, Provider must contact the NCDOR Service Desk immediately. Provider will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the Major Incident;    2. The Office of Safeguards will coordinate with the Agency regarding appropriate follow-up actions required to be taken by the Provider to ensure continued protection of FTI and the Agency will instruct the Provider on any necessary actions to be taken;    3. Once the Major Incident has been addressed, the Provider will conduct a post-action review to ensure the Major Incident response policies and procedures provide adequate guidance. 5. Any identified deficiencies in the Major Incident response policies and procedures should be resolved immediately; and 6. Additional training or any changes to the Major Incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.   Control Enhancement  CE2. The Agency coordinates incident response testing with organizational elements responsible for related plans. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d.1 |  |
|  | d.2 |  |
|  | d.3 |  |
|  | e. |  |
|  | f. |  |
|  | CE2 | *Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d.1 |  |
|  | d.2 |  |
|  | d.3 |  |
|  | e. |  |
|  | f. |  |
|  | CE2 |  |

|  |  |  |
| --- | --- | --- |
| **(IR-4) Major Incident Handling** | | |
| The purpose of the policy is to ensure that Major Incident processes are coordinated and improved over time.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-4 | IR-4(CE1) | IR-4 |   It is the policy of the Agency that Major Incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery:   1. Coordinate Major Incident handling activities with contingency planning activities; and 2. Incorporate lessons learned from ongoing Major Incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.   Control Enhancement  CE1. The Provider employs automated mechanisms to support the incident handling process. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.* | | |
|  | a. |  |
|  | b. |  |
|  | CE1 | *Automated mechanisms supporting incident handling processes include, for example, online incident management systems.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | CE1 |  |

|  |  |
| --- | --- |
| **(IR-5) Incident Monitoring** | |
| The purpose of the policy is to ensure that Major Incidents are documented.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-5 | IR-5 | IR-5 |   It is the policy of the Agency that Major Incidents are tracked and documented. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* *NCDOR will track and document all incidents as defined in the NCDOR Information Security Incident Management Plan.* | |
| <Provider> Response | |
|  | *Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(IR-6) Incident Reporting** | | |
| The purpose of the policy is to ensure that Major Incidents are reported timely and to all required parties.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-6 | IR-6(CE1) | IR-6 |   It is the policy of the Agency that the Provider report suspected security incidents to the NCDOR Service Desk upon discovery of the incident. The NCDOR Service Desk will follow the NCDOR Incident Response process to ensure that incidents are reported as required.  Control Enhancement  CE1. The Provider employs automated mechanisms to assist in the reporting of security incidents. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.* | | |
|  | CE1 | *Related control: IR-7.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |

|  |  |  |
| --- | --- | --- |
| **(IR-7) Incident Response Assistance** | | |
| The purpose of the policy is to ensure that Major Incidents are reported.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-7 | IR-7(CE1) | IR-7 |   It is the policy of the Agency that the Provider’s IT Security Department will provide an incident response support resource, integral to the Provider incident response capability that offers advice and assistance to users of Resources for the handling and reporting of security incidents.  Control Enhancement  CE1. The Provider employs automated mechanisms to increase the availability of incident response-related information and support. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.* | | |
|  | CE1 | *Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |

|  |  |  |
| --- | --- | --- |
| **(IR-8) Incident Response Plan** | | |
| The purpose of the policy is to ensure that there is a Major Incidents response plan.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | IR-8 | IR-8 | IR-8 |   It is the policy of the Agency that the there is a process for dealing with Major Incidents.   1. The process:    1. Provides the Provider with a process for implementing its Major Incident response capability; and    2. Describes the structure of the Major Incident response capability; and    3. Provides a high-level approach for how the Major Incident response process fits into the overall Agency; and    4. Meets the unique requirements of the Provider, which relate to mission, size, structure, and functions; and    5. Provides metrics for measuring the Major Incident response capability within the Agency; and    6. Defines the resources and management support needed to effectively maintain and mature a Major Incident response process; and    7. Is reviewed and approved by the Provider’s CIO. 2. Distribute copies of the Major Incident response process to authorized Major Incident response personnel; and 3. Review the Major Incident response process at a minimum on an annual basis or as an after-action review; and 4. Update the Major Incident response process to address system/Agency changes or problems encountered during plan implementation, execution, or testing; and 5. Communicate Major Incident response process changes to authorized Major Incident response personnel; and 6. Protect the Major Incident response procedure from unauthorized disclosure and modification. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.* | | |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | a.5 |  |
|  | a.6 |  |
|  | a.7 |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
| NCDORResponse | | |
|  | | |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | a.4 |  |
|  | a.5 |  |
|  | a.6 |  |
|  | a.7 |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |

|  |  |  |
| --- | --- | --- |
| **(IR-9) Data Spillage Response** | | |
| The purpose of the policy is to ensure that if Data is mishandled, that there is a process to address it.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | IR-9 |   It is the policy of the Agency that the there is a process for dealing with Data spillage. The process must respond to spills by:   1. Identifying the specific Data involved in the Resource contamination; and 2. Alerting authorized Major Incident response personnel and NCDOR of the spill using a method of communication not associated with the spill; and 3. Isolating the contaminated Resource or component; and 4. Eradicating the Data from the contaminated Resource or component; and 5. Identifying other Resources or components that may have been subsequently contaminated. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |

### Maintenance Policy Family (MA)

|  |  |
| --- | --- |
| **(MA-1) Resource Maintenance Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the maintenance policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MA-1 | MA-1 | MA-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the maintenance procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MA-2) Controlled Maintenance** | | | |
| The purpose of the policy is to ensure that maintenance activities on Resources are managed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MA-2 | MA-2 | MA-2 |   It is the policy of the Agency to:  a) Schedule, perform, document, and review records of maintenance and repairs on Resources and components in accordance with manufacturer or vendor specifications and Agency requirements; and  b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the Resource is serviced on site or removed to another location; and  c) Require that the CIO explicitly approve the removal of the Resource or components from Agency facilities for off-site maintenance or repairs; and  d) Sanitize Resources to remove all Data classified as Data from associated media prior to removal from Agency facilities for off-site maintenance or repairs; and  e) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions and update Agency maintenance records accordingly. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |  |
| --- | --- | --- |
| **(MA-3) Maintenance Tools** | | |
| The purpose of the policy is to ensure that maintenance tools are appropriate.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | MA-3 (CE1) (CE2) | MA-3 |   It is the policy of the Agency that the CISO must approve, control, and monitor Resource maintenance tools.  **Control Enhancements**  CE1. The Agency inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.  CE2. The Agency checks media containing diagnostic and test programs for malicious code before the media are used in the information system. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.* | | |
|  | CE1 | *If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.* |
|  | CE2 | *If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE2 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MA-4) Non-Local Maintenance** | | | |
| The purpose of the policy is to ensure that maintenance that is provided remotely doesn’t compromise the confidentiality or integrity of Data or Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MA-4 | MA-4 (CE2) | MA-4 (CE2) |   It is the policy of the Agency that the CISO must:  a) Approve and monitor non-local maintenance and diagnostic activities; and  b) Allow the use of non-local maintenance and diagnostic tools only as consistent with Agency policy and documented in the security plan for the Resource; and  c) Employ multi-factor authenticator in the establishment of non-local maintenance and diagnostic sessions; and  d) Maintain records for non-local maintenance and diagnostic activities; and  e) Terminates session and network connections when non-local maintenance is completed.  **Control Enhancement**  CE2. The Agency documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | CE2 |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | CE2 |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MA-5) Maintenance Staff** | | | |
| The purpose of the policy is to ensure that maintenance Staff is properly tracked.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MA-5 | MA-5 | MA-5 |   It is the policy of the Agency the CISO:  a) Establish a process for maintenance Staff authorization and maintain a list of authorized maintenance organizations or personnel; and  b) Ensure that non-escorted Staff performing maintenance on the Resource have required access authorizations; and  c) Designate Agency Staff with required access authorizations and technical competence to supervise the maintenance activities of Staff who do not possess the required access authorizations. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |

### Media Protection Policy Family (MP)

|  |  |
| --- | --- |
| **(MP-1) Media Protection Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the media protection policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MP-1 | MP-1 | MP-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the Media protection procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MP-2) Media Protection** | | | |
| The purpose of the policy is to ensure that Data is properly handled and unauthorized disclosure is prevented.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MP-2 | MP-2 | MP-2 |   It is the policy of the Agency that all Media is protected by:     1. Restricting access to Media to only authorized individuals; and 2. Protecting Media during transport outside of controlled areas; and 3. Sanitizing Media prior to disposal or release for reuse. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |

|  |  |  |
| --- | --- | --- |
| **(MP-3) Media Marking** | | |
| The purpose of the policy is to ensure that Data is properly handled and unauthorized disclosure is prevented.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | MP-3 | MP-3 |   It is the policy of the Agency that all Media must be labeled as the most restrictive Data Classification as is stored on the Media.  a) Any Media that contains any Data classified, as Federal Tax Information must be labeled as “Federal Tax Information”.  1. The Provider must label removable Media and Resource output containing FTI (reports, documents, data files, back-up tapes) indicating “Federal Tax Information”. Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.  b) Any Media that contains no Data classified as FTI, but does have Data classified as Confidential must be labeled as “DOR Confidential;” and  c) Any Media that contains no Data classified as FTI or Confidential must be labeled as “DOR Public”. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3.* | | |
|  | a. |  |
|  | a.1 |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | a.1 |  |
|  | b. |  |
|  | c. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MP-4) Media Storage** | | | |
| The purpose of the policy is to ensure that Data is properly stored.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | MP-4 | MP-4 |   It is the policy of the Agency that all Media must be:  a) Physically controlled and securely stored; and  b) Protected until it is destroyed or sanitized using approved equipment, techniques, and procedures.  For Data classified as Federal Tax Information, see IRS Publication 1075 Revision October 2014 - Section 4.0, Secure Storage—IRC 6103(p)(4)(B), on additional secure storage requirements. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations* | |
|  | a. |  | |
|  | b. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MP-5) Media Transport** | | | |
| The purpose of the policy is to ensure that the confidentiality of Data is maintained during transport.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | MP-5(CE4) | MP-5(CE4) |   It is the policy of the Agency that:  a) All Media must be protected and controlled during transport outside of controlled areas. The NCDOR must assist and be included in with any Media transport activities related to the Resource; and  b) Accountability for the Media is maintained during transport outside of controlled areas; and  c) The Provider must document activities associated with the transport of Media:  1. For Data classified as Federal Tax Information (FTI) the Provider, assisted by the NCDOR, must use transmittal forms (transmittals) or an equivalent tracking method to ensure FTI reaches its intended destination. See IRS Publication 1075 Rev October 2014, Section 4.4, FTI in Transit, for more information on transmittals and media transport requirements.  d) The Provider restricts the activities associated with the transport of Media to authorized personnel.  Control Enhancement  CE4. The Resource must implement a cryptographic mechanism that is FIPS 140-2 compliant to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | c.1 |  | |
|  | d. |  | |
|  | CE4 | *This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | c.1 |  | |
|  | d. |  | |
|  | CE4 |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(MP-6) Media Sanitization** | | | |
| The purpose of the policy is to ensure that the confidentiality of Data is maintained through sanitization.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | MP-6 | MP-6 | MP-6(CE1) |   It is the policy of the Agency that:  a) Sanitizes all media prior to disposal, release out of organizational control, or release for reuse using IRS-approved sanitization techniques in accordance with applicable federal and organizational standards and policies; and  b) Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.  Control Enhancement  CE1.Processes should be in place to review, approve, track, document, and verify media sanitization and disposal actions. For Data classified as FTI:  a) Processes should be in place to ensure that the review and approval of media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing Staff who reviewed and approved sanitization and disposal actions, types of Media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, Staff who performed the verification, and disposal action taken; and  b) The procedures must include the verification that the sanitization of the Media was effective prior to disposal (see Information Handling and Retention (SI-12)); and  c) The use of Media on Resources that receive, store, process or transmit FTI must be restricted using physical or automated controls; and  d) Additional requirements for protecting FTI during Media sanitization are provided in IRS Publication 1075 Revision October 2014 - Exhibit 10, Data Warehouse Security Requirements and Section 9.4.7, Media Sanitization. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.* | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 | *Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.* | |
|  | CE1 a. |  | |
|  | CE1 b. |  | |
|  | CE1 c. |  | |
|  | CE1 d. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | CE1 |  | |
|  | CE1 a. |  | |
|  | CE1 b. |  | |
|  | CE1 c. |  | |
|  | CE1 d. |  | |

### Physical and Environmental Protection Control Family (PE)

|  |  |
| --- | --- |
| **(PE-1) Physical Security Environment Protection** | |
| The purpose of the policy is to ensure that proper physical and environmental controls are in place to protect Staff and Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-1 | PE-1 | PE-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the physical security environment protection procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PE-2) Physical Access Authorizations** | | | |
| The purpose of the policy is to ensure that physical access to Agency Facilities is restricted to authorized Staff.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-2 | PE-2 | PE-2 (CE1) |   The Provider must:  a) Develop, approve, and maintain a list of Staff with authorized access to the Agency facilities where Resources and Data reside.  b) Issue authorization credentials for Agency facility access.  c) Review the access list detailing authorized Agency facility access by Staff, at least annually.  d) Remove Staff from the facility access list when no longer required.  **Control Enhancement**  CE1. Enforce physical access authorizations to Resources in addition to the physical access controls for the Facility where Data is received, processed, stored, or transmitted. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | CE1 | *Related controls: AC-2, AC-3, AC-6.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | CE1 |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PE-3) Physical Access Control** | | | |
| The purpose of the policy is to ensure that physical access controls at the entry/exit points to Facilities where Agency Resources reside.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-3 | PE-3 | PE-3 |   It is the policy of the Agency to:  a) Enforce physical access authorizations at entry/exit points to Facilities by:  1. Verifying individual access authorizations before granting access to the Facility; and  2. Controlling ingress/egress to the Facility using physical access control systems/devices or guards.  b) Maintain physical access audit logs for entry/exit points; and  c) Provide security safeguards to control access to areas within the Facility officially designated as publicly accessible; and  d) Escort visitors and monitor visitor activity; and  e) Secure keys, combinations, and other physical access devices; and  f) Inventory physical access devices; and  g) Change combinations and keys when an employee who knows the combination retires, terminates employment, or transfers to another position or at least annually. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.* | |
|  | a. |  | |
|  | a.1 |  | |
|  | a.2 |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | f. |  | |
|  | g. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | a.1 |  | |
|  | a.2 |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | f. |  | |
|  | g. |  | |

|  |  |
| --- | --- |
| **(PE-4) Access Control for Transmission Medium** | |
| The purpose of the policy is to ensure that physical access to Agency Facilities is controlled.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PE-4 | PE-4 |   Is the policy of the Agency to control physical access within Facilities. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(PE-5) Access Control for Output Devices** | |
| The purpose of the policy is to ensure that physical access to Resources is controlled.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PE-5 | PE-5 |   The Agency or Provider must control physical access to Resources to prevent unauthorized disclosure. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(PE-6) Monitoring Physical Access** | | |
| The purpose of the policy is to ensure that physical access to Facilities is monitored.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-6 | PE-6 (CE1) | PE-6 (CE1) |   It is the policy of the Agency to monitor physical access to the Facility where the Resources reside in order to detect and respond to physical security incidents.  The Provider must:  a) Review physical access logs annually; and  b) Coordinate results of reviews and investigations with the agency incident response capability; and  c) Monitor physical intrusion alarms and surveillance equipment.  CE1. The organization monitors physical intrusion alarms and surveillance equipment. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE1 |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE1 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PE-8) Visitor Access Records** | | | |
| The purpose of the policy is to ensure that records of visitors are maintained and reviewed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-8 | PE-8 | PE-8 |   a. It is the policy of the Agency to maintain visitor access records to the facility where Resources reside for 5 years; and  b. Review visitor access records at least annually. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.* | |
|  | a. |  | |
|  | b. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |

|  |  |
| --- | --- |
| **(PE-9) Power Equipment and Cabling** | |
| The purpose of the policy is to determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to Agency facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PE-9 |  |   It is the policy of the Agency to protect power equipment and power cabling for the Resource from damage and destruction. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Physically separate, redundant power cables help to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PE-10) Emergency Shutoff** | | | |
| This policy applies primarily to facilities containing concentrations of Resources including, for example, in data centers or server rooms.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PE-10 |  |   It is the policy of the Agency to require Providers to:  a) Provide the capability of shutting off power to the Resource; and  b) Place emergency shutoff switches or devices in any location where Agency Resources are permanently located, to facilitate safe and easy access for personnel; and  c) Protect emergency power shutoff capability from unauthorized activation. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related control: PE-15.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |

|  |  |
| --- | --- |
| **(PE-11) Emergency Power** | |
| The purpose of the policy is sustaining operations of Resources in the event of loss of power.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PE-11 |  |   It is the policy of the Agency to ensure that Providers provide a short-term uninterruptible power supply to facilitate either an orderly shutdown of the Resource or transition of the Resources to long-term alternate power in the event of a primary power source loss. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Related controls: AT-3, CP-2, CP-7.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(PE-12) Emergency Lighting** | |
| This policy applies primarily to facilities containing concentrations of Resources including, for example, in data centers or server rooms.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-12 | PE-12 |  |   It is the policy of the Agency to employ and maintains automatic emergency lighting for the Resource that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(PE-13) Fire Protection** | | |
| The purpose of the policy is to protect Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-13 | PE-13 (CE3) |  |   It is the policy of the Agency to employ and maintain fire suppression and detection devices/systems for the Resources that are supported by an independent energy source. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | *This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.* | |
|  | CE3 |  |
| NCDORResponse | | |
|  |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PE-14) Temperature and Humidity Controls** | | | |
| The purpose of the policy is to provide stable environmental conditions conducive to the operation of the Resource.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-14 | PE-14 |  |   It is the policy of the Agency that Providers:  a. Maintain temperature and humidity levels within the facility where the Resource resides at; and  b. Monitor temperature and humidity levels; and  c. Notify NCDOR of any changes to air conditioning. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |

|  |  |
| --- | --- |
| **(PE-15) Water Damage Protection** | |
| The purpose of the policy is to protect Resources from water damage.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-15 | PE-15 |  |   It is the policy of the Agency to protect the Resource from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(PE-16) Delivery and Removal** | |
| The purpose of the policy is to ensure that Resource components entering and exiting the Facilities are controlled.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PE-16 | PE-16 | PE-16 |   It is the policy of the Agency to authorize, monitor and control Resource components entering and exiting the Facility and maintain records of those items. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  |  |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(PE-17) Alternate Work Site** | | |
| The purpose of the policy is to ensure that Data & Resources are protected at alternate work sites.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PE-17 | PE-17 |   It is the policy of the Agency to employ Office of Safeguards requirements at alternate work sites.  The Agency must:  a) Assess, as feasible, the effectiveness of security controls at alternate work sites; and  b) Security incidents or problems must be immediately reported to the IT Service Desk. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.* | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |

|  |  |
| --- | --- |
| **(PE-18) Location of Resource Components** | |
| The purpose of the policy is to ensure that Resources are physically placed as to minimize potential damage from environmental hazards.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | PE-18 |   It is the policy of the Agency to position Resources within the Facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.* |
| NCDORResponse | |
|  |  |

### Planning Control Family (PL)

|  |  |
| --- | --- |
| **(PL-1) Security Planning Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the security planning policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PL-1 | PL-1 | PL-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the security planning procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(PL-2) Resource Security Plan** | | |
| The purpose of the policy is to ensure that every resource has a security plan.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PL-2 | PL-2(CE2) | PL-2 |   It is the policy of the Agency that every Resource must have a Resource Security Plan.  Each Resource that is being implemented or undergoing a major modification, must have a Resource Security Plan, prior to being placed into general production, that:  a) Is consistent with the organization’s enterprise architecture; and  b) Explicitly defines the authorization boundary for the system and is documented with a Technical Architecture diagram; and  c) Describes the operational context of the Resource in terms of missions and business processes as documented by business process diagrams; and  d) Provides the security categorization of the Resource including supporting rationale. Categorizations are based on the most restrictive Data classification that the Resource will store, process or transmit as defined in the General Security Policies Manual; and  e) Describe the operational environment for the Resources and relationships with or connections to other information systems as documented in a Solution Architecture; and  f) Provides an explanation of the security requirements, control by control, for the Resource as approved by the Agency’s Chief Information Security Officer; and  g) Is reviewed and approved by the Agency’s Chief Information Officer prior to the Resource being placed into general production; and  h) The Resource Security Plan should be developed using the NIST Special Publication 800-18 Revision 1.  Control Enhancement  CE2. The Provider plans and coordinates security-related activities affecting the Resource with the Agency before conducting such activities in order to reduce the impact on other organizational entities. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.*  *Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
|  | CE2 |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
|  | CE2 |  |

|  |  |  |
| --- | --- | --- |
| **(PL-4) Rules of Behavior** | | |
| The purpose of the policy is to make sure Staff understands their responsibilities as it relates to Resource usage and Data security.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PL-4 | PL-4(CE1) | PL-4(CE1) |   It is the policy of the Agency that all Staff be trained on their responsibilities as it relates to the use of Data and Resources. Provider must:  a) Establish and make readily available to Staff requiring access to Resources, the rules that describe their responsibilities and expected behavior with regard to Data and Resource usage; and  b) Receive a signed acknowledgement from such Staff, indicating that they have read, understand, and agree to abide by the applicable policies, before authorizing access to Data and the Resources; and  c) Review and update the rules of behavior at least annually; and  d) Require Staff who signed a previous version of the rules of behavior to read and re-sign when the applicable policies are revised/updated.  e) Signed acknowledgement forms are provided to NCDOR upon request for audits and assessments.  Control Enhancement  CE1. Include in the applicable policies, explicit restrictions on the use of social media/networking sites and posting Agency information on public websites. The Office of Safeguards prohibits sharing FTI using any social media/networking sites. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control Implementation:** | | |
| <Provider> Response | | |
| *This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | CE1 | *This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | CE1 |  |

|  |  |  |
| --- | --- | --- |
| **(PL-8) Information Security Architecture** | | |
| The purpose of the policy is to make sure security architecture is considered for all Resources that store, process or transmit Data classified as Confidential.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | PL-8 |  |   It is the policy of that Agency to:  a) Develop, with the assistance of the Provider, an information security architecture for the information system that:  1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; and  2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and  3. Describes any information security assumptions about, and dependencies on, external services.  b) Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture; and  c) Provider ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.*  *In today’s modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization’s enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.* | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | a.3 |  |
|  | b. |  |
|  | c. |  |

### Personnel Security Policy Family

|  |  |
| --- | --- |
| **(PS-1) Personnel Security Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the personnel security policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-1 | PS-1 | PS-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the personnel security procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(PS-2) Position Risk Designation** | |
| The purpose of the policy is to ensure Staff are screened according to risk levels.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-2 | PS-2 | PS-2 |   It is the policy of the Agency that all positions are assigned a risk designation. Screening criteria must be established for each position risk designation and they are reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). Related controls: AT-3, PL-2, PS-3.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(PS-3) Personnel Screening** | |
| The purpose of the policy is to ensure Staff are screened.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PL-3 | PL-3 | PL-3 |   It is the policy of the Agency that all Staff are screened prior to authorizing access to Resources and rescreened if deemed necessary. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PS-4) Termination** | | | |
| The purpose of the policy is to ensure that the confidentiality and integrity of Data and Resources is maintained when Staff are terminated.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-4 | PS-4 | PS-4 |   It is the policy of the Agency that upon termination of Provider Staff with access to components within the boundaries of this Resource that the Provider:  a) Disable Resource access; and  b) Terminate/revoke any authenticators/credentials associated with the Staff;  c) Conduct exit interviews, as needed; and  d) Retrieve all security-related Agency Resource–related property; and  e) Retain access to Agency Data and Resources formerly controlled by the terminated Staff; and  f) Notify the NCDOR and appropriate Staff of the termination.  It is the policy of the Agency that upon termination of NCDOR Staff with physical access to components within the boundaries of this Resource that NCDOR:  a) Disable Resource access; and  b) Terminate/revoke any authenticators/credentials associated with the Staff; and  c) Conduct exit interviews, as needed; and  d) Retrieve all security-related Agency Resource–related property; and  e) Retain access to Agency Data and Resources formerly controlled by the terminated Staff; and  f) Notify the Provider and appropriate Staff of the termination. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | f. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
|  | f. |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PS-5) Personnel Transfer** | | | |
| The purpose of the policy is to ensure that the confidentiality and integrity of Data and Resources is maintained when Staff is transferred.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-5 | PS-5 | PS-5 |   It is the policy of the Agency that upon transfer of Provider Staff with access to components within the boundaries of this Resource that the Provider:  a) Review and confirm ongoing operational need for current logical and physical access authorizations to Resources/facilities when Provider Staff are reassigned or transferred to other positions within the Agency; and  b) Initiate transfer or reassignment actions following the formal transfer action; and  c) Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and  d) Notify designated Agency personnel and the NCDOR, as required.  It is the policy of the Agency that upon transfer of NCDOR Staff with physical access to components within the boundaries of this Resource that the NCDOR:  a) Review and confirm ongoing operational need for current logical and physical access authorizations to Resources/facilities when NCDOR Staff are reassigned or transferred to other positions within the Agency; and  b) Initiate transfer or reassignment actions following the formal transfer action; and  c) Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and  d) Notify designated Agency personnel and the Provider, as required. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PS-6) Access Agreements** | | | |
| The purpose of the policy is to ensure that access agreements are in place prior to Staff accessing Data classified as Federal Tax Information (FTI).   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-6 | PS-6 | PS-6 |   It is the policy of the Agency that prior to Agency or Provider’s Staff accessing Data, each must:  a) Develop and document access agreements for Agency Resources; and  b) Review and update the access agreements, at least annually; and  c) Ensure that Staff requiring access to Agency Data and Resources:  1. Sign appropriate access agreements prior to being granted access; and  2. Re-sign access agreements to maintain access to Agency Resources when access agreements have been updated or at least annually.  d) Review Resource administrator Accounts, every 3 months as required by the NC Statewide Information Security Manual - Chapter 2, section 020101. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | c.1 |  | |
|  | c.2 |  | |
|  | d. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | c.1 |  | |
|  | c.2 |  | |
|  | d. |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(PS-7) Third Party Personnel Security** | | | |
| The purpose of the policy is to ensure that all Staff, including third-party personnel, has defined security requirements.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-7 | PS-7 | PS-7 |   It is the policy of the Agency that third-party Provider Staff:  a) Have defined personnel security requirements, including security roles and responsibilities; and  b) Comply with all security policies and procedures; and  c) Notify the NCDOR of any third-party personnel new hires, transfers, or terminations who possess NCDOR credentials or badges or who have access to Resources or Data; and  d) Provider will monitor provider compliance.  It is the policy of the Agency that third-party NCDOR Staff:  a) Have defined personnel security requirements, including security roles and responsibilities; and  b) Comply with all security policies and procedures; and  c) Notify the Provider of any personnel transfers or terminations who possess Provider credentials or badges or who have access to Resources or Data; and  d) NCDOR will monitor provider compliance. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |

|  |  |
| --- | --- |
| **(PS-8) Personnel Sanctions** | |
| The purpose of the policy is to ensure that the policies regarding personnel sanctions are adhered to.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | PS-8 | PS-8 | PS-8 |   It is the policy of the Agency that all policies and procedures regarding personnel sanctions are adhered to. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.* |
| NCDORResponse | |
|  |  |

### Risk Assessment Policy Family (RA)

|  |  |
| --- | --- |
| **(RA-1) Risk Assessment Procedures** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the risk assessment policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | RA-1 | RA-1 | RA-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the risk assessment procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(RA-2) Security Categorization** | | |
| The purpose of the policy is to ensure that Data is properly handled and unauthorized disclosure is prevented.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | RA-2 | RA-2 | RA-2 |   It is the policy of the Agency that all Data may only be disclosed to appropriate individuals and only to the extent allowed by the classification. All Data must be classified and handled accordingly. A willful, unauthorized disclosure of Data will be prosecuted under all applicable statutes. If Data is comingled then the more restrictive classification shall apply.  It is the policy of the Agency to:  a) Categorize Data and the Resource in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and  b) Document the security categorization results (including supporting rationale) in the security plan for the information system; and  c) Ensures that the Agency CIO reviews and approves the security categorization decision.  Agency Staff will classify all Data as one of the following:  Federal Tax Information  Federal Taxpayer Information (FTI) is defined by Internal Revenue Service Publication 1075.   * Federal regulations require FTI be maintained separately from other Data whenever possible. If FTI is combined or commingled with other information and can no longer be identified specifically as FTI, then the commingled information must all be treated as FTI. * Any Staff disclosing FTI must ensure that it is authorized under IRC, Section 6103. * Only approved Resources may be used to process or store FTI. * No FTI shall be transmitted to a non-Agency email address using non-Agency IT approved methods without prior approval of the CISO.   Confidential Information  Confidential Information is non-FTI Data that is exempted from public records requests defined by NC G.S. 132-1. Confidential Information includes, but is not limited to:   * Information that pertains to the security of our information systems as defined in G.S. 132-6.1(c). * Information that pertains to the physical security of our public buildings such as detailed plans of public buildings and infrastructure facilities as defined in G.S. 132-1.7. * State Taxpayer Information (STI) as defined by G.S. 105-259(B). * Payment Card Industry (PCI) Data Security Standard data. * Personally Identifiable Information (PII) as defined in G.S. 75-61, G.S. 75-66, G.S. 132-1.10, G.S. 14-113.20. * National Automated Clearing House Association (NACHA).   Public Information   * All electronic information that is not classified as FTI or Confidential Information is considered Public Information as defined by the North Carolina General Statute G.S. 132-1 and is subject to public records requests. * l) All public records requests must be submitted to the Public Information Officer (PIO). The PIO will coordinate the Agency response to public records requests. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* *Note: The information in the <PROVIDER> Resource has been classified as “<classification.”* | | |
| <Provider> Response | | |
| *Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(RA-3) Risk Assessment** | | | |
| The purpose of the policy is to establish the procedure requirements for risk assessment.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | RA-2 | RA-2 | RA-2 |   It is the policy of the Agency that for every Resource, prior to implementation, the Chief Information Security Office (CISO) must perform an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the Resource and the Data it stores, processes or transmits.  The Provider’s CISO must:  a) Document risk assessment results in a risk assessment report; and  b) Review risk assessment results at least annually; and  c) Disseminate risk assessment results to the NCDOR, Resource owner, Chief Information Officer and the Chief Technology Officer; and  d) Update the risk assessment report at least every three years or whenever there are significant changes to the Resource or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the Resource.  e) The risk assessment should take into account NIST SP 800-37 rev 1 - Guide for Applying the Risk Management Framework to Federal Information Systems.  The Agency’s CISO must:  a) Document risk assessment results in a risk assessment report; and  b) Review risk assessment results at a minimum of every 18 months; and  c) Disseminate risk assessment results to the Chief Information Officer and the Chief Information Officer; and  d) Update the risk assessment report at least every three years or whenever there are significant changes to the Resource or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the Resource.  e) The risk assessment should take into account NIST SP 800-37 rev 1 - Guide for Applying the Risk Management Framework to Federal Information Systems. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.*  *Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |  |
| --- | --- | --- |
| **(RA-5) Vulnerability Scanning** | | |
| The purpose of the policy is to ensure that Resources are protected from vulnerabilities.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | RA-5 | RA-5 (CE1) (CE2) (CE5) | RA-5 (CE1) |   It is the policy of the Agency that all Resources are protected from vulnerabilities.  The Provider must:  a) Scan for vulnerabilities in the Resource and hosted applications at a minimum of monthly for all Resources and when new vulnerabilities potentially affecting the Resources are identified and reported; and  b) Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:  1. Enumerating platforms, software flaws, and improper configurations; and  2. Formatting checklists and test procedures; and  3. Measuring vulnerability impact.  c) Analyze vulnerability scan reports and results from security control assessments; and  d) Remediate legitimate vulnerabilities in accordance with an assessment of risk; and  e) Share information obtained from the vulnerability scanning process and security control assessments with designated Agency officials to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).  Control Enhancements  CE1. Employ vulnerability scanning tools that include the capability to readily update the Resource vulnerabilities to be scanned.  CE2. The Provider updates the Resource vulnerabilities scanned weekly.  CE5. The Resource implements privileged access authorization to IT Security Staff or to a specified system account for vulnerability scanning activities. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.* | | |
|  | a. |  |
|  | b. |  |
|  | b.1 |  |
|  | b.2 |  |
|  | b.3 |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | CE1 | *The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.* |
|  | CE2 | *Related controls: SI-3, SI-5.* |
|  | CE5 | *In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | b.1 |  |
|  | b.2 |  |
|  | b.3 |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | CE1 |  |
|  | CE2 |  |
|  | CE5 |  |

### Resource and Services Acquisition Policy Family (SA)

|  |  |
| --- | --- |
| **(SA-1) Resource and Service Acquisition** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the system and service acquisition policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-1 | SA-1 | SA-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the system and service acquisition procedures must be documented, disseminated and reviewed at least annually | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| **(SA-2) Allocation of Resources** | |
| The purpose of the policy is to ensure that information security is planned for the life of the Resource.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-2 | SA-2 | SA-2 |   It is the policy of the Agency that all Resources have sufficient funding to ensure the confidentiality and integrity of Data and Resources commensurate with their defined risk level. The Chief Information Security Officer (CISO) must:  a) Determine information security requirements for the Resource or service in mission/business process planning; and  b) Determine, document, and allocate the resources required to protect the Resource or service as part of the budget planning and investment control process; and  c) Establish a discrete line item for information security in Agency programming and budgeting documentation. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* *The <PROVIDER> bills the NCDOR for services.* | |
| a. | The NCDOR and <PROVIDER> have determined the information security requirements for this resource; and |
| b. | As a part of budgeting and investment control process both the NCDOR and <PROVIDER> have determined, documented, and allocated the resources required to protect the resource; and |
| c. | NCDOR has a discrete line item for information security in 1605-5005. |

|  |  |  |
| --- | --- | --- |
| **(SA-3) System Development Lifecycle** | | |
| The purpose of the policy is to ensure that security is considered during the development and maintenance of Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-3 | SA-3 | SA-3 |   It is the policy of the Agency to manage Resources using a System Development Life Cycle (SDLC) that incorporates information security considerations.  a) Define and document information security roles and responsibilities throughout the SDLC; and  b) Identify Staff having information security roles and responsibilities; and  c) Integrate the Provider information security risk management process into SDLC activities. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |  |
| --- | --- | --- |
| **(SA-4) Acquisition Process** | | |
| The purpose of the policy is to ensure that security requirements are included in any acquisition of a Resource or service.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-4 (CE10) | SA-4 (CE1)(CE2)(CE9)(CE10) | SA-4 (CE1) |   It is the policy of the Agency that the following requirements, descriptions, and criteria, explicitly or by reference, is included in the acquisition contract for the Resource, component, or service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:  a) Security functional requirements; and  b) Security strength requirements; and  c) Security assurance requirements; and  d) Security-related documentation requirements; and  e) Requirements for protecting security-related documentation; and  f) Description of the Resource development environment and environment in which it is intended to operate; and  g) Acceptance criteria.  Control Enhancements  CE1. The Agency requires the developer of the Resource, component, or service to provide a description of the functional properties of the security controls to be employed.  CE2. The Agency requires the developer of the Resource, component, or service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces, high-level design at sufficient detail to satisfy the Service Design process and as approved by the Service Design lifecycle manager.  CE9. The Agency requires the developer of the Resource, component, or service to identify early in the Service Design lifecycle, the functions, ports, protocols, and services intended for organizational use.  CE10. The Agency employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| **<Provider> Response** | | |
| *Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.*  *Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE1 | *Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.* |
|  | CE2 | *Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.* |
|  | CE9 | *The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.* |
|  | CE10 | *Related controls: IA-2, IA-8.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE1 |  |
|  | CE2 |  |
|  | CE9 |  |
|  | CE10 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(SA-5) Resource Documentation** | | | |
| The purpose of the policy is to ensure that adequate system documentation is obtained for all Resources procured by the Agency.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-5 | SA-5 | SA-5 |   It is the policy of the Agency that for all Resources and/or services being procured the Agency must:  a) Obtain administrator documentation for the Resource, component, or service that describes:  1. Secure configuration, installation, and operation of the system, component, or service; and  2. Effective use and maintenance of security functions/mechanisms; and  3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.  b) Obtain Staff (i.e. user) documentation for the Resource, component, or service that describes:  1. Staff-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; and  2. Methods for Staff interaction, which enable Staff to use the Resource, component, or service in a more secure manner; and  3. Staff responsibilities in maintaining the security of the Resource, component, or service.  c) Document attempts to obtain Resource, component, or service documentation when such documentation is either unavailable or nonexistent; and  d) Protect documentation, as required; and  e) Distribute documentation to designated Agency officials. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.* | |
|  | a. |  | |
|  | a.1 |  | |
|  | a.2 |  | |
|  | a.3 |  | |
|  | b. |  | |
|  | b.1 |  | |
|  | b.2 |  | |
|  | b.3 |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | a.1 |  | |
|  | a.2 |  | |
|  | a.3 |  | |
|  | b. |  | |
|  | b.1 |  | |
|  | b.2 |  | |
|  | b.3 |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |
| --- | --- |
| **(SA-8) Security Engineering Principals** | |
| The purpose of the policy is to ensure that security is properly considered in the specification, design, development, implementation, and modification of Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-8 | SA-8 | SA-8 |   It is the policy of the Agency to apply Resource security engineering principles in the specification, design, development, implementation, and modification of the Resource. Specifically NIST Publication 800-27 Revision A - Engineering Principles for IT Security should be considered where appropriate.  Security engineering principles include, for example:  (i) developing layered protections  (ii) establishing sound security policy, architecture, and controls as the foundation for design  (iii) incorporating security requirements into the system development lifecycle  (iv) delineating physical and logical security boundaries  (v) ensuring that system developers are trained on how to build secure software  (vi) tailoring security controls to meet organizational and operational needs  (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack  patterns as well as compensating controls and design patterns needed to mitigate risk  (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| **(SA-9) External Information System Services** | | |
| The purpose of the policy is to ensure that security is properly considered when outsourcing services.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SA-9 | SA-9(CE2) | SA-9(CE5) |   It is the policy of the Agency that providers of external services comply with Agency information security requirements and employ to include (at a minimum) security requirements contained within applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements.  The Agency:  a. Requires that providers of external information system services comply with organizational information security requirements and employ controls are defined in the DOR Security Policy Manual based on Agency determined data classification, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;  b. Defines and documents Agency oversight and user roles and responsibilities with regard to external information system services; and  c. Employs and employ Agency approved processes, methods, and techniques based on Agency determined data classification to monitor security control compliance by external service providers on an ongoing basis.  Control Enhancement  CE2: The Agency requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.  CE5: The Agency restricts the location of Resources that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE2 | *Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.* |
|  | CE5 | *The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE2 |  |
|  | CE5 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **(SA-10) Developer Configuration Management** | | | |
| The purpose of the policy is to ensure that security is considered during the development, implementation or operation of a Resource, component, or service.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SA-10 | SA-10 |   It is the policy of the Agency that any developer of a Resource, component, or service must:  a) Perform configuration management during Resource, component, or service development, implementation, and operation; and  b) Document, manage, and control the integrity of changes to the Resource, component, or service; and  c) Implement only Agency-approved changes to the Resource, component, or service; and  d) Document approved changes to the Resource, component, or service and the potential security impacts of such changes; and  e) Track security flaws and flaw resolution within the Resource, component, or service and report findings to NCDOR IT Security. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **(SA-11) Developer Security Testing and Evaluation** | | | |
| The purpose of the policy is to ensure that all developers of Agency Resources plan for security testing and evaluation.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SA-11 | SA-11 |   It is the policy of the Agency that any developer of a Resource, component, or service must:    a) Submit the security plan for review so that NCDOR can create and implement a security assessment plan; and  b) Give NCDOR access to perform security testing/evaluation; and  c) Review evidence of the execution of the security assessment plan and the results of the security testing/evaluation; and  d) Implement a verifiable flaw remediation process; and  e) Correct flaws identified during security testing/evaluation. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |
| --- | --- |
| **(SA-22) Unsupported Resource Components** | |
| The purpose of the policy is to ensure that the Agency has continued support for Resources, components and services.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | SA-22 |   It is the policy of the Agency that the Provider replace Provider-owned Resource components when support for the components is no longer available from the developer, Provider, or manufacturer. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Related controls: PL-2, SA-3.* |
| NCDORResponse | |
|  |  |

### Resource and Communications Protection Policy Family (SC)

|  |  |
| --- | --- |
| ***(SC-1) Application Partitioning*** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the Resource and communication protection policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-1 | SC-1 | SC-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the Resource and communication protection procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-2) Application Partitioning*** | |
| The purpose of the policy is to make sure that privileged accounts are not being used for work that can be done with a less privileged account.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-2 | SC-2 | SC-2 |   It is the policy of the Agency that all Resources must separate Staff functionality (including Staff interface services) from Resources management functionality. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separa****t****e authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-4) Data in Shared Resources*** | |
| The purpose of the policy is to ensure that residual Data is protected even when objects are reused.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-4 | SC-4 |   It is the policy of the Agency that all Resources must prevent unauthorized and unintended transfer of Data via shared system resources. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-5) Denial of Service Protection*** | |
| The purpose of the policy is to ensure that Resources are protected from a Denial of Service attack.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-5 | SC-5 | SC-5 |   It is the policy of the Agency that the Resource must protect against or limit the effects of denial of service attacks. Refer to NIST SP 800-61 R2 - Computer Security Incident Handling Guide, for additional information on denial of service. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| ***(SC-7) Network Boundary Protection*** | | |
| The purpose of the policy is to ensure managed interfaces for boundary protection of Resources are employed, monitored, audited and controlled.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-5 | SC-5 (CE3)(CE4)(CE5)(CE7) | SC-5 (CE3)(CE4)(CE5)(CE7) |   It is the policy of the Agency that managed interfaces for boundary protection of Resources are employed, monitored, audited and controlled at connection points to external networks using security devices (e.g. firewalls, routers, encrypted tunnels) in accordance with Agency enterprise architecture.  The Resource must:   1. Monitor and control communications at the external boundary of the Resource and at key internal boundaries within the Resource; and 2. Implement sub-networks for publicly accessible Resource components that are physically and logically separated from internal Agency networks; and 3. Connect to external networks or Resource only through managed interfaces consisting of boundary protection devices arranged in accordance with Agency security architecture requirements. Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected sub-networks).   Control Enhancements  CE3. The Provider must limit the number of external network connections to the Resource.  CE4. The Provider must:   1. Implement a secure managed interface for each external telecommunication service; and 2. Establish a traffic flow policy for each managed interface; and 3. Protect the confidentiality and integrity of the Data being transmitted across each interface; and 4. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need, and accept the associated risk; and 5. Review exceptions to the traffic flow policy at a minimum annually, and remove exceptions that are no longer supported by an explicit mission/business need.   CE5. The Resource at managed interfaces must deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).  CE7. The Resource must, in conjunction with a remote device, prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e. bridging).  Additional requirements for protecting FTI on networks are provided in IRS Publication 1075 Revision October 2014 - Section 9.4.10 - Network Protections. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE3 | *Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.* |
|  | CE4 | *Related control: SC-8.* |
|  | CE4 a. |  |
|  | CE4 b. |  |
|  | CE4 c. |  |
|  | CE4 d. |  |
|  | CE4 e. |  |
|  | CE5 | *This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.* |
|  | CE7 | *This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | CE3 |  |
|  | CE4 a. |  |
|  | CE4 b. |  |
|  | CE4 c. |  |
|  | CE4 d. |  |
|  | CE4 e. |  |
|  | CE5 |  |
|  | CE7 |  |

|  |  |  |
| --- | --- | --- |
| ***(SC-8) Transmission Confidentiality and Integrity*** | | |
| The purpose of the policy is to establish the proper transmission of Data to ensure the integrity and confidentiality of the Data.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-8(CE1) | SC-8(CE1) |   It is the policy of the Agency that the Resource protects the confidentiality and integrity of transmitted information commiserate with the Data classification in (RA-2)  Control Enhancement  CE1. The Resource implements cryptographic mechanisms to prevent unauthorized disclosure of information during transmission using FIPS 140-2 compliant cryptographic mechanisms.  a) If encryption is infeasible or impractical, the CISO may approve mitigating safeguards such as implementing vLANs to segregate network traffic or the use of physical security safeguards; and  b) The Provider must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized Provider Staff; and  c) Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.* | | |
|  | CE1 | *Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.* |
|  | CE1 a. |  |
|  | CE1 b. |  |
|  | CE1 c. |  |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE1 a. |  |
|  | CE1 b. |  |
|  | CE1 c. |  |

|  |  |
| --- | --- |
| ***(SC-10) Network Disconnect*** | |
| The purpose of the policy is to ensure the integrity and confidentiality of Data by terminating connections that are not being actively used.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-10 | SC-10 |   It is the policy of the Agency that all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information must terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-12) Cryptographic Key Management*** | |
| The purpose of the policy is to ensure that cryptographic keys are properly managed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-12 | SC-12 | SC-12 |   It is the policy of the Agency to establish and manage cryptographic keys for required cryptography employed within the Resource. Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-13) Cryptographic Protection*** | |
| The purpose of the policy is to ensure that cryptographic keys are properly managed.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-13 | SC-13 | SC-13 |   It is the policy of the Agency that all Resources using cryptographic modules must implement them in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-15) Collaborative Computing Resources*** | |
| The purpose of the policy is to establish the appropriate use of collaborative computing devices   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SC-15 | SC-15 | SC-15 |   It is the policy of the Agency that the Resource must prohibit remote activation of collaborative computing devices and the Resource must provide an explicit indication of its use to Staff physically present at the devices. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-17) Public Key Infrastructure Certificates*** | |
| The purpose of the policy is to ensure that certificates are supplied by a reputable source.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-17 | SC-17 |   It is the policy of the Agency to issue public key infrastructure certificates or obtain public key infrastructure certificates from an approved service provider. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SC-18) Mobile Code*** | |
| The purpose of the policy is to define the use of mobile code technologies.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-18 | SC-18 |   It is the policy of the Agency that the use of mobile code technology is permitted with the exception of some internet client usage. Mobile code technologies that exhibit functionality allowing unmediated access to host and remote system services, Resources and Data will be blocked or disabled via web proxy with content filtering for Internet browsing sessions. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| ***(SC-19) Voice over Internet Protocol*** | | |
| The purpose of the policy is to make sure that Data integrity and confidentiality is maintained when transmitting voice over the network.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-19 | SC-19 |   It is the policy of the Agency to establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and authorizes, monitors, and controls the use of VoIP within the Resource.  In order to use a VoIP network that provides information classified as FTI or Confidential to a customer, the following requirements must be met:   1. VoIP traffic should be segmented off from non-VoIP traffic through segmentation. If complete segmentation is not feasible, the Provider must have compensating controls in place and properly applied that restrict access to VoIP traffic; and 2. When Data is in transit across the network (either Internet or Agency’s network), the VoIP traffic must be encrypted using a cryptographic module that is FIPS 140-2 compliant; and 3. Each Resource within the Agency’s network that transmits Data to an external customer through the VoIP network should be subject to frequent vulnerability testing; and 4. VoIP-ready firewalls must be used to filter VoIP traffic on the network; and 5. Security testing must be conducted on the VoIP system prior to implementation and annually thereafter; and 6. VoIP phones must be logically protected, and agencies must be able to track and audit all applicable conversations and access; and 7. VoIP network Resources (e.g. servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security (See IRS Publication 1075 IRC 6103(p)(4)(B) Section 4.2 – Minimum Protection Standards). | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Related controls: CM-6, SC-7, SC-15.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |

|  |  |
| --- | --- |
| ***(SC-23) Session Authenticity*** | |
| The purpose of the policy is to ensure that communications sessions are valid.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-23 | SC-23 |   It is the policy of the Agency that Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information must protect the authenticity of communications sessions. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.* |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| ***(SC-28) Data at Rest*** | | |
| The purpose of the policy is to ensure that Data classified as Confidential or Federal Tax Information (FTI) is properly handled so that the confidentiality and integrity is maintained and unauthorized disclosure is prevented. Data at rest could be located on storage devices as specific components of Resources.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SC-23 | SC-23 |   It is the policy of the Agency that all Resources must protect the confidentiality and integrity of Data classified as Confidential or as Federal Tax Information at rest.  a) The Provider may employ different mechanisms to achieve confidentiality and integrity protections, including encryption using a cryptographic module that is FIPS 140-2 compliant, file share scanning, and integrity protection. The Provider may also employ other security controls, including for example, secure offline storage in lieu of online storage, when adequate protection of Data at rest cannot otherwise be achieved or when continuously monitoring to identify malicious code at rest; and  b) The confidentiality and integrity of Data at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms that are FIPS 140-2 compliant; and  c) Data stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology; and  d) Mobile devices do require encryption at rest (see AC-19). | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.* | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |

### Resource and Data Integrity Policy Family (SI)

|  |  |
| --- | --- |
| ***(SI-1) Resource and Data Integrity Procedures*** | |
| The purpose of the policy is to establish the procedure requirements for the effective implementation of the Resource and Data integrity policy family.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SI-1 | SI-1 | SI-1 |   It is the policy of the Agency that procedures to facilitate the implementation of the Resource and Data integrity procedures must be documented, disseminated and reviewed at least annually. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ***(SI-2) Flaw Remediation*** | | | |
| The purpose of the policy is to ensure that Resources are patched to ensure the confidentiality and integrity of Data.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SI-2 | SI-2(CE2) | SI-2(CE1) |   It is the policy of the Agency that Provider, for owned Components:  a) Identifies, reports to NCDOR, and corrects Component flaws; and  b) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; and  c) Installs security-relevant software and firmware updates based on severity and associated risk to the confidentiality of Data; and  d) Incorporates flaw remediation into the Provider’s configuration management process.  Control Enhancement  CE1. Centrally manage the flaw remediation process.  CE2. The Provider employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | CE1 | *Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.* | |
|  | CE2 | *Related controls: CM-6, SI-4.* | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | CE1 |  | |
|  | CE2 |  | |

|  |  |  |
| --- | --- | --- |
| ***(SI-3) Malicious Code Protection*** | | |
| The purpose of the policy is to ensure Resources are protected against malicious code.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SI-3 | SI-3 (CE1) (CE2) | SI-3 (CE1) (CE2) |   It is the policy of the Agency that malicious code protection mechanisms are employed at Resource entry and exit points to detect and eradicate malicious code.  a) Malicious code protection mechanisms must be updated whenever new releases are available in accordance with Agency configuration management policy and procedures; and  b) Malicious code protection mechanisms must be configured to:  1. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with Agency security policy; and  2. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection.  c) False positives must be addressed during malicious code detection and eradication and the resulting potential impact on the availability of the Resource.  Control Enhancements  CE1. Malicious code protection mechanisms must be centrally managed by IT Security.  CE2. The Resource must automatically update malicious code protection mechanisms. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.* | | |
|  | a. |  |
|  | b. |  |
|  | b.1 |  |
|  | b.2 |  |
|  | c. |  |
|  | CE1 | *Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.* |
|  | CE2 | *Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | b. |  |
|  | b.1 |  |
|  | b.2 |  |
|  | c. |  |
|  | CE1 |  |
|  | CE2 |  |

|  |  |  |
| --- | --- | --- |
| ***(SI-4) Resource Monitoring*** | | |
| The purpose of the policy is to ensure that Resources are constantly monitored for malicious activity.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SI-4 | SI-4 (CE2)(CE4)(CE5) | SI-4 (CE4)(CE5)(CE7) (CE11)(CE23) |   It is the policy of the Agency that Agency and Provider monitor all Resources.  Each will:  a) Monitor all Resources to detect:  1. Attacks and indicators of potential attacks; and  2. Unauthorized local, network, and remote connections.  b) Identify unauthorized use of Resources; and  c) Deploy monitoring devices:  1. Strategically within the Resources to collect essential information; and  2. At ad hoc locations within the Resource to track specific types of transactions of interest to the Agency.  d) Protect Data obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; and  e) Heighten the level of Resource monitoring activity whenever there is an indication of increased risk to Agency operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information; and  f) Provide Resource monitoring information to the CISO as needed; and  g) Analyze outbound communications traffic at the external boundary of the Resource and selected interior points within the network (e.g., sub-networks, subsystems) to discover anomalies—anomalies within Agency Resources include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.  Control Enhancements  CE2. The Provider employs automated tools to support near real-time analysis of events.  CE4. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. This is also a requirement for PCI data in PCI DSS 3.0 section 10.6.1, which calls for at least daily IDS/IPS monitoring of security events and system logs.  CE5. Alert designated Provider Staff and the NCDOR Service Desk when indications of compromise or potential compromise occur—alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms intrusion detection or prevention mechanisms; or boundary protection Resources, such as firewalls, gateways, and routers and alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Agency Staff on the notification list can include, for example, system administrators, mission/business owners, system owners, or Resource security officers.  CE7. Notify designated Provider officials and the NCDOR Service Desk of detected suspicious events and take necessary actions to address suspicious events.  CE11. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications.  CE23. Implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on Resources. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.* | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | b. |  |
|  | c.1 |  |
|  | c.2 |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE2 | *Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.* |
|  | CE4 | *Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.* |
|  | CE5 | *Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.* |
|  | CE7 | *Least-disruptive actions may include, for example, initiating requests for human responses.* |
|  | CE11 | *Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.* |
|  | CE23 | *Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers.* |
| NCDORResponse | | |
|  | | |
|  | a. |  |
|  | a.1 |  |
|  | a.2 |  |
|  | b. |  |
|  | c.1 |  |
|  | c.2 |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | CE2 |  |
|  | CE4 |  |
|  | CE5 |  |
|  | CE7 |  |
|  | CE11 |  |
|  | CE23 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ***(SI-5) Security Alerts, Advisories and Directives*** | | | |
| The purpose of the policy is to ensure that the Agency is receiving security alerts.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SI-5 | SI-5 | SI-5 |   It is the policy of the Agency that Providers:  a) Receive security alerts, advisories, and directives from designated external organizations on an ongoing basis; and  b) Generate internal security alerts, advisories, and directives as deemed necessary; and  c) Disseminate security alerts, advisories, and directives to designated Provider officials; and  d) Implement security directives in accordance with established time frames or notifies the issuing Agency of the degree of noncompliance. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.* | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |
|  | c. |  | |
|  | d. |  | |
|  | e. |  | |

|  |  |  |
| --- | --- | --- |
| ***(SI-7) Software, Firmware and Information Integrity*** | | |
| The purpose of the policy is to prevent unauthorized changes to software, firmware, and Data due to errors or malicious activity. Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Data includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SI-7 (CE1)(CE7) |  |   It is the policy of the Agency to employ integrity verification tools to detect unauthorized changes to software, firmware and Data.  Control Enhancements  CE1. The Resource performs an integrity check of software, firmware and Data at startup.  CE7. The Provider incorporates the detection of unauthorized changes to the Resource into the organizational incident response capability. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.* | | |
|  | CE1 | *Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.* |
|  | CE7 | *This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.* |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE7 |  |

|  |  |  |
| --- | --- | --- |
| ***(SI-8) Spam Protection*** | | |
| The purpose of the policy is to prevent spam.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SI-8 (CE1)(CE2) | SI-8 |   It is the policy of the Agency that IT Security employ spam protection mechanisms at Resource entry and exit points to detect and take action on unsolicited messages. In addition, they should update spam protection mechanisms when new releases are available in accordance with Agency configuration management policy and procedures.    CE1. The Provider centrally manages spam protection mechanisms.    CE2. The resource automatically updates spam protection mechanisms. | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
| *Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.* | | |
|  | CE1 | *Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.* |
|  | CE2 |  |
| NCDORResponse | | |
|  | | |
|  | CE1 |  |
|  | CE2 |  |

|  |  |
| --- | --- |
| ***(SI-10) Data Input Validation*** | |
| The purpose of the policy is to ensure that all Resources have some form of quality control around Data inputs and to prevent unauthorized or inappropriate input.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SI-10 | SI-10 |   It is the policy of the Agency that all Resources must check the validity of Data inputs. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.* |
| NCDORResponse | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ***(SI-11) Error Handling*** | | | |
| The purpose of the policy is to make sure that all Resources can generate error notices.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SI-11 | SI-11 |   It is the policy of the Agency that all Resources must:  a) Generate error messages that provide Data necessary for corrective actions without revealing Data that could be exploited by adversaries; and  b) Reveal error messages only to designated Provider or Agency officials. | | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | | |
| **Control implementation***:* | | | |
| <Provider> Response | | | |
|  | *Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.* | |
|  | a. |  | |
|  | b. |  | |
| NCDORResponse | | | |
|  | a. |  | |
|  | b. |  | |

|  |  |
| --- | --- |
| ***(SI-12) Data Handling and Retention*** | |
| The purpose of the policy is to ensure that Staff properly handles Data.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | | SI-12 | SI-12 | SI-12 |   It is the policy of the Agency that Staff must handle and retain Data within the Resource and Data output from the Resource in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.* |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***(SI-16) Memory Protection*** | |
| The purpose of the policy is to ensure that all Resources protect their memory.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  | SI-16 | SI-16 | | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.* |
| NCDORResponse | |
|  |  |

### Program Management Policy Family (PM)

|  |  |
| --- | --- |
| ***(PM-2) Senior Information Security Officer*** | |
| The purpose of the policy is to establish the Chief Information Security Officer.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | PM-2 |   It is the policy of the Agency that the Provider appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an Agency-wide information security program. | |
| **Security Control Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  | *The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.* |
| NCDORResponse | |
|  |  |

### Data Warehouse Security Policies – FTI Only

|  |  |  |
| --- | --- | --- |
| ***Data Warehousing Implications*** | | |
| The purpose of the policy is to clarify the understanding of expectations related to warehousing FTI data.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   It is the policy of the Agency that all FTI data placed in a warehouse environment:  a) May only be used for “tax administration purposes” or for other authorized purposes defined with the IRS publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies.  b) Must retain its identity as FTI to the data element level (i.e., it must be obvious that the IRS is the source of the data).  c) Whenever calculations or data manipulations are performed that could comingle FTI with any other data, the access to FTI must be restricted to Agency Staff with a need-to-know and their contractors or agents authorized by law. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| **<Provider> Response** | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |  |
| --- | --- | --- |
| ***Management Controls – Risk Assessment*** | | |
| The purpose of the policy is to define specific and unique controls related to data warehousing risk assessments.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   The Agency shall:  a) Have a risk management program in place to ensure that each aspect of the data warehouse is assessed for risk; and  b) Any risk documents shall identify and document all vulnerabilities associated with the data warehousing environment. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |

|  |  |  |
| --- | --- | --- |
| ***Management Controls – Planning*** | | |
| The purpose of the policy is to define specific and unique controls related to data warehousing planning.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) A security plan shall be in place to address organizational policies, security testing, rules of behavior, contingency plans, architecture and network diagrams, and requirements for security reviews. Although such a security plan will provide planning guidelines, it does not replace requirements documents, which contain specific details and procedures for security operations.  b) Policies and procedures are required to define how activities and day-to-day procedures will occur. They contain the specific policies, relevant to all of the security disciplines covered in this document. Because they relate to data warehousing, any data warehousing documents can be integrated into overall security procedures. A section shall be dedicated to the data warehouses to define the controls specific to that environment.  c) The agency must develop policies and procedures to document all existing business processes. The agency must ensure that roles are identified for the organization and develop responsibilities for the roles.  d) Within the security planning and policies, the purpose or function of the warehouse shall be defined. The business process shall include a detailed definition of configurations and the functions of the hardware and software involved. In general, the planning shall define any unique issues related to data warehousing.  e) The agency must define how “legacy system data” will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the ETL transformation process.  f) The policy shall ensure that FTI will not be subject to public disclosure. Only authorized users with a demonstrated need-to-know can query FTI data within the data warehouse. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |

|  |  |  |
| --- | --- | --- |
| ***Management Controls – System and Services Acquisition*** | | |
| The purpose of the policy is to define the specific and unique requirements related to data warehousing system and services acquisition.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   Because FTI is used within data warehousing environments, it is important that the services and acquisitions have adequate security in place, including the capacity to block information to contractors in cases in which they are not authorized to access FTI. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
| NCDORResponse | | |
|  | a. |  |

|  |  |
| --- | --- |
| ***Management Controls – Certification, Accreditation, and Security Assessments*** | |
| The purpose of the policy is to define specific and unique requirements related to data warehousing certification, accreditation, and security assessments.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   State and local agencies shall develop a process or policy to ensure that data warehousing security meets the baseline security requirements defined in the current revision of NIST SP 800-53. The process or policy must contain the methodology used by the state or local agency to inform management, define accountability, and address known security vulnerabilities. Risk assessments must follow the guidelines provided in NIST Publication 800-30, Risk Management Guide for Information Technology Systems. | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  |  |
| NCDORResponse | |
|  |  |

|  |  |
| --- | --- |
| ***Operational Controls – Personnel Security*** | |
| The purpose of the policy is to define the specific and unique requirements related to data warehousing personnel security.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   Agency should comply with IRS publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies - Section 5.1.1 Background Investigation Minimum Requirements. | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  |  |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| ***Operational Controls – Contingency Planning*** | | |
| The purpose of the policy is to define specific and unique requirements related to data warehousing contingency planning.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) Online data resources shall be provided adequate tools for the backup, storage, restoration, and validation of data. Agencies will ensure that the data provided is reliable.  b) Both incremental and special purpose data backup procedures are required, combined with off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy and are tested and verified. The agency’s contingency plan must be evaluated to ensure that all data resources are synchronized and restored to allow re-creation of the data to take place. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |

|  |  |  |
| --- | --- | --- |
| ***Operational Controls – Configuration Management*** | | |
| The purpose of the policy is to define specific and unique requirements related to data warehousing configuration management.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   The agency shall have a process and documentation to identify and analyze how FTI is used and how FTI is queried or targeted by end users.  a) Parts of the system containing FTI shall be mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server; and  b) During the life cycle of the data warehouse, online and architectural adjustments and changes will occur. The agency shall document these changes and ensure that FTI always is secured from unauthorized access or disclosure. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |

|  |  |
| --- | --- |
| ***Operational Controls – Media Protection*** | |
| The purpose of the policy is to define specific and unique requirements related to data warehousing media protection.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   The agency shall have policy and procedures in place that describe the cleansing process at the staging area and how the ETL process cleanses the FTI when it is extracted, transformed, and loaded. In addition, the agency shall describe the process of object reuse once FTI is replaced from data sets. IRS requires that all FTI be removed by a random overwrite software program. | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | |
| **Control implementation***:* | |
| <Provider> Response | |
|  |  |
| NCDORResponse | |
|  |  |

|  |  |  |
| --- | --- | --- |
| ***Operational Controls – Incident Response*** | | |
| The purpose of the policy is to define specific and unique requirements related to data warehousing incident response.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) Parts of Intrusion-detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data; and  b) The agency’s incident reporting policy and procedures must cover the data warehousing environment. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |

|  |  |  |
| --- | --- | --- |
| ***Operational Controls – Awareness and Training*** | | |
| The purpose of the control is to define specific and unique controls related to data warehousing awareness and training.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) The agency shall have a disclosure awareness training program in place that includes how FTI security requirements are communicated to end users; and  b) Training shall be user- specific to ensure that all personnel receive appropriate training for a particular job, such as training required for administrators or auditors. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |

|  |  |  |
| --- | --- | --- |
| ***Technical Controls – Identification and Authentication*** | | |
| The purpose of the control is to define specific and unique controls related to data warehousing identification and authentication.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) The agency shall configure the Web services to be authenticated before access is granted to users via an authentication server. The Web portal and two-factor authentication requirements in Section 9.0 of IRS Publication 1075 – *Tax Information Security Guidelines For Federal, State, and Local Agencies* apply in a data warehouse environment; and  b) Business roles and rules shall be imbedded at either the authentication level or application level. In either case, roles must be in place to ensure that only authorized personnel have access to FTI information; and  c) Authentication shall be required both at the operating system level and at the application level, whenever the data warehousing environment is accessed. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |  |
| --- | --- | --- |
| ***Technical Controls – Access Control*** | | |
| The purpose of the control is to define specific and unique controls related to data warehousing access control.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) Access to systems shall be granted based upon the need to perform job functions. Agencies shall identify which application programs use FTI and how access to FTI is controlled. The access control to application programs relates to how file shares and directories apply file permissions to ensure that only authorized personnel have access to the areas that contain FTI; and  b) The agency shall have security controls in place that include preventive measures to keep an attack from being a success. These security controls shall also include detective measures in place to let the IT staff know that an attack is occurring. If an interruption of service occurs, the agency shall have additional security controls in place that include recovery measures to restore operations; and  c) Within the data warehouse, the agency shall protect FTI as sensitive data and be granted access to FTI for the aspects of its job responsibilities;  d) The agency shall enforce effective access controls so that end users have access to programs with the least privilege needed to complete the job; and  e) The agency shall set up access controls in its data warehouse based on personnel clearances; and  f) Access controls in a data warehouse are classified in general as follows:  1. General users  2. Limited access users  3. Unlimited access users; and  g) FTI shall always fall into the limited access users category; and  h) All FTI shall have an owner assigned to provide responsibility and accountability for its protection. Typically, this role is assigned to a management official such as an accrediting authority; and  i) The agency shall configure control files and data sets to enable the data owner to analyze and review both authorized and unauthorized accesses; and  j) The database servers that control FTI applications will copy the query request and load it to the remote database to run the application and transform its output to the client. Therefore, access controls must be implemented at the authentication server; and  k) Web-enabled application software shall do the following:  1. Prohibit generic meta-characters in input data; and  2. Arrange to have all database queries constructed with parameterized stored procedures to prevent structured query language (SQL) injection; and  3. Protect any variable used in scripts to prevent direct OS command attacks; and  4. Arrange to have all comments removed for any code passed to the browser; and  5. Prevent users from seeing any debugging information on the client; and  6. Undergo a check before production deployment to ensure that all sample, test, and unused files have been removed from the production system. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | f.1 |  |
|  | f.2 |  |
|  | f.3 |  |
|  | g. |  |
|  | h. |  |
|  | i. |  |
|  | j. |  |
|  | k.1 |  |
|  | k.2 |  |
|  | k.3 |  |
|  | k.4 |  |
|  | k.5 |  |
|  | k.6 |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | f.1 |  |
|  | f.2 |  |
|  | f.3 |  |
|  | g. |  |
|  | h. |  |
|  | i. |  |
|  | j. |  |
|  | k.1 |  |
|  | k.2 |  |
|  | k.3 |  |
|  | k.4 |  |
|  | k.5 |  |
|  | k.6 |  |

|  |  |  |
| --- | --- | --- |
| ***Technical Controls – Audit and Accountability*** | | |
| The purpose of the control is to define specific and unique controls related to data warehousing audit and accountability.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) The agency shall ensure that audit reports are created and reviewed for data warehousing related access attempts; and  b) A data warehouse must capture all changes made to data, including additions, modifications, or deletions by each unique user; and  c) If a query is submitted, the audit log must identify the actual query made, the originator of the query, and relevant time and stamp information. The results of the query would not be as significant as the type of query made. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |

|  |  |  |
| --- | --- | --- |
| ***Technical Controls – System and Communication Protection*** | | |
| The purpose of the control is to define specific and unique controls related to data warehousing system and communication protection.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) Whenever FTI is located on both production and test environments, these environments are to be segregated. Such action is especially important in the development stages of the data warehouse; and  b) All Internet transmissions are to be encrypted with the use of HTTPS protocol and secure sockets layer encryption based on a certificate that contains a key no less than  128 bits in length, or FIPS 140-2 compliant, whichever is stronger. This encryption will allow information to be protected between the server and the workstation. Data is at its highest risk during the ETL stages when it enters the warehouse. Encryption shall occur as soon as possible. All sessions shall be encrypted and provide end-to-end encryption (i.e., from workstation to point of data); and  c) Web server(s) that receive online transactions shall be configured in a “demilitarized zone” to receive external transmissions but still have some measure of protection against unauthorized intrusion; and  d) Application server(s) and database server(s) shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers; and  e) Transaction data shall be “swept” from the Web server(s) at frequent intervals, consistent with good system performance, and removed to a secured server behind the firewalls to minimize the risk that these transactions could be destroyed or altered by intrusion; and  f) Antivirus software shall be installed and maintained with current updates on all servers and clients that contain tax data; and  g) For critical online resources, redundant systems shall be employed with automatic failover capability. | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |

|  |  |  |
| --- | --- | --- |
| ***Multi-Functional Devices and High Volume Printers*** | | |
| The purpose of this control is to address the use of FTI in a multi-functional device (MFD) or high-volume printer.   |  |  |  | | --- | --- | --- | | **Applicability of Controls** | | | | **Public** | **Confidential** | **FTI** | |  |  | Applies |   a) The agency should have a current security policy in place for secure configuration and operation of the MFD or High Volume Printer; and  b) Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to the MFD or High Volume Printer; and  c) Strong security controls should be incorporated into the MFD or High Volume Printer management and administration; and  d) Access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions; and  e) MFD's or High Volume Printers should be locked with a mechanism to prevent physical access to the hard disk; and  f) Firmware should be up to date with the most current firmware available and should be currently supported by the vendor; and  g) Devices and print spoolers have auditing enabled, including auditing of user access and fax logs (if fax is enabled), and audit logs should be collected and reviewed by a security administrator; and  h) All FTI data in transit should be encrypted when moving across a WAN and within the LAN; and  i) Disposal of all hardware follows media sanitization and disposal procedure requirements (see Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization). | | |
| **Requirement Implementation Details:**  Met  Partially Met  Not Met  N/A | | |
| **Responsible Parties:**  NC Department of Revenue  <PROVIDER> | | |
| **Control implementation***:* | | |
| <Provider> Response | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
|  | i. |  |
| NCDORResponse | | |
|  | a. |  |
|  | b. |  |
|  | c. |  |
|  | d. |  |
|  | e. |  |
|  | f. |  |
|  | g. |  |
|  | h. |  |
|  | i. |  |