Security Policy Manual

Revision History

Version	Date	Author	Description
v0-1	4-13-23	SSTech, Policy Team	Draft Created
v1-0	9-21-23	David Roseberry	Policy Approved

Contents

Overview

This document contains the security and privacy policies of the North Carolina Department of Revenue (Agency) with respect to the management of information, referred to in this document as Agency Data, and security of Resources. The purpose of this document is to set forth expectations of behavior to protect Agency Data and Resources managed by the Agency.

Executive Management has approved all of these policies and is committed to their enforcement. Executive Management and Divisions agree to this policy and ensure their staff members are aware of and adhere to this policy.

The Chief Information Officer (CIO) disseminates this manual and Executive Management reviews the policies at least every three years.

All policies contained herein apply to anyone working on behalf of the Agency including, but not limited to, employees, officers, agents, contractors, consultants, vendors, interns, or any other person performing work for the Agency or for any individual, partnership, corporation or other entity providing goods or services to the Agency that will participate in the handling of Agency Data and Resources. No exceptions to these policies are permitted unless previously approved. Any questions related to this document should be referred to your supervisor or the Chief Information Security Officer (CISO).

The intent of this security policy manual and any supporting documentation that originates from the office of the Secretary, COO, CIO, and/or the CISO is to establish the security policies of the Agency that will fully comply with the most recent revision of IRS Publication 1075.

Definitions

Access: Access is defined as the time when an individual: enters a restricted or locked area, room, container, or system containing Agency Data; or obtains, acquires, receives, examines, uses, or gains knowledge of Agency Data, by physical, electronic, or any other methods. Access also means the authority or approval to access restricted records or data, such as FTI when authorized under 6103 and with a need-to-know.

Access Tier: consists of entry points to the virtual environment. Access Tier devices include gateways, web interfaces, authentication servers and session manager. This tier brokers connections between Client Tier devices and Virtual Desktop Tier components.

Accountability: A process of holding users responsible for actions performed on an Agency Resource.

Adverse Action: A suspension of 15 days or more, a reduction in pay, or termination of employment.

Adequate Security: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

Agency: The North Carolina Department of Revenue.

Agency Data: Agency Data means all non-public information, formulae, algorithms, or other content, regardless of the form, that originates from the North Carolina Department of Revenue. Agency Data includes but is not limited to State Tax Information (STI), Personal Identifiable Information (PII), Federal Taxpayer Information (FTI), electronic payment information, physical and information systems security information, and any materials containing such information.

Alternate Work Site: Any working area that is attached to the wide area network either through a public switched data network or through the Internet.

Assurance: A measure of confidence that management, operational and technical controls are operating as intended and achieving the security requirements for the Resource.

Assurance Testing: A process used to determine if security features of a Resource are implemented as designed and are adequate for the proposed operating environment. This process may include hands-on functional testing, penetration testing and/or verification.

Audit: An independent examination of security controls associated with a representative subset of Agency Resources to determine the operating effectiveness of Resource controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy or procedures where needed.

Audit Trail: A chronological record of Agency Resource activities sufficient to enable the reconstruction, review and examination of security events related to an operation, procedure, or event in a transaction from its inception to results.

Authentication: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to Agency Resources; see Identification.

Authorization: Access privileges granted to a user, program, or process.

Availability: Timely, reliable access to information and information services for authorized users.

Basic Input/Output System (BIOS): In Agency security policies, refers collectively to boot firmware based on the conventional BIOS, Extensible Firmware Interface (EFI), and the Unified Extensible Firmware Interface (UEFI).

Blurring: The act of obscuring data so that it cannot be read or reconstructed.

Configuration Advisory Board: Group of individuals who are responsible for the decision as to when and if any changes are to be made to Resources and/or the NCDOR architecture.

Client Application Tier: Includes the applications that are delivered to the end user via the virtual desktop.

Client Tier: Includes the thin client devices (laptops, desktops, etc.) the end user employs to access their desktop within the virtual desktop tier.

Compromise: The disclosure of sensitive information to persons not authorized to receive such information.

Commingling: The presence of FTI and non-FTI data together on the same paper or electronic media.

Confidentiality: The preservation of authorized restrictions on information access and disclosure.

Configuration Management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle (SDLC).

Container: An object that can be used to hold or transport something for physical environments and software that has everything needed to run an application for cloud environments.

Containerize: To package (freight) in uniform, sealed containers for shipment for physical environments and the packaging of software code and all the necessary dependencies to run code in a single executable for cloud environments.

Control Number: A code that identifies a unique document or record.

Control Schedule: A record retention and disposal schedule established by the Agency.

Corrective Action Plan (CAP): A report detailing the Agency's planned and completed actions to resolve findings identified during an IRS safeguard review, Third Party Audit, or GRC Assessment.

Countermeasure: Action, device, procedure, mechanism, technique, or other measure that reduces the vulnerability of an Agency Resource.

Cryptography: The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable, computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. To determine if an IT service is considered as a "cloud" please see the document titled, "Do we have a cloud?"

Decryption: The process of converting encrypted information into a readable form. This term is also referred to as deciphering.

Degauss: To erase information electromagnetically from a magnetic disk or other storage device.

Digital Subscription Line: A public telecommunications technology that delivers high bandwidth over conventional copper wire that covers limited distances.

Disciplinary Action: An admonishment, written reprimand, or suspension of 14 days or less.

Discretionary Access Control: A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups, or processes.

External Resources/External Systems: External information systems, or non-Agency-owned equipment, include any technology used to receive, process, store, access, protect and/or transmit Agency Data that is not owned and managed by 1) the Agency or the Agency-run mobile device management system, 2) a state's consolidated IT office, 3) one of the Agency's approved contractors or sub-contractors (e.g., print vendors, collections agencies, application development contractors, network engineers at a state consolidated IT office, etc.) or 4) one of the Agency's constituent counties. To ensure a third-party contractor system is not considered an external information system, the Agency must include Exhibit 7 language in its contract with the service provider. Examples of external information systems include but are not limited to 1) personally owned devices, which includes any device owned by an individual employee, rather than the Agency itself; and 2) devices owned and managed by Agency stakeholders that do not have proper approvals to receive, process, store, access, protect and/or transmit Agency Data.

External Network: Any network that resides outside the security perimeter established by the telecommunications system.

FTI: FTI consists of federal tax returns and return information (and information derived from it) that is in the Agency's possession or control and received from the Internal Revenue Service (IRS) or any other entity acting on behalf of the IRS. Non-FTI data that is stored with FTI data ("Commingled Data"), must be protected as if it were entirely FTI.

Firmware: Microcode programming instructions permanently embedded into the read-only memory control block of a computer system. Firmware is a machine component of a computer system, like a computer circuit component.

Gateway: An interface that provides compatibility between heterogeneous networks by converting transmission speeds, protocols, codes, or security rules. This interface is sometimes referred to as a protocol converter.

Host: A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers or servers that provide dynamic host configuration protocol services.

Identification: A mechanism used to request access to Agency Resources by providing a recognizable unique form of identification such as a Login ID, User ID, or token; see Authentication.

Inadvertent Access: Access to Agency Data without authority that is non-willful and unanticipated or accidental.

Incidental Access: Access to Agency Data without a need-to-know that may occur in extraordinary circumstances (i.e., system failure, data incident response, disaster response).

Internet of Things (IoT): the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves. Examples of IoT are smart home devices (temperature control devices, electric usage applications), smart car applications, and inventory management systems.

Information Spillage: Instances where classified or controlled unclassified information (e.g., FTI) is inadvertently placed on systems that are not authorized to process such information. Such information spills occur when Agency Data that is initially thought to be of lower sensitivity is transmitted to a system and then subsequently determined to be of higher sensitivity.

Insider Threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, the state, and the nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information or through the loss or degradation of organizational resources or capabilities.

Integrity: The protection of Agency Resources and Data from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

Internet: Two or more networks connected by a router; the world's largest network, which uses TCP/IP to connect government, university, and commercial institutions.

Intranet: A private network that uses TCP/IP, the Internet and World Wide Web technologies to share information quickly and privately between authorized user communities, including organizations, vendors, and business partners.

Key: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

Least Privilege: A security principle under which users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

Local Access: Is any access to Agency Resources by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks.

NCDOR Facilities: Any facility that has been authorized to receive, process, store, transmit, or protect Agency data.

Nonlocal Maintenance and Diagnostic Activities: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the Resource or Resource component and not communicating across a network connection.

Mobile Code: Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on an Agency Resource without explicit installation or execution by the recipient.

Mobile Device: A computing device (other than a laptop) that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source.

Need-to-Know: Is established when individuals require access to non-public Agency Data and Resources to perform their official duties and, when accessing FTI, are authorized under the IRC.

Network: A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected Agency Resources or authorized External Resources or Systems that receive, process, store, access, protect and/or transmit Agency Data. Examples of networks include local area networks, wide area networks, metropolitan area networks and wireless area networks.

Network Access: Is access to Agency Resources and Data by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses).

Node: A device or object connected to a network.

Non-Agency-Owned Equipment: Any technology used to receive, process, store, access, protect and/or transmit Agency Data that is not owned and managed by the Agency but is owned by a contractor and centrally managed by their own IT department.

Nonrepudiation: The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets (i.e., senders and recipients of information cannot deny their actions).

Object: Passive system-related entity including, for example, devices, files, records, tables, processes, programs, and domains, that contain or receive information. Access to an object (by a subject) implies access to the information it contains.

Object Reuse: The reassignment of a storage medium, which contains residual information, to potentially unauthorized users or processes.

Personally Owned Devices: Any equipment purchased and owned by an individual, not owned or approved for use by the Agency, and not managed by an IT department.

Personnel Sanction: A disciplinary or adverse action for individuals failing to comply with established information security policies and procedures.

Privileged User: A user that has advanced privileges with respect to Agency Resources or authorized External Systems or Resources that receive, process, store, access, protect and/or transmit Agency Data. Such users in general include administrators.

POA&M/POAM: The Plan of Actions and Milestones is the sum of all compliance findings for the Agency. GRC/Third Party Audit (3PA) findings for Resource and supporting technologies are in individual Corrective Action Plans (CAPs) that are provided to key stakeholders for remediation purposes. IRS Safeguards findings are in the IRS CAP, one document that contains all IRS findings. These documents are highly confidential and are not shared without authorization from the CIO or CISO. Individual findings are shared only with staff who are directly involved in the remediation of those findings.

PII: Personally Identifiable Information (PII) is a person's first name or first initial and last name in combination with identifying information, (e.g., Social Security Number, driver’s license, state identification card or passport number, or other identifying information as defined in G.S. 14-113.20(b)). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and

does not include information made lawfully available to the public from federal, state, or local government records.

Remote Access: Remote access is access to Agency Resources (or processes acting on behalf of users) communicating through external networks such as the Internet. Remote access methods include, for example, dial-up, broadband, and wireless. Remote access controls apply to Resources other than public Resources designed for public access. Any remote access where (i) Agency Data is accessed or (ii) an Agency Resource is administered over the remote connection must be performed using multifactor authentication.

Resources: The collective parts that work together to serve an Agency function. This can include Staff, I.T. components, physical environments, data (physical or logical), or physical parts.

Safeguards: Protective measures prescribed to enforce the security requirements specified for Agency Resources; synonymous with security controls and countermeasures.

SCSEMS: Safeguard Computer Security Evaluation Matrix (or SCSEM for short) can serve several functions. The IRS utilizes SCSEMs as audit plans for IRS Safeguards Inspections conducted every three years to evaluate the security of Agency Resources. GRC utilizes SCSEMs in the same way the IRS does to continuously monitor compliance and to prepare the Agency for IRS Safeguards Inspections. IT “out of the box” or “off the shelf” typically has no security applied, so NCDOR IT utilizes SCSEMs as a security baseline to apply security measures/controls to all Agency Resources.

Staff: Anyone working on behalf of the Agency regardless of employment status and includes contractual relationships with entities that provide goods or services. This term is intended to be all encompassing and no exclusions are intended. The term employment in this document should be broadly interpreted to indicate any relationship between the Agency and members of its workforce. The term termination shall be broadly interpreted to indicate the end of that relationship.

SSR: Safeguards Security Report submission is a requirement of receiving FTI data. The report template is provided by the Office of Safeguards to entities receiving FTI data who submit the completed report back to the Office of Safeguards on an annual basis. The contents of the report are broken down into sections which contain requests for information from the Office of Safeguards, along with responses providing the requested information from the submitting entity. The submitted report is reviewed by

the Office of Safeguards and then returned with comments and additional requests to serve as the template for the following year's report submission. The annual submission dates are directed by the Office of Safeguards.

STI: State Tax Information (STI) is information collected by the North Carolina Department of Revenue for the purpose of administering taxes on behalf of the state of North Carolina. STI includes information contained in a tax return, report, or application for a license for which taxes are imposed, information obtained through an audit of a taxpayer or correspondence with a taxpayer, information on whether a taxpayer has filed a tax return or report, list or other compilation of information related to or concerning taxpayers, standards, methods, and data used for the determination of tax return examinations and audits.

Transcript Delivery System (TDS): the IRS E-Services Transcript Delivery System whereby authorized; registered users can access certain Federal Tax Information.

Trust Boundary: a border between two connected zones with different trust levels.

Unauthorized Access: Occurs when a person gains logical or physical access to Agency Data or Resources without authority under 6103 for FTI and without a need-to-know for all data types that are non-public.

Unauthorized Disclosure: Occurs when a person with access to Agency Data discloses it to another person without authority under 6103 for FTI and without COO, CISO, or CIO approval for all other data types.

Unified Extensible Firmware Interface (UEFI): A possible replacement for the conventional BIOS that is becoming widely deployed in new x86-based computer systems. The UEFI specifications were preceded by the EFI specifications.

Virtual Desktop Infrastructure (VDI): A virtual desktop infrastructure (VDI) provides users access to enterprise resources, including a virtual desktop from locations both internal to and external to the Agency's networks. In a VDI environment, a user can access Agency Data by connecting to a virtual workstation via a vendor-specific agent, connection client, or through an Internet browser from practically any mobile device with Internet access. Using VDI environments is the only way the Agency may authorize users to leverage personally owned devices to access and/or manage information systems that receive, process, store, access, protect and/or transmit Agency Data.

Virtual Desktop Tier: Contains the virtual desktop images residing on servers in the data center. Other components within the Virtual Desktop Tier include management

consoles, databases, virtualization components that publish virtualization resources and the hypervisor that handles the execution of the virtual environment. A virtual desktop is built using a modular approach where each component layers on top of another component to give the end-user a customized desktop environment.

Voice over Internet Protocol (VoIP): A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks, such as the Internet.

Vulnerability: A known deficiency in an information system, which threat agents can exploit to gain unauthorized access to sensitive or classified information.

Vulnerability Assessment: Systematic examination of an information system to determine its security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.

Management Commitment

The management of NCDOR is committed to enforcing these security policies and supporting the individuals responsible for ensuring compliance to this document. The Chief Information Officer serves as the primary custodian for security policies, is responsible for coordinating points of contact for all security policy related issues, and for delegating responsibilities among department entities and resource owners to ensure adherence to all elements contained in security policies.

Coordination Among Organizational Entities

The CIO coordinates with the CISO in the delegation of policy requirements among organizational entities.

Compliance

NCDOR utilizes IRS Publication 1075, the Management, Operational, and Technical (MOT) Safeguards Computer Security Evaluation Matrix (SCSEM), and Safeguards Computer Security Evaluation Matrices (SCSEMs), PCI, and all other applicable State and federal statutes to determine implementation and control effectiveness. The process includes a determination if policies have been adequately implemented or if a gap might exist.

Security Policies

Access Control Policy

Purpose

The purpose of this policy is to ensure that only authorized individuals and entities access Agency Data, Agency Resources that store and maintain Agency Data, and that controls are implemented to authenticate and grant access to Agency Resources and Data. This policy guarantees that protections are in place as a countermeasure to unauthorized access.

Scope

This policy applies to all Agency Staff, Resources, and Data (both physical and logical).

Policy

It is the policy of the Agency that protections will be implemented, managed, and maintained in accordance with all applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

Required Procedural Elements

Account Management

NCDOR will define and document the types of accounts allowed and specifically prohibited for use for Agency Resources that receive, process, store, or transmit Agency Data.

NCDOR will assign account managers and require conditions for group and role membership.

NCDOR uses automation management tracking solutions to control the workflow of managing accounts, and requires the following controls to be included:

1. Authorized users of the Resource.
2. Conditions for group and role membership.
3. Access authorizations as required for each account.
4. Require approvals by the Resource owner or designated representative for requests to create accounts.
5. Role-based access controls for authorized users of Agency Resources.

Accounts will be created, enabled, modified, disabled, and removed in accordance with NCDOR account management procedures and will include:

1. Notification to account managers and designated NCDOR officials within 24 hours when accounts are no longer required, 24 hours when users are terminated or transferred, and 24 hours when Resource usage or need-to-know change for an individual.
2. Authorization of access to the Resource will be based on a valid access authorization, intended Resource usage, and the under the authority to re-disclose FTI under the provisions of IRC § 6103.

NCDOR will require the monitoring of account usage.

Accounts will be reviewed for compliance with account management requirements annually for user accounts and semi-annually for privileged accounts.

NCDOR will establish and implement a process for changing shared or group account authenticators when individuals are removed from the group.

Account management processes will be aligned with terminations and transfer processes.

Automated Systems Management

NCDOR will support the management of Resource accounts using an approved automated system.

Removal of Temporary or Emergency Accounts

Automated workflows will be required to disable and remove temporary and emergency accounts after two (2) business days.

Disable Accounts

Accounts will be disabled after 120 business days when accounts have expired, are no longer associated with a user or individual, are in violation of an Agency policy, or have been inactive for 120 days for non-privileged accounts and 60 days for privileged accounts.

Automated Audit Actions

Account creation, modification, enabling, disabling and removal actions will be audited using an automated security tool. The solution will maintain alerting and logging capability that will be periodically reviewed.

Privileged User Accounts

Privileged accounts will be established and administered in accordance with role-based access and/or attribute-based access, will be monitored according to role assignments and changes in role, and revoked when no longer appropriate.

Restrictions on Use of Shared and Group Accounts

The use of shared and group accounts is prohibited unless an exception is approved by the CIO.

Account Monitoring for Atypical Usage

NCDOR will monitor Resource accounts for IT Security-defined atypical usage, and report atypical usage of Resource accounts to IT Security.

Disable Accounts for High-Risk Individual

NCDOR will Disable accounts of users posing a significant risk within one (1) day upon discovery.

Access Enforcement

NCDOR will enforce access permissions and authorizations by using the principle of least amount of privilege, separation of duties, and configuring Resources to provide only essential capabilities**.**

Users with administrative privileges will only access administrative accounts from NCDOR owned Resources or authorized contractor systems.

Controlled Release

NCDOR only allows the release of Agency Data outside of the Agency if**:**

- The COO, CIO, or CISO have formally approved the release of the information; and
- The receiving system accessing, processing, storing, or transmitting Agency Data provides Publication 1075 required protections; and
- MOUs, Publication 1075 requirements, Data Classification, and FedRAMP ATOs are used to validate the appropriateness of the information designated for release.

Restrict Access to Specific Information Types

Access will be restricted to data repositories containing Agency Data.

Information Flow Management

NCDOR will manage the flow of Agency Data by enforcing restrictions that include blocking external traffic that claims to be from within the department, keeping export-controlled Agency Data from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting Agency-approved information transfers between organizations based on data structures and content.

Separation Of Duties

NCDOR will divide mission or business/support functions among different individuals or roles when feasible. In addition, the department requires that individuals that administer access control functions will not administer audit functions.

NCDOR will identify and document separate duties of individuals to prevent harmful activity without collusion and define Resource access authorizations to support separation of duties.

Least Privilege

NCDOR will only allow authorized access (or processes acting on behalf of a user) that are necessary to accomplish assigned department tasks.

Authorize Access to Security Functions

NCDOR will explicitly authorize access to security functions deployed in hardware, software, and firmware.

NCDOR will restrict access to security functions and security-relevant information to authorized personnel only.

Non-Privileged Access for Non-security Functions

NCDOR requires that users of Resource accounts (or roles) with access to security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

NCDOR will prohibit accounts with administrative privileges (including local administrator rights) from web browsing and other Internet connections outside of the local protected boundary unless such risk is accepted in writing by the Agency's CISO.

NCDOR will require accounts to be blocked that have administrative privileges (including local administrator rights) from access to email unless such risk is accepted in writing by the Agency's CISO.

Privileges

NCDOR will prohibit privileged access to the Resource by non-Agency users.

NCDOR will perform an annual review of assigned user privileges to Agency Data to validate the need for such privileges and reassign or remove privileges, if necessary, to correctly reflect the company mission or business needs.

Privilege Levels for Code Execution

NCDOR will evaluate applications or programs that may require elevated privileges to function and prevent the execution of such privileges without an exception. The exception will be tracked through the Agency's Security Exemption Process and tracked on the Agency's POA&M.

Auditing Use of Privileged Functions

NCDOR will audit the execution of privileged functions.

Prohibit Non-Privileged Users from Executing Privileged Functions

NCDOR will prevent non-privileged users from executing privileged functions.

Unsuccessful Logon Attempts

NCDOR will enforce a limit of 3 consecutive invalid logon attempts by a user during a 120-minute period by automatically locking the account for 15 minutes or until unlocked by an administrator.

Mobile devices will be wiped of information based on Agency defined purging or wiping requirements and techniques after ten (10) consecutive, unsuccessful device logon attempts.

Resource Use Notification

NCDOR will display the Agency approved Resource warning banner to users before granting access to Resources to provide privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

The warning banner will state the following:

- Users are accessing a U.S. Government System.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

The warning banner must be applied to the application, database, operating system, and network device levels for all Resources that receive, process, store, or transmit Agency Data.

The notification message or banner will be retained on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the Resource; and

Publicly accessible Resources will:

1. Display the Agency approved Resource warning notification banner before granting further access to the publicly accessible Resource.
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such Resources that generally prohibit those activities.
3. Include a description of the authorized uses of the Resource.

Device Lock

A device lock of inactivity will be initiated after 15 minutes of inactivity; requiring the user to initiate a device lock before leaving the Resource unattended. The device will remain locked until the user re-establishes access using established identification and authentication procedures.

Pattern-hiding Displays

NCDOR, when locking the device, will conceal information previously visible on the display with a publicly viewable image.

Session Termination

User sessions will be terminated after 30 Minutes of inactivity are reached or when targeted responses to certain types of incidents, or time-of-day restrictions on Resource use are triggered.

User-Initiated Logouts

Logout capability for user-initiated communications sessions will be provided whenever authentication is used to gain access to Resources accessing, processing, storing, or transmitting Agency Data.

Permitted Actions Without Identification or Authentication

NCDOR will permit specific user actions without identification or authentication if it is determined that identification and authentication are consistent with organizational mission and business functions.

NCDOR will document and provide supporting rationale in the security plan for the Resource, user actions not requiring identification or authentication.

Remote Access

NCDOR will establish document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

NCDOR will authorize each type of remote access to the Resource prior to allowing such connections.

Monitoring and Control

Automated mechanisms will be employed to monitor and control remote access methods.

Protection of Confidentiality and Integrity Using Encryption

NCDOR will implement the latest FIPS 140 validated cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Managed Access Control Points

NCDOR will route remote accesses through authorized and managed network access control points.

Privileged Commands and Access

NCDOR will authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for an established business need.

NCDOR will document the rationale for remote access for the Resource in project documentation and in the SSR.

Disconnect or Disable Access

Capabilities will exist to disconnect or disable remote access to the Resource within 30 minutes of inactivity.

Wireless Access

NCDOR does not permit wireless access of system components and only allows wireless access to the network through Agency provided VPN.
NCDOR only allows wireless connections to the network via VPN. Wireless access to Resource components and/or Resources that contain FTI is prohibited.

Authentication and Encryption

NCDOR will protect wireless access to Agency Data using authentication of users and devices and FIPS 140-x validated encryption.

Disable Wireless Networking

NCDOR will disable, when not intended for use, wireless networking capabilities embedded within Resource components prior to issuance and deployment.

The guest wireless networks provided by the department are logically separated from other secure internal networks. Capabilities exist to provide guest wireless access to internet Resources only without commingling networks.

Wireless access will be logged, and I.T. Security will be alerted in the event of a potential event.

The latest FIPS 140 validated encryption will be employed on all wireless networks. Agency Data is not accessed and/or managed utilizing wireless networks without approval from the CISO.

Wireless networks will be monitored utilizing Artificial Intelligence/Machine Learning solutions for possible cyber-attacks.

Access Control for Mobile Devices

NCDOR will establish configuration requirements, connection requirements, and implementation guidance for the Agency -controlled mobile devices, to include when such devices are outside of controlled areas.

NCDOR will authorize the connection of mobile devices to Agency Resources.

Full Device or Container-based Encryption

NCDOR will employ full-device encryption using the latest FIPS 140 validated encryption to protect the confidentiality and integrity of information on mobile devices. NCDOR will not allow the use of Bring Your Own Devices (BYOD) in the department ecosystem, nor does it allow Agency Data or Resources to be accessed from BYOD devices.

POA&M findings will be documented and tracked when no such encryption technology solutions are available to address a specific device.

Use Of External Systems

The CISO is required to approve connections from Agency Resources to external systems.

NCDOR will establish terms and conditions consistent with trusted relationships established with other organizations owning, operating and/or maintaining external systems, allowing authorized individuals to:

- Access the system from external systems.
- Process, store, or transmit Agency Data using external systems.

NCDOR prohibits the use of non-Agency managed external resources.

Portable Storage Devices – Restricted Use

NCDOR will restrict the use of Agency controlled portable storage devices in CISO-approved external systems and restrict how the devices may be used and under what conditions the devices may be used.

NCDOR will restrict the use of Agency-controlled portable storage devices by authorized individuals on external systems for established business needs.

NCDOR will restrict the use of non-Agency owned systems or system components to process, store, or transmit Agency Data using Publication 1075 requirements.

The CISO is required to approve connections of non-government furnished or contractor-owned IT devices (including USB-connected portable storage and mobile devices) to Agency-owned Resources or networks receiving, processing, storing, accessing, protecting and/or transmitting Agency Data.

Non-Organizationally Owned Systems and Components - Restricted Use

NCDOR will restrict the use of non-department owned resources or system components to process, store, or transmit Agency Data as defined in Publication 1075.

Information Sharing

The CIO or delegate will determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions. For FTI data, this includes compliance with IRC § 6103.

NCDOR will employ automated mechanisms or manual processes compliant with IRC § 6103 to assist users in making information sharing and collaboration decisions.

Publicly Accessible Content

The PIO or their delegate are the only Agency staff authorized to make information publicly accessible.

NCDOR will train authorized individuals to ensure that publicly accessible information does not contain non-public information.

The PIO or their delegate review the proposed content of information prior to posting onto the publicly accessible Resource to ensure that nonpublic information is not included.

The PIO or their delegate will conduct a quarterly review of the content on publicly accessible Resources for nonpublic information and remove such information, if discovered.

Data Mining Protection

NCDOR will employ data mining prevention and detection techniques.

Alternate Work Site Policy

Purpose

The purpose of this policy is to provide a set of guidelines and rules that define the conditions under which NCDOR will approve alternate work locations and to ensure the security of Agency Data when employees work from alternate work sites.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

If the confidentiality of Agency Data can be adequately protected, telework sites such as employee's homes or other non-traditional work sites can be used.

Agency Data remains subject to the same safeguard requirements and the highest level of attainable security.

It is the policy of the Agency that security and privacy controls will be implemented in alternative work site environments.

Agency Staff Responsibilities

Agency Staff that are approved to work at alternate work sites must comply with all NCDOR policies and procedures and acceptable use of Agency Resources.

Agency Staff must regularly communicate with their manager and work within the agreed upon hours of operation.

Agency Staff are responsible for creating a safe and secure work environment using the agencies required controls for both logical and physical access.

All Staff must:

a) Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done.

b) Use secure and Agency authorized devices with approved connections to access Agency Data.

c) Ensure that any Agency-owned devices are physically secure and protected from theft or unauthorized access. Basic security requirements must be met, such as keeping Agency Data locked up when not in use.

d) Protect Agency Data from disclosure by securing the physical workspace from unauthorized entry. Do not leave computers unprotected at any time, including brief absences while staff are away from the computer. All computers, electronic media and removable media containing Agency Data must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

e) Only Agency-approved security access control devices and Agency-approved software will be used. Use of illegal and/or non-approved software is prohibited.

f) Use secure communication methods in the transmission of Agency Data (encryption, secure file transfer, etc.).

g) Participate in training and awareness programs specific to remote work and alternate work site security.

Agency Data may be stored on hard disks only if Agency-approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance including upgrades and are being used. Access controls must include password security, an audit trail, encryption, virus detection and data overwriting capabilities. When removable media contains FTI, it must be labeled as FTI.

Agency Requirements

All computers and mobile devices that contain Agency Data and reside at an alternate work site must employ encryption mechanisms to ensure that the data may not be accessed if the computer is lost or stolen.

Computers and electronic media (including telephones using Voice Over Internet Protocol [VOIP]) that receive, process, store, access, protect and/or transmit Agency Data must be in a secure area with restricted access.

The Agency will retain ownership and control of all hardware, software and end-point equipment connecting to public communication networks, where these are present at alternate work sites. Electronic media that is to be reused must follow media sanitization requirements.

The Agency must ensure employees have access to locking file cabinets or desk drawers so that documents, disks, and tax returns may be properly secured when not in use. If Agency furniture is not furnished to the employee, the Agency must ensure that an adequate means of storage exists at the alternate work site. The Agency must provide “locking hardware” to secure automated data processing equipment to large objects, such as desks or tables. Smaller, Agency-owned equipment must be locked in a filing cabinet or desk drawer when not in use.

The use of virtual desktop infrastructure with non-Agency-owned devices (including personally owned devices) is an acceptable alternative, where all requirements in the Agency’s security policies are followed.

Audit and Accountability Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered when developing audit and accountability programs and that assurances are in place that standards, guidelines, and procedures align with NCDOR’s compliance strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that a logging and monitoring capability will be implemented and that the logs will be retained as a part of an auditable function.

Required Procedural Elements

Audit Events

NCDOR will identify the types of events that the Resource is capable of logging in support of the audit function:

- All accesses or attempts to access an Agency Resource, including the identity of each user and device.
- Logoff activities.
- Activities that might modify, bypass, or negate IT security safeguards.
- Security-relevant actions associated with processing Agency Data.
- User generation of reports and extracts containing Agency Data.
- Any interaction with Agency Data through an application.
- Password changes.
- Creation or modification of groups.
- Privileged user actions.
- Access to the Resource.
- Creating and deleting files.
- Change of permissions or privileges.
- Command line changes and queries.
- Changes made to an application or database.
- Resource and data interactions.
- Opening and/or closing of files.
- Program execution activities.

NCDOR will coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged.

NCDOR will specify the following event types for logging within the Resource:

- Program execution activities.
- Creating and deleting files.
- Change of permissions or privileges.
- Access to the Resource.
- Password changes.
- Creation or modification of groups.

NCDOR will provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.

NCDOR will review and update the event types selected for logging annually or when there is a Resource change.

NCDOR will document changes in the SSR.

Content of Audit Records

NCDOR will ensure that audit records contain information that establishes the following:

- What type of event occurred.
- When the event occurred.
- Where the event occurred.
- Source of the event.
- Outcome of the event
- Identity of any individuals, subjects, or objects/entities associated with the event.

NCDOR will generate audit records that contain all details necessary to reconstruct events linked to an occurrence involving actual or suspected unauthorized activity, or when a malfunction occurs or is suspected.

NCDOR will limit personally identifiable information contained in audit records.

Audit Storage Capacity

NCDOR will allocate audit log storage capacity to accommodate the retention of audit records for the retention period.

Response to Audit Processing Failures

NCDOR will alert designated organizational officials, per the incident response policy, in the event of an audit processing failure.

NCDOR will take the following additional actions:

1. Monitor Resources 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 Owner.

2. If logs are not available, shut down the Resource. The Resource will remain offline until an investigation is conducted, and the CIO determines that the Resource is safe to resume normal operations.

NCDOR will require that a warning be provided to IT Security within 24 hours when an audit logs storage volume reaches 80% of maximum audit log storage capacity.

Audit Review, Analysis and Reporting

NCDOR will review and analyze Resource audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.

NCDOR will report findings to the individual(s) specified within the Agency's incident response procedures.

NCDOR will adjust the level of audit record review, analysis, and reporting within the Resource when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

NCDOR will integrate audit record review, analysis, and reporting processes using automated mechanisms to support Agency processes for investigation and response to suspicious activities.

NCDOR will analyze and correlate audit records across different repositories to gain Agency wide situational awareness.

NCDOR will specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit record information.

NCDOR will correlate information from nontechnical sources with audit record information to enhance Agency-wide situational awareness.

Audit Reduction and Report Generation

NCDOR will provide and implement an audit record reduction and report generation capability that:

- Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents.
- Does not alter the original content or time ordering of audit records.

NCDOR will provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: likelihood of potential inappropriate access or unauthorized disclosure of Agency Data.

Time Stamps

NCDOR will use internal system clocks to generate time stamps for audit records.

NCDOR will record time stamps for audit records that meet AU-2 and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Protection of Audit

NCDOR will protect audit information and audit logging tools from unauthorized access, modification, and deletion,

The CIO, CISO, or designated authority will be notified upon detection of unauthorized access, modification, or deletion of audit information.

NCDOR will authorize access to management of audit logging functionality to only authorized Resource Owners.

Audit Record Retention

NCDOR will retain audit records seven (7) years to provide support for after-the-fact investigations of incidents and to meet regulatory and Agency information retention requirements unless stated otherwise in North Carolina General Statue or Governor's Executive Order.

Audit Generation

NCDOR will provide audit record generation capability for the following event types, if the Resource is capable, and for Resources that receive, process, store, access, protect and/or transmit Agency Data:

- All accesses or attempts to access an Agency Resource, including the identity of each user and device.
- Logoff activities.
- Activities that might modify, bypass, or negate IT security safeguards.
- Security-relevant actions associated with processing Agency Data.
- User generation of reports and extracts containing Agency Data.

- Any interaction with Agency Data through an application.
- Password changes.
- Creation or modification of groups.
- Privileged user actions.
- Access to the Resource.
- Creating and deleting files.
- Change of permissions or privileges.
- Command line changes and queries.
- Changes made to an application or database.
- Resource and data interactions.
- Opening and/or closing of files.
- Program execution activities.

NCDOR will allow IT Security to select the event types that are to be logged by specific components of the Resource.

NCDOR will generate audit records for the following event types:

- Program execution activities.
- Creating and deleting files.
- Change of permissions or privileges.
- Access to the Resource.
- Password changes.
- Creation or modification of groups.

And will include:

- What type of event occurred.
- When the event occurred.
- Where the event occurred.
- Source of the event.
- Outcome of the event
- Identity of any individuals, subjects, or objects/entities associated with the event.

NCDOR will compile audit records from Resources that receive, process, store, access, protect and/or transmit Agency Data into a Resource-wide logical audit trail that is time

correlated to within 1 minute for the relationship between time stamps of individual records in the audit trail.

Cross-Organizational Auditing

NCDOR will employ methods for coordinating audit information among external organizations when audit information is transmitted across organizational boundaries on a case-by-case basis depending on the needs of the business.

NCDOR will preserve the identity of individuals in cross-organizational audit trails.

NCDOR will provide cross-organizational audit information to our vendors and other state agencies based on MOU and other similar agreements.

Awareness and Training Policy

Purpose

The purpose of this policy is to outline NCDOR's policy for security awareness and training in response to the AT control family defined by NIST SP 800-53 rev 5 and IRS Publication 1075.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

NCDOR will develop a training and awareness program that addresses all federal laws, executive orders, directives, regulations, and guidance pertaining to security and privacy controls as well as preventions needed from staff in response to the cyber security threat landscape.

Required Procedural Elements

Literacy Training and Awareness

NCDOR will ensure that all Staff receive security and privacy literacy training as a part of initial training for new users, Resource changes or following audit findings, security or privacy incidents, changes in applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and on annual basis thereafter.

NCDOR will employ online training modules by a third-party service provider and periodic security and privacy reminders by email to increase employee awareness.

NCDOR will update content for literacy training and awareness on an annual basis or following Resource changes.

NCDOR will incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness.

Practical Exercises

NCDOR will evaluate training and create awareness training based on simulated events and incidents. The training might include:

1. Impacts of opening email suspicious email attachments
2. Impacts of clinking on unknown weblinks
3. Spear phishing attacks

Insider Threat

NCDOR will provide literacy training on recognizing and reporting potential indicators of insider threat.

Insider threat training will include:

1. Precursors of insider threats inordinate, long-term job dissatisfaction, attempts to gain unauthorized data.
2. Unexplained access or gain to financial Resources.
3. Violations to policy, directives, or regulations.
4. Communication mediums for employees to report.

Social Engineering and Mining

NCDOR will provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Training will include:

1. Phishing Campaign Exercises
2. Social Media Exploitation
3. Attacks leveraging social mining.

Suspicious Communications

NCDOR will train users on recognizing suspicious communications and anomalous behavior. Training may include:

1. Checking the source of email addresses
2. Receiving emails from unfamiliar senders
3. Emails with poor or strange grammar
4. Unusual attachments or weblinks

Additional Directives

NCDOR will train users on the protections needed to ensure workstations are secure from possible theft.

NCDOR will distribute reminders/updates to all users on a quarterly basis based on the most relevant security and privacy threats.

NCDOR will conduct phishing simulation exercises on a quarterly basis.

Role-Based Training

NCDOR will provide role-based security and privacy training to employees with following roles:

1. Information Security Officer
2. Information Security Manager
3. Information System Specialists
4. Network and Systems Administrators
5. Personnel with access to FTI

NCDOR will require training before authorizing access to the Resource, Agency Data, or performing assigned duties upon hire, Resource changes, changes in job function, and on an annual basis.

NCDOR will update role-based training content annually and following changes to job related duties or migration to new Resources.

NCDOR will incorporate lessons learned from internal or external security incidents or breaches to role-based training.

Training Records

NCDOR will document and monitor security and privacy training activities, including security and privacy awareness training and role-based training. In addition, NCDOR will retain individual training records for 5 years.

Training Feedback

NCDOR will provide feedback to the following staff:

- Agency Senior Management; and
- Agency Disclosure Personnel.

Background Investigation Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered when conducting background investigations, and that assurances are in place that standards, guidelines, and procedures align with NCDOR's compliance strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency to complete a suitability background investigation prior to granting access to Agency data.

Required Procedural Elements

Minimum Standards

NCDOR will initiate a background investigation for all newly hired employees, contractors, and sub-contractors who will require access to Agency Data to perform their assigned duties.

NCDOR will require that employees, contractors, and sub-contractors (if authorized), with access to Agency Data complete a background investigation that is favorably adjudicated.

Background investigations for any individual granted access to Agency Data will include, at a minimum:

1. FBI fingerprinting (FD-258) -review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. Contact the appropriate state identification bureau for the correct procedures to follow. A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary-checks/state-identification-bureau-listing.

   This national agency check is the key to evaluating the history of a prospective candidate for access to Agency Data. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.

2. Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last five (5) years and if applicable, of the appropriate agency for any identified arrests.

   The local law enforcement check will assist the Agency in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.

3. Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization).

   Employers must complete USCIS Form I-9 to document verification of the identity and employment authorization of each new employee hired after November 16, 1986, to work in the United States. Within three (3) days of completion, any new employee must also be processed through E-Verify to assist with verification of their status and the documents provided with Form I-9. The E-Verify system is free of charge and can be located at www.uscis.gov/e-verify. This verification process may only be completed on new employees. Any employee with expiring employment eligibility must be documented and monitored for continued compliance.

NCDOR will conduct a suitability or security background investigation based on the position sensitivity of the individual's assigned position and risk designation associated with the investigative Tier established by the Federal Investigative Standard (FIS).

NCDOR will at a minimum, every five (5) years, conduct reinvestigation.

If the Agency can encrypt data in transit and at rest using the latest FIPS 140 certified solutions and maintain sole ownership of encryption keys, preventing logical access

from the cloud service providers, the Agency will consider this a logical barrier and will allow data types with restrictions to move to a cloud environment. Using FIPS 140 certified encryption at rest exempts third-party contractors from some protection requirements such as training and background investigation requirements.

Preventing or Removing Access

Access to Agency Data may be prevented and/or removed under the following circumstances:

- Attempts to access non-public data without authorization from the COO, CIO, or CISO.
- Separation or transfer (where access requirement changes are needed).
- Non-completion of all required security training.
- Willful attempts to circumvent security controls.
- Data incidents involving employees where continued access could further jeopardize data.
- Attempts to access Agency Data from outside of the US.
- Where the originating IP address or location of a technology cannot be determined

Certificate Authority - Assessment, Authorization, and Monitoring Policy

Purpose

The purpose of this policy is to ensure that controls designed to facilitate security assessment, authorization, or monitoring are identified to support the certification and evaluation functions.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that the assessment selection process will include a predetermined plan that considers the type of assessment to be performed and that the appropriate assessor or team is vetted.

Required Procedural Elements

Control Assessments

NCDOR will develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment.
2. Assessment procedures to be used to determine control effectiveness.
3. Assessment environment, assessment team, and assessment roles and responsibilities.

NCDOR will ensure the control assessment plan is reviewed and approved by the CISO designated representative prior to conducting the assessment.

NCDOR will assess the controls in the Resource and its environment of operation annually 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 and privacy requirements.

NCDOR will produce a control assessment report that documents the results of the assessment.

NCDOR will provide the results of the control assessment to the CIO or CISO.

NCDOR will employ independent assessors or assessment teams to conduct control assessments. NCDOR will:

- Ensure assessors are free from conflict of interests due to being involved in the development, operation, sustainment, or management of the Resources in scope.
- Ensure assessors do not evaluate their own work.
- Ensure that assessments are obtained from independent, unbiased entities (internal audit, GRC, etc.)

Information Exchange

NCDOR will approve and manage the exchange of information between External Resources and internal Resources using Interconnection Security Agreements (ISAs).

NCDOR will document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each Resource, and the impact level of the information communicated; and

NCDOR will review and update the Resource interconnection on an annual basis.

Plan of Action and Milestones

NCDOR will develop a plan of action and milestones for the Resource to document the planned remediation actions of the Agency to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the Resource.

NCDOR will update existing plan of action and milestones on a quarterly basis, at a minimum, based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

NCDOR will identify in the POA&M the Resource Owner or department responsible for correcting the noted weakness.

NCDOR will enter all weaknesses into appropriate POA&Ms within two (2) months for weaknesses identified during assessments.

Authorization

The CIO is the authorizing official for NCDOR information technology Resources.

NCDOR will assign a senior official as the authorizing official for common controls available for inheritance by Agency Resources.

NCDOR will ensure that the authorizing official for the Resource, before commencing operations:

1. Accepts the use of common controls inherited by the Resource.
2. Authorizes the Resource to operate.

NCDOR will ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by Agency Resources.

NCDOR will update the authorizations whenever there is a significant change to the Resource, or every three (3) years, whichever occurs first.

Continuous Monitoring

NCDOR will develop a Resource-level continuous monitoring strategy and implement continuous monitoring in accordance with the Agency continuous monitoring strategy that includes:

- The Agency will establish metrics to be monitored.
- The Agency will monitor metrics no less than quarterly.
- Ongoing control assessments in accordance with the continuous monitoring strategy.
- Ongoing monitoring of Resource and Agency-defined metrics in accordance with the continuous monitoring strategy.
- Correlation and analysis of information generated by control assessments and monitoring.
- Response actions to address results of the analysis of control assessment and monitoring information.
- Reporting the security and privacy status of the Resource to the CIO, CISO and COO annually, at a minimum.
- Employ independent assessors or assessment teams to monitor the controls in the Agency Resource on an ongoing basis.
- Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

    a. Effectiveness monitoring; and

    b. Compliance monitoring; and

    c. Change monitoring.

Penetration Testing

NCDOR will conduct penetration testing every 3 years on Agency Resources.

Internal Resource Connections

NCDOR will manage internal Resource connections by:

- Authorizing internal connections of Resource components or classes of components to the Agency Resource; and
- Documenting, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; and
- Terminating internal Resource connections after conditions defined by policy or at the discretion of the CIO; and
- Reviewing annually the continued need for each internal connection; and
- Performing security and privacy compliance checks on constituent Resource components prior to the establishment of the internal connection.

Cloud Computing Policy

Purpose

The purpose of this policy is to ensure that Agency Data that is received, processed, stored, transmitted, or accessed from a cloud environment is protected with predefined security and privacy controls.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that cloud environments will be managed under Agency requirements for security and privacy controls and following the guidance/notification requirements of the Office of Safeguards and Publication 1075.

Required Procedural Elements

Cloud Computing

NCDOR will document the physical locations where Agency Data will be processed to ensure Agency Data remains onshore.

NCDOR will document the cloud service provider's FedRAMP authorization such that the Agency and/or IRS Safeguards does not have the responsibility to assess the physical security of cloud service provider facilities.

NCDOR will provide a brief explanation of how encryption will be used to prevent unauthorized disclosures to cloud service provider employees.

NCDOR will document all Agency-managed security and privacy controls.

If the Agency is unable to demonstrate how cloud service providers can be prevented from having logical access to data, NCDOR will submit a notification for disclosure to a contractor or sub-contractor that contains all required information as outlined in Publication 1075.

Mandatory Requirements

NCDOR will adhere to the following mandatory requirements when utilizing a cloud computing model to receive, process, store, access, protect and/or transmit Agency Data:

- FedRAMP Authorization: Agency Data may only be introduced to cloud environments that have been provided an authorization by the Joint Advisory Board (JAB) or a Federal Agency.
- Onshore Access: Agencies must leverage vendors and services where (i) all Agency Data physically resides in systems located within the United States; and (ii) all accesses and support of the systems and services are performed from the United States, its possessions, and territories.
- Physical Description: Agencies and their cloud providers must provide a complete listing of all data center addresses where FTI will be received, processed, stored, accessed, protected and/or transmitted in their 45-Day notification form.
- Data Encryption in Transit: Agency Data must be encrypted in transit within the cloud environment. All mechanisms used to encrypt Agency Data must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA.
- Data Encryption at Rest: Agency Data must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA.

- 45-Day Notification: The Agency must notify the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment, per Section 2.E.6, Notification Reporting Requirements.
- Service Level Agreements and Contracts: The Agency must establish security and privacy controls, based on IRS Publication 1075, for how Agency Data is received, processed, stored, accessed, protected and/or transmitted inside the cloud environment. Agencies must provide the requirements through a legally binding contract or SLA with their third-party cloud provider.
- Data Isolation: Software and/or services that receive, transmit, process or store Agency Data must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.
- Risk Assessment: The Agency must conduct an annual assessment of the security and privacy controls in place on all Resources used for receiving, processing, storing, accessing, protecting and/or transmitting Agency Data.
- Persistence of Data in Relieved Assets: Storage devices where Agency Data has resided must be securely sanitized and/or destroyed using methods acceptable by NIST. This requirement must be included in the SLA and in the Agency Resource Sanitization plan signed by all parties involved.
- Multifactor Authentication: Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the Agency's trusted network). If the cloud can only be accessed from the Agency's internal network, multifactor authentication must be implemented by Agency solution(s) when establishing a remote connection.
- Security Control Implementation: Customer defined security and privacy controls must be identified, documented, and implemented, and must comply with Publication 1075 requirements.

Configuration Management Policy

Purpose

The purpose of this policy is to ensure that a process is in place for approving and managing changes over a Resource life cycle.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that Resources will adhere to a baseline configuration and that changes will have a managed approval process to ensure the integrity of NCDOR security standards.

Required Procedural Elements

Baseline Configuration

NCDOR will develop, document, and maintain under configuration control, a current baseline configuration of the Resource.

NCDOR will review and update the baseline configuration of the Resource:

1. At a minimum annually.
2. When required due to reorganizations, refreshes, etc.
3. When Resource components are installed or upgraded.

NCDOR will maintain the currency, completeness, accuracy, and availability of the baseline configuration of the Resource using automated mechanisms. NCDOR will utilize the following:

- Hardware and software inventory tools.
- Configuration Management Tools and Compliance Scan solutions.
- Network Management Tools

NCDOR will retain older versions of baseline configurations of the Resource to support rollback.

NCDOR will utilize SCSEMS to ensure secure configurations of all Agency information technology and communication Resources receiving, processing, storing, accessing, protecting and/or transmitting Agency Data.

NCDOR will issue a specifically configured computing device with more stringent configuration settings and the minimum-needed access to individuals traveling to locations that are deemed to be of significant risk.

NCDOR will examine the device upon the individual's return to examine for signs of tampering and the device will be reformatted before reintroduction into the environment.

Configuration Change Control

NCDOR will determine and document the types of changes to the Resource that are configuration controlled.

NCDOR will review proposed configuration-controlled changes to the Resource and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.

NCDOR will document configuration change decisions associated with the Resource.

NCDOR will implement approved configuration-controlled changes to the Resource.

NCDOR will retain records of configuration-controlled changes to the Resource for 3 years.

NCDOR will monitor and review activities associated with configuration-controlled changes to the Resource.

NCDOR will coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes at least monthly when changes are proposed.

NCDOR will test, validate, and document changes to the Resource before finalizing the implementation of the changes.

NCDOR will require the Deputy Chief Information Security Officer, Resources Owners, application managers, server managers, and any other members designated by the CIO or CISO to be members of the Configuration Control Board.

Security and Privacy Impact Analyses

NCDOR will analyze changes to the Resource to determine potential security and privacy impacts prior to change implementation.

NCDOR, after Resource changes, will verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome regarding meeting the security and privacy requirements for the Resource.

Access Restrictions for Change

NCDOR will define, document, approve, and enforce physical and logical access restrictions associated with changes to the Resource.

NCDOR will limit privileges to change Resource components and Resource-related information within a production or operational environment.

NCDOR will review and reevaluate privileges semi-annually.

NCDOR will restrict administration of configurations to only authorized administrators.

NCDOR will verify the authenticity and integrity of Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) updates to ensure that the BIOS or UEFI is protected from modification outside of the secure update process.

Configuration Settings

NCDOR will establish and document configuration settings for components employed within the Resource that reflect the most restrictive mode consistent with operational requirements using Office of Safeguards–approved compliance tools (e.g., SCSEMs, automated assessment tools).

NCDOR will implement the configuration settings.

NCDOR will identify, document, and approve any deviations from established configuration settings for information Resources that receive, process, store, or transmit Agency Data based on explicit operational requirements.

NCDOR will monitor and control changes to the configuration settings in accordance with Agency policies and procedures.

NCDOR will ensure that all devices across the enterprise that store Agency data are appropriately reviewed for security purposes prior to connection or reconnection to the Agency's network.

Least Functionality

NCDOR will configure the Resource to provide only mission essential capabilities.

NCDOR will prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:

1. Those not needed to conduct business.
2. Those defined in the IRS Office of Safeguards approved compliance requirements (e.g., SCSEMs, assessment tools).

3. Maintenance ports when not in use.
4. File Transfer Protocol (FTP).

NCDOR will review the Resource annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services.

NCDOR will disable or remove identified functions, ports, protocols, and services within the Resource deemed to be unnecessary and/or nonsecure.

NCDOR will identify software programs authorized to execute on the Resource.

NCDOR will employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the Resource.

NCDOR will review and update the list of authorized software programs at a minimum annually.

NCDOR will periodically scan Agency networks to detect and remove any unauthorized or unlicensed software.

NCDOR does not allow any personally owned equipment for business use. In addition, only equipment that is procured by the Agency is allowed to be used for business purposes.

NCDOR will prohibit the use or connection of unauthorized hardware components.

NCDOR will review and update the list of authorized hardware components annually.

Resource Component Inventory

NCDOR will develop and document an inventory of Resource components that:

- Accurately reflects the Resource.
- Includes all components within the Resource.
- Does not include duplicate accounting of components or components assigned to any other Resource.
- Is at the level of granularity deemed necessary for tracking and reporting.

And further includes:

- Hardware inventory specifications
- Software license information
- Software version numbers.

- Resource owners for networked components or devices.
- Machine names and network addresses.
- Manufacturer, device type, model, serial number, and physical location.

NCDOR will review and update the Resource inventory at a minimum annually.

NCDOR will update the inventory of Resource components as part of component installations, removals, and Resource updates.

NCDOR will detect the presence of unauthorized hardware, software, and firmware components within the Resource always using automated mechanisms.

NCDOR will take the following actions when unauthorized components are detected:

1. Disable network access with such components.
2. Isolate the components.
3. Notify designated Agency IT personnel.

Configuration Management Plan

NCDOR will develop, document, and implement a configuration management plan for the Resource that:

- Addresses roles, responsibilities and configuration management processes and procedures.
- Establishes a process for identifying configuration items throughout the systems development lifecycle (SDLC) and for managing the configuration of the configuration items.
- Defines the configuration items for the Resource and places the configuration items under configuration management.
- Is reviewed and approved by designated Agency personnel.
- Protects the configuration management plan from unauthorized disclosure and modification.

Software Usage Restrictions

NCDOR will use software and associated documentation in accordance with contract agreements and copyright laws.

NCDOR will track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

NCDOR will control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

User-Installed Software

NCDOR will establish policies governing the installation of software by users.

NCDOR will enforce software installation policies through the following methods: procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on Agency Resources), or both.

NCDOR will Monitor policy compliance at a minimum annually.

Information Location

NCDOR will identify and document the location of Agency Data and the specific Resource components on which the information is processed and stored.

NCDOR will identify and document the users who have access to the Resource and Resource components where the information is processed and stored.

NCDOR will document changes to the location (i.e., Resource or Resource components) where the information is processed and stored.

NCDOR will use automated tools to identify Agency Data on Resource components to ensure controls are in place to protect Agency information and individual privacy.

NCDOR will include all FTI Resource and Resource components in the Agency's FTI inventory.

Data Action Mapping

NCDOR will develop and document a map of Resource data actions.

Approved Components

For non-public facing systems, NCDOR will prevent the installation of unauthorized software and firmware components through AD policy and by preventing non-administrative positions the ability to install software. For public facing systems, NCDOR will prevent the installation of software and firmware components without verification

that the component has been digitally signed using a certificate that is recognized and approved by the Agency.

Contingency Planning Policy

Purpose

The purpose of this policy is to ensure the continuance of operations in mission achievement and business critical functions.

Scope

The policy applies to all Agency Resources and Data (physical and logical).

Policy

It is the policy of NCDOR to implement contingency plan controls that ensure that the information technology environment is replicated to a secondary environment and that protections for the restoration and reconstitution of Agency Resources are in place.

Required Procedural Elements

Contingency Plan

NCDOR will develop a plan that:

- Identifies essential missions and business functions and associated contingency requirements.
- Provides recovery objectives, restoration priorities and metrics.
- Addresses contingency roles, responsibilities, assigned individuals with contact information.
- Addresses maintaining essential missions and business functions despite a Resource disruption, compromise, or failure.
- Addresses eventual, full Resource restoration without deterioration of the controls originally planned and implemented.
- Addresses the sharing of contingency information.
- Is reviewed and approved by designated Agency officials and other applicable Agency stakeholders.

NCDOR will distribute copies of the contingency plan to key contingency personnel.

NCDOR will coordinate contingency planning activities with incident handling activities.

NCDOR will review the contingency plan for the Agency Resource at a minimum annually.

NCDOR will update the contingency plan to address changes to the organization, Resource, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

NCDOR will communicate contingency plan changes to key contingency personnel.

NCDOR will incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.

NCDOR will protect the contingency plan from unauthorized disclosure and modification.

NCDOR will coordinate the contingency plan's development with Business Operations, Business Representatives, IT Operations, IT Security, and key role players as identified by the CISO.

NCDOR will strive to resume essential mission and business functions within the time frame identified in approved contingency plans.

NCDOR will identify critical Resource assets that support mission and business functions.

Contingency Training

NCDOR will provide contingency training to Resource users consistent with assigned roles and responsibilities:

1. Within 30 days of assuming a contingency role or responsibility.
2. When required by Resource changes.
3. Annually thereafter.

NCDOR will review and update contingency training content every three (3) years and following a significant change.

Contingency Plan Testing

NCDOR will test the contingency plan for the Resource at a minimum, annually using table-top exercises in accordance with NIST SP 800-84 Guide to Test, Training, and Exercise Process for IT Plans and Capabilities, NIST SP-34 Contingency Planning Guide for Federal Information Systems and other applicable guidance, and Business-unit Defined Tests and Exercises.

NCDOR will review the contingency plan test results and initiate corrective actions, if needed.

Testing will include Agency departments that are deemed mission critical or personnel that have roles and responsibilities in business continuance, disaster recovery, business operations, crisis management, cyber security incident response, and with Agency personnel responsible for the protection of Agency Data.

Resource Backup

NCDOR will conduct backups of user-level information contained in Resource documentation, including security-related documentation, weekly.

NCDOR will conduct backups of system-level information contained in the Resource weekly.

NCDOR will conduct backups of Resource documentation, including security- and privacy-related documentation weekly.

NCDOR will protect the confidentiality, integrity, and availability of backup information.

Backup transmissions, media, and data will be protected by cryptographic mechanisms to prevent unauthorized disclosure and modification or backup information containing Agency Data.

Resource Recovery and Reconstitution

NCDOR will provide for the recovery and reconstitution of the Resource to its known state within predefined time periods that are consistent with impact and the criticality of the Resource. Recovery times will remain consistent with Resource recovery time and point objectives.

NCDOR will recover transaction-based Resources that includes a mechanism to recover transactions either through a rollback or journaling process.

Email Communications, Facsimile, and Facsimile Devices Policy

Purpose

The purpose of this policy is to establish guidelines for the appropriate use of email and fax communication within NCDOR.

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that Agency Data is permitted to be included in email or facsimile communications provided that all security policies and procedures, along with Publication 1075 requirements are met.

All Staff must:

a) Ensure that all transmissions are sent to only authorized recipients.
b) Follow all guidelines and protocols related to sending Agency Data internally and/or externally.
c) Provide adequate labeling (e.g., email subject contains FTI) and protection.
d) Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, that includes:
    1. A notification of the sensitivity of the data and the need for protection.
    2. A notice to unintended recipients to telephone to report the disclosure and confirm destruction of the information.

NCDOR employees must immediately report any email or fax containing Agency Data that is inadvertently sent to the wrong person or that is in violation of this policy to the Service Desk or by opening a security incident ticket.

Required Procedural Elements

Email Protections

All Staff must:

- Prohibit Agency Data in email transmissions outside of the Agency's internal network; and

- Ensure transmissions are sent only to authorized recipients; and
- Provide adequate labeling (e.g., email subject contains “FTI”) and protection.

NCDOR will securely configure mail servers and clients. The underlying operating systems of on-premises mail servers will be hardened and included in the Agency’s mail servers and clients.

NCDOR will configure the network infrastructure to block unauthorized traffic.

NCDOR will provide additional layers of security to the Agency’s mail servers and clients as well as limit the number of security related vulnerabilities.

NCDOR will implement audit logging to track all sent and received emails containing Agency Data.

NCDOR will deploy methods of encryption for email transmissions containing Agency Data using the latest FIPS 140 validated mechanism.

NCDOR will implement malware protection at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware.

NCDOR will block accounts with administrative privileges (including local administrator rights) from access to email unless such risk is accepted in writing by the Agency's CISO.

Fax Protections

NCDOR will ensure approved fax communications are transmitted to an authorized recipient by adhering to the following requirements:

- Have a trusted staff member at both the sending and receiving fax machines.
- Accurately maintain broadcast lists and other preset numbers of frequent recipients of Agency Data.
- Place fax machines in a secured area
- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, that includes:
  1. A notification of the sensitivity of the data and the need for protection
  2. A notice to unintended recipients to telephone the sender via collect call, if necessary, to report the disclosure and confirm destruction of the information.

NCDOR will ensure facsimile devices used to transmit Agency Data are properly protected and secured. At a minimum:

a. When applicable, encrypt information or be connected to a secure network.

b. Securely configure multifunction devices (MFD) used to receive or transmit fax communications.

Digital fax servers will be hardened to reflect secure standards for servers that maintain Agency Data.

Prohibited Uses of Email and Fax

Prohibited uses of e-mail include, but are not limited to:

- The distribution of insulting, offensive, or disruptive messages. Among those which are considered offensive, are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.
- Opening e-mail attachments from unknown or unsigned sources.
- Use of third-party email sources to send communications on behalf of the Agency.
- Represent personal opinions not authorized by the Agency.
- Sharing email passwords account passwords.
- The solicitation or persuasion of commercial ventures, religious or political causes, outside organizations, or to other non-job-related solicitations
- To send (upload) or receive (download) copyrighted materials, proprietary company information, or similar materials without prior authorization.
- Solicit non-Agency business for personal profit or gain.
- Send Agency Data without using an approved method of encryption.
- Excessive personal use of company email Resources is prohibited.
- No Agency Data shall be transmitted to or from a non-Agency email address without prior approval of the CISO.
- Email must never be used while logged into an administrator account. A non-administrator account must be used instead.

All messages will be archived and will be subject to North Carolina Public Records law. N.C.G.S. §132 defines public records as "documents, papers, letters… regardless of physical form or characteristics, made or received . . . in connection with the transaction of public business. . ." (emphasis added). Email, text messages, and messages related to public business may be disclosed to third parties.

Identification and Authentication Policy

Purpose

The purpose of this policy is to ensure that processes are implemented to identify and authenticate Agency users and users working on behalf of the Agency as well as associate the unique id with transactions and processes performed by those users.

Scope

This policy applies to all Agency Staff, Resources, and Data (both physical and logical).

Policy

It is the policy of the Agency that users of Agency Data or Resources will be assigned a unique identifier that will be used to authenticate the user to the Resource they are being granted access to.

Required Procedural Elements

Identification and Authentication (Organizational Users)

NCDOR will uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

NCDOR will implement multi-factor authentication for access to privileged accounts.

NCDOR will implement multi-factor authentication for access to non-privileged accounts.

NCDOR will implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:

- One of the factors is provided by a device separate from the Resource gaining access.
- The device meets Authenticator Assurance Level 2 (AAL) per NIST SP 800-63.

NCDOR will implement replay-resistant authentication mechanisms for access to privileged accounts with network access.

Device Identification and Authentication

NCDOR will uniquely identify and authenticate devices before establishing a remote or network connection.

NCDOR will authenticate all devices before establishing a remote network connection using bidirectional authentication that is cryptographically based.

Identifier Management

NCDOR will manage Resource identifiers by:

- Receiving authorization from designated Agency officials to assign an individual, group, role, service, or device identifier.
- Selecting an identifier that identifies an individual, group, role, service, or device.
- Assigning the identifier to the intended individual, group, role, service, or device.
- Preventing reuse of identifiers indefinitely

NCDOR will manage individual identifiers by uniquely identifying everyone based on the employment type (e.g., contractor, temporary, permanent employee).
NCDOR will change all default vendor-set or factory-set administrator accounts prior to implementation (e.g., during installation or immediately after installation).

Authenticator Management

NCDOR will manage Resource authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.
- Establishing initial authenticator content for any authenticators issued by the Agency.
- Ensuring that authenticators have sufficient strength of mechanism for their intended use.
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators.
- Changing default authenticators prior to first use.
- Changing or refreshing authenticators every 90 days for all user accounts and every 366 days for service accounts or when events such as loss, theft or compromise occur.
- Protecting authenticator content from unauthorized disclosure and modification.

- Requiring individuals to take, and having devices implement, specific controls to protect authenticators.
- Changing authenticators for group or role accounts when membership to those accounts' changes.

NCDOR will require the following for password-based authentication:

- Maintain a list of commonly used, expected, or compromised passwords and update the list every three (3) years and when Agency Resource passwords are suspected to have been compromised directly or indirectly.
- Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords.
- Transmit passwords only over cryptographically protected channels.
- Store passwords using an approved salted key derivation function, preferably using a keyed hash.
- Require immediate selection of a new password upon account recovery.
- Allow user selection of long passwords and passphrases, including spaces and all printable characters.
- Employ automated tools to assist the user in selecting strong password authenticators.

NCDOR will enforce the following composition and complexity rules:

- Enforce minimum password length of fourteen (14) characters.
- Enforce minimum password complexity to contain a combination of numbers, uppercase letters, lowercase letters, and special characters.
- Enforce at least one (1) character change when new passwords are selected for use.
- Store and transmit only cryptographically protected passwords.

NCDOR will enforce password lifetime restrictions:

- One (1) day minimum and 90 days maximum.
- Service accounts passwords shall expire within 366 days (inclusive).

NCDOR will adhere to the following password History/Reuse criteria:

- For all Resources: 24 generations.

- For Resources unable to implement history/reuse restriction by generations but can restrict history/reuse for a specified time, passwords shall not be reusable for a period of six (6) months.

NCDOR will allow the use of a temporary password for Resource logons with an immediate change to a permanent password.

NCDOR will train users not to use a single dictionary word as their password.

For IT devices using a personal identification number (PIN) as an authenticator for MFA, NCDOR will enforce the following requirements:

- Minimum length of eight (8) digits. If the Resource does not enforce a minimum length of 8 digits, the maximum length possible must be used.
- Enforce complex sequences (e.g., 73961548 – no repeating digits and no sequential digits).
- Do not store with Smartcards, if used.
- Do not share.

NCDOR will enforce authorized access to the corresponding private key for public key-based authentication.

NCDOR will map the authenticated identity to the account of the individual or group.

When public key infrastructure (PKI) is used:

1. NCDOR will validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information.
2. NCDOR will implement a local cache of revocation data to support path discovery and validation.

NCDOR will require developers and installers of Resource components to provide unique authenticators or change default authenticators prior to delivery and installation.

NCDOR will protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

NCDOR will ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

For biometric-based authentication, NCDOR will employ mechanisms that satisfy the following biometric quality requirements defined in NIST SP 800-63.

Authenticator Feedback

NCDOR will obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Cryptographic Module Authentication

NCDOR will implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Identification and Authentication (Non-Organizational Users)

NCDOR will uniquely identify and authenticate non-Agency users or processes acting on behalf of non-Agency users.

NCDOR will accept only external authenticators that are NIST-compliant.

NCDOR will document and maintain a list of accepted external authenticators.

NCDOR will conform to the following profiles for identity management: NIST or FICAM-issued profiles.

NCDOR will deploy identification and authentication technology consistent with the results of the e-authentication risk analysis.

Service Identification and Authentication

NCDOR will uniquely identify and authenticate Agency-defined Resource services and applications before establishing communications with devices, users, or other services or applications.

Re-Authentication

NCDOR will require users to re-authenticate when switching to a privileged user role.

Identity Proofing

NCDOR will identify proof users that require accounts for logical access to Resources based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.

NCDOR will resolve user identities to a unique individual.

NCDOR will collect, validate, and verify identity evidence.

NCDOR will require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

NCDOR will require evidence of individual identification to be presented to the registration authority.

NCDOR will require that the presented identity evidence be validated and verified through NIST SP 800-63 compliant methods of validation and verification.

NCDOR will require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.

Media Protection Policy

Purpose

The purpose of this policy is to ensure media access is limited to only authorized individuals and that media has protections in place against unauthorized access.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that media in digital and non-digital form has protections in place that ensure that restrictions are implemented from its creation, use, storage, disposal, and sanitization.

Required Procedural Elements

Media Access

NCDOR will restrict access to digital and/or non-digital media containing Agency Data to authorized individuals.

Media Marking

NCDOR will mark Resource media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

If media is not marked or labeled, NCDOR will treat media with the highest of restrictions and handling.

NCDOR will label media containing FTI to indicate distribution limitations, proper handling, and “Federal Tax Information”. NCDOR will utilize labels from Notice 129-A and Notice 129-B for labeling purposes.

Media Storage

NCDOR will physically control and securely store digital and non-digital media containing Agency Data within Agency-controlled areas.

NCDOR will protect Resource media types containing Agency Data until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

NCDOR will utilize a combination of locked rooms, data centers, guards, reinforced perimeters, and security monitoring systems to secure media from unauthorized access.

Media Transport

NCDOR will protect and control digital and/or non-digital media containing Agency Data during transport outside of controlled areas using the following defined safeguards in accordance with IRC § 6103 (p)(4)(B) regarding secure storage and Publication 1075 SC-28 control requirements:

- Encryption
- Locked or Secured Containers
- Secured Container
- Authorized Access logs

NCDOR will maintain accountability for Resource media during transport outside of controlled areas.

NCDOR will document activities associated with the transport of Resource media utilizing a workflow tracking system.

NCDOR will restrict the activities associated with the transport of Resource media to authorized personnel.

NCDOR will require the identification of a custodian prior to transporting Resource media outside of NCDOR controlled areas.

Media Sanitization

NCDOR will sanitize digital and non-digital media containing Agency Data prior to disposal, release out of Agency control using NIST 800-88, Guidelines for Media Sanitization approved sanitization techniques and procedures.

NCDOR will employ sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

NCDOR will Review, approve, track, document, and verify media sanitization and disposal actions.

NCDOR will clear or purge any sensitive data from the system BIOS or UEFI before a computer system is disposed of and leaves the Agency. Reset the BIOS or UEFI to the manufacturer's default profile, to ensure the removal of sensitive settings such as passwords or keys.

NCDOR will only allow media provided by foreign visitors (end users) to be loaded into an Agency Resource upon approval. The Resource must remain standalone until such time as it is sanitized. Additionally, no other media loaded into the standalone system can be loaded into a non-standalone Agency Resource until sanitized.

Media Use

NCDOR will prohibit the use of personally owned media on Agency Resources or Resource components.

NCDOR will prohibit the use of portable storage devices in Agency Resources when such devices have no identifiable owner.

NCDOR prohibits the connection of non-Agency portable storage devices.

NCDOR will implement data loss prevention and protections against the use of USB storage devices.

MFD and HVP Minimum Protections Policy

Purpose

The purpose of this policy is to ensure that minimum protection standards are implemented to address not only the physical security of MVD and HVP but to address the preventive measures to ensure unauthorized access.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that minimum protections will be implemented to ensure the physical security of devices that print, fax, scan, or photocopy Agency Data and that additional security measures will be enforced to prevent unauthorized access.

All Staff must adhere to all guidelines for handling of printed Agency Data.

Required Procedural Elements

NCDOR will implement minimum protection standards to ensure a basic framework of minimal security requirements and physical protections. Standards will include the following:

- Secured Perimeters
- Security Room
- Badged Employees
- Security Containers

Secured Perimeters will be enclosed and secured with locking systems. NCDOR will maintain areas with durable construction and slab-to-slab walls. Monitoring, alarms, and intrusion detection systems will be implemented.

NCDOR will secure rooms with HVPs by limiting traffic to only those individuals with a need-to-know. The room will be constructed with non-removable or hidden door hinge pins with force resistant entry points.

NCDOR will require authorized personnel to wear picture identification badges or displayed credentials as a second barrier between unauthorized individuals and Agency Data.

NCDOR will utilize secure storage device containers that are resistant to tampering/forced penetration and have keys or combinations to control access.

MFDs and HVPs will be locked with a mechanism or encrypted with FIPS validated encryption to prevent physical access to hard drives or storage mediums that may contain stored Agency Data.

NCDOR will ensure that personnel are trained in the proper handling and disposal methods for printed Agency Data.

NCDOR will implement a managed print environment with controlled access and secure Resource configurations.

NCDOR does not allow printing of FTI to printers outside of the Agency's internal network without prior authorization from the CISO, CIO, or COO.

Mobile Device Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered and enforced when issuing and using mobile devices.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that the mobile device environment will be centrally managed to ensure that proper controls are deployed prior to accessing Agency approved applications or Agency Data using mobile devices. Mobile devices must not be operated or taken outside of the United States.

Required Procedural Elements

NCDOR will ensure mobile device management controls are in place that include security policies and procedures, inventory, and standardized configurations for all devices.

NCDOR will conduct an annual risk assessment of the security controls for all devices that receive, process, store, or transmit agency data.

NCDOR will encrypt devices and deploy a mechanism to remotely wipe a device if it is lost or stolen.

Mobile device encryption standards will meet FIPS 140 compliancy.

NCDOR administers controls to ensure that end users are limited to downloading only agency approved applications.

Mobile devices will be hardened using the latest SCSEMS prior to being deployed.

Security events will be logged and reviewed.

NCDOR will dispose of all mobile device components following media sanitization and disposal procedures.

NCDOR will include the following mobile device access controls:

- Use a secure password/PIN and/or other authentication (e.g., domain authentication or certificate-based authentication) to access Agency's Resources that contain agency data. Where capable, mobile device authentication controls will meet Pub. 1075 standards for password complexity, length, and aging.
- The device will automatically lock an account after three failed login attempts.
- The device will be set to automatically lock out as defined in IRS SCSEMS.
- Features such as swipe-based visual passwords will be disabled.
- Passwords and keys will be encrypted and not be visible in cache or logs.
- Access to the device operating system will be limited to prevent rooting/jail breaking.
- The device will be configured to ensure an individual does not have the ability to revert to the factory default setting.

NCDOR will configure the following security configurations:

- Perform risk assessments on third party applications before permitting their use.

- Ensure that apps are from only trusted entities and that code has not been modified.
- Maintain a blacklist or whitelist of agency applications that can or cannot be installed on the device.
- Maintain an approved partitioned application environment for users.
- Ongoing mobile device monitoring.
- Antimalware protection.
- Ensure devices ae kept up to date.

NCDOR will provide the following details of the mobile device environment on a quarterly basis to the Joint Legislative Oversight Committee on Information Technology, the Fiscal Research Division, and the Office of the State Chief Information Officer (CIO) to satisfy S.L. 2013-360 Section 7.18(a) and 7.18(b):

- Changes to agency policy on the use of mobile devices.
- The number and types of new devices issued since the last report.
- The total number of mobile devices issued by the agency.
- The total cost of mobile devices issued by the agency.
- The contracts were used to obtain the devices.

It is the policy of the North Carolina Department of Revenue that the PC Mobile Manager produce and provide a mobile device report to management who will review the list of devices provided to their staff at least annually to determine if a business need for the devices still exists.

Patch Management Policy

Purpose

The purpose of this policy is to ensure that a set of guidelines and procedures are followed to ensure that software, hardware, and Agency Resources are up to date with the latest security patches and updates.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that changes to Resources, including patches, service packs, updates, and modifications will be controlled through a formal change management process.

Required Procedural Elements

NCDOR will prioritize critical patches and updates based on high-risk vulnerabilities over those that are less critical in nature.

NCDOR will test the stability of patches prior to deployment and provide rollback procedures if an applied patch causes unexpected problems.

NCDOR will develop a patching schedule that limits the impact of slowdowns on business operations.

- Thursday – Windows workstations and OS environments
- Sunday - Windows Servers

NCDOR will rely on continuous real time scans to monitor and ensure that all patches and updates have been applied correctly.

NCDOR will take immediate action in response to threat collaboration platform alerts and manufacture recommended updates.

NCDOR will retain older versions of baseline configurations of the Resource to support rollback.

Additional considerations for patch management can be found in the Configuration Management Policy and the Resource and the Services Acquisition Policy.

Personally Identifiable Information Processing and Transparency Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered when handling PII and that assurances are in place that standards, guidelines, and procedures align with NCDOR's risk management strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that the Agency will permit the receipt of personally identifiable information only under the conditions of proper handling in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements, including IRS Publication 1075.

Required Procedural Elements

Personally Identifiable Information

NCDOR considers the following elements in determining PII:

- Name of a person with respect to whom a return is filed.
- Taxpayer mailing address.
- Taxpayer identification number
- Email addresses
- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother’s maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- All FTI Data
- Any combination of the above

NCDOR will establish, maintain, and update continually and inventory of all systems, applications, and projects that process personally identifiable information.

NCDOR will create diagrams depicting the logical flow of FTI within the Agency's network to include specific boundary protection, infrastructure devices and endpoints where FTI will be stored.

Authority to Process Personally Identifiable Information

NCDOR will restrict the access of personally identifiable information only to Staff who are authorized.

NCDOR will establish and maintain a permanent system of standardized records with respect to any request, the reason for the request and the date of the request, and any disclosure of return or return information made by or to it.

NCDOR will establish and maintain secure areas or places to store PII.

Risks to PII

NCDOR will determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

NCDOR will conduct privacy and risk impact assessments for Resources, programs, or other activities before:

- Developing or procuring information technology that processes personally identifiable information.

- Initiating a new collection of personally identifiable information that:

    1. Will be processed using information technology.
    2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

Risk Management Strategy

NCDOR will develop a comprehensive strategy to manage privacy risks to individuals resulting from the authorized processing of personally identifiable information.

PII Management and Retention

NCDOR will Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

Limit Personally Identifiable Information

NCDOR will limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment:

- Date of birth
- Place of birth
- Business telephone number
- Business mailing or email address
- Race
- Religion
- Geographical indicators
- Employment information
- Medical information
- Education information
- Financial information

NCDOR must complete submission of the DTR form for review and approval by IRS Office of Safeguards to comply with FTI PII requirements.

Training

NCDOR will provide training to systems users on the proper handling of PII and the techniques needed to protect PII that is entrusted to the Agency.

Disclosures

NCDOR will adhere to IRC § 6103 and only use FTI for an authorized use and will not use information in any manner of for any purpose not consistent with that authorized use.

NCDOR will develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

- Date, nature, and purpose of each disclosure.
- Name and address, or other contact information of the individual or organization to which the disclosure was made.
- Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made.
- Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Safeguards Security Report (SSR)

NCDOR will report to the IRS Office of Safeguards processes, procedures, security, and privacy controls that are in place for protecting PII related to FTI.

Security and Privacy Architectures

NCDOR will develop security and privacy architectures for the Resource that:

- Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of Agency Data.
- Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.
- Describe how the architectures are integrated into and support the enterprise architecture.
- Describe any assumptions about, and dependencies on, external systems and services.
- Review and update the architecture at a minimum annually to reflect changes in the enterprise architecture.
- Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, Agency procedures, and procurements and acquisitions.

Breach Response

NCDOR will include the following in the Incident Response Plan for breaches involving personally identifiable information:

- A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.
- An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms.
- Identification of applicable privacy requirements.

Personnel Security Policy

Purpose

The purpose of this policy is to ensure that personnel security is developed and that assurances are in place that standards, guidelines, and procedures are compliant and align with NCDOR's risk management strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency to utilize a personnel security process to authorize and grant access to Resources.

Required Procedural Elements

Position Risk Designation

NCDOR will assign a risk designation to all Agency positions.

NCDOR will establish screening criteria for individuals filling those positions.

NCDOR will review and update position risk designations when recruitment actions are taken or when position descriptions are rewritten.

Personnel Screening

NCDOR will screen individuals prior to authorizing access to Agency Resources.

NCDOR will rescreen individuals no less than once every five years.

Personnel Termination

NCDOR will disable Resource access within one (1) business day.

NCDOR will terminate or revoke any authenticators and credentials associated with the individual.

NCDOR will conduct exit interviews that include a discussion of information security topics, specifically nondisclosure agreements.

NCDOR will retrieve all security-related Agency Resource-related property.

NCDOR will retain access to Agency information and Resources formerly controlled by terminated individual.

Personnel Transfer

NCDOR will review and confirm ongoing operational need for current logical and physical access authorizations to Resources and facilities when individuals are reassigned or transferred to other positions within the Agency.

NCDOR will initiate transfer or when warranted extended reassignment actions within five (5) business days of the formal transfer action.

NCDOR will modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

NCDOR will notify designated Agency personnel of transfers within five (5) business days.

Access Agreements

NCDOR will develop and document access agreements for Agency Resources.

NCDOR will review and update the access agreements at a minimum annually.

NCDOR will verify that individuals requiring access to Agency information and Resources:

- Sign appropriate access agreements prior to being granted access.
- Re-sign access agreements to maintain access to Resources when access agreements have been updated or at a minimum annually.

NCDOR will notify individuals of applicable, legally binding post-employment requirements for protection of Agency Data.

NCDOR will require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

External Personnel Security

NCDOR will establish personnel security requirements, including security roles and responsibilities for external providers.

NCDOR will require external providers to comply with personnel security policies and procedures established by the Agency.

NCDOR will document personnel security requirements.

NCDOR will require external providers to notify designated Agency personnel of any personnel transfers or terminations of external personnel who possess Agency credentials and/or badges, or who have Resource privileges within three (3) business days.

NCDOR will monitor provider compliance with personnel security requirements.

Personnel Sanctions

NCDOR will employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures.

NCDOR will notify designated Agency personnel within 72 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Position Descriptions

NCDOR will incorporate security and privacy roles and responsibilities into Agency position descriptions.

Physical and Environmental Protection Policy

Purpose

The purpose of this policy is to ensure that physical and environmental protections are implemented, and controls are administered that create defenses for unauthorized access.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that NCDOR will protect Agency Data from unauthorized disclosure by establishing physical and environmental controls for areas that contain critical Resources that maintain, transmit, store, or create Agency Data.

NCDOR will develop policy and procedures as needed to address their specific building access systems (e.g., restriction of physical access, identification and authentication and audit logging), that are critical to the security of a facility.

NCDOR will develop and implement a clean desk policy for the protection of Agency Data (e.g., paper output, electronic storage media) to preclude unauthorized disclosures.

NCDOR will designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals, and communications equipment.

Required Procedural Elements

Physical Access Authorizations

NCDOR will develop, approve, and maintain active lists of individuals with authorized access to NCDOR Facilities where Agency Data resides. The following will be included as a part of the authorization process:

1. Automated workflows will be created to assist in streamlining operations and logging authorizations.
2. Authorization credentials will be issued for facility access in the form of badges and keys depending on the area's controls and the individuals' roles/responsibilities and need-to-know.
3. Access lists detailing authorized facility access will be reviewed annually.
4. Access authorizations will be removed when access is no longer required.

Physical Access Controls

NCDOR will enforce physical access authorizations at entry/exit points to facilities where Resources that receive, process, store, access, or transmit Agency Data by:

1. Approving and verifying authorizations before granting access to Agency Facilities; and
2. Controlling ingress and egress to the facility using badging, key fobs, and key entry depending on the physical structure and the individuals need-to-know.

NCDOR will maintain logs and conduct audits on entry or exit points that are isolated from the general user population due to the sensitivity of the data or the criticality of the Resource.

NCDOR will control access to areas deemed publicly accessible by implementing the following controls:

1. Dedicated reception areas requiring screening for further entry.
2. North Carolina State Police
3. Locked doors to entries to back-office locations
4. Door signage stating employees only.
5. Cameras

6. Approvals in the form of appointments with a requirement for an NCDOR point of contact.

NCDOR will require an escort and controls will be implemented to control visitor activity that complies with all relevant department policies.

NCDOR will physically secure all keys, combinations, and badging.

NCDOR will conduct an inventory every twelve (12) months of badge card readers, locks, and keys.

NCDOR will change combinations, cipher codes, combinations, locks, and keys when individuals are transferred or terminated or if an entry point has been compromised.

NCDOR will perform security checks daily of physical perimeters (maybe by third parties) to ensure no signs of exfiltration of information or removal of Resource components.

Access Control for Transmission

NCDOR will control access to physical locations that contain transmission hubs or areas that exchange or distribute information digitally.

Access Control for Output Devices

NCDOR will control physical access to monitors, printers, and audio devices that might be accessed by an individual not authorized to do so. NCDOR will utilize locked rooms or entry points that limit user access.

Monitoring Physical Access

NCDOR will monitor physical access to locations deemed restricted and areas that require protection of Agency Data. When physical security incidents are suspected, they will be handled through the Agency incident management processes and procedures.

Access logs will be reviewed monthly or on upon an indication of a security event.

Review and investigation will be in coordination with incident response capabilities.

NCDOR will utilize intrusion alarm and surveillance systems to monitor physical access.

NCDOR will create restricted areas, security rooms, or locked rooms for preventing unauthorized access to areas that contain Agency Data during duty and non-duty hours.

All restricted areas will require secured area criteria or provision to properly store Agency Data in appropriate containers during non-duty hours.

NCDOR will follow guidance from IRS Safeguards Publication 1075 Section 2.B.3 on the required controls needed to be implemented to qualify as a “restricted area”.

Visitor Access Records

NCDOR will maintain records for 5 years related to visitor access where Resources receive, process, store, protect, or transmit Agency Data.

Access records will be reviewed monthly.

Anomalies in visitor access will be reported to physical security for further review.

NCDOR will maintain a visitor access log at a designated entrance to a restricted area and all visitors (persons not assigned to the area) entering the area will be directed to the designated entrance.

The visitor access log will require the visitor to provide the following information:

- Name and organization of the visitor
- Signature of the visitor
- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and organization of person visited.

Authorization for entry will be granted after the appropriate personnel validate the person’s identity by examining government-issued identification (e.g., state driver’s license or passport) and compare the name and signature entered in the access log with the name and signature of the government-issued identification.

NCDOR requires that all visitors enter their time of departure.

NCDOR will review restricted area access logs at the end of each month and retain the logs for a period of 5 years.

Additional requirements can be found in IRS Publication 1075, 2.B.3.2, Authorized Access List for visitor access (AAL).

Delivery and Removal

NCDOR will control Resource components that receive, store, process, and transmit Agency Data that enter and exit the facility by requiring authorizations from Resource Owners and security.

NCDOR will maintain records for Resources that enter or exit the facility.

Alternate Work Site

NCDOR will determine and document the Agency permitted alternate work sites allowed for use by employees.

NCDOR will employ security and privacy controls at alternate work sites.

NCDOR will assess the effectiveness of security and privacy controls at alternated work sites.

NCDOR will deploy communication protocols to ensure that employees are aware of who needs to be contacted in the event of a security or privacy related incident.

NCDOR will require that teleworking sites adhere to the same physical security for computers, electronic and removable media including:

- Secure areas with restricted access to Agency-Data.
- If the requirements for secure access cannot be maintained, equipment authorized for use must have the highest level of protection practical, including full disk encryption.
- Basic security requirements for locking Agency data when not in use.
- Encrypting and labeling removable media.

NCDOR will maintain an inventory record of computers, electronic and removable media and conduct a review of the record semi-annually.

Planning Policy

Purpose

The purpose of this policy is to ensure procedures are implemented to facilitate security and privacy planning for the NCDOR technical ecosystem.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that protections for the confidentiality, integrity, and availability of the technical architecture are evaluated pre-deployment and are a part of the planning process for future integration and new technologies.

Required Procedural Elements

Resource Security and Privacy Plans

NCDOR will provide an accurate Safeguards Security Report (SSR) to satisfy requirements related to security and privacy planning. NCDOR will submit the SSR on an annual basis after the initial receipt of FTI.

NCDOR will include, in the planning stage, media sanitization and disposition requirements addressing all Resource media and backups related to the Resource.

Rules of Behavior

NCDOR will establish and provide to individuals requiring access to the Resource, the rules that describe their responsibilities and expected behavior for information and Resource usage, security, and privacy.

NCDOR will receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to Agency Data and Resources.

NCDOR will review and update the rules of behavior at a minimum annually.

NCDOR will require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

NCDOR will include in the rules of behavior, restrictions on:

- Use of social media, social networking sites, and external sites/applications.
- Posting Agency information on public websites.
- Use of Agency-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

NCDOR will provide guidance for the proper use of Internet-supported technologies (e.g., Instant Messaging).

Security and Privacy Architectures

NCDOR will develop security and privacy architectures for the Resource that:

- Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of Agency Data.
- Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.
- Describe how the architectures are integrated into and support the enterprise architecture.
- Describe any assumptions about, and dependencies on, external systems and services.

NCDOR will Review and update the architectures at a minimum annually to reflect changes in the enterprise architecture.

NCDOR will reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, Agency procedures, and procurements and acquisitions.

NCDOR will design the security and privacy architectures for the Resource using a defense-in- depth approach that:

- Allocates Resource communication and other relevant controls to Agency Resources processing, storing, and transmitting Agency Data.
- Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

Privacy Policy

Purpose

The purpose of this policy is to provide guidelines for the creation of a privacy program that defines the use of PII and methods the Agency utilizes to control risks associated with handling personal information.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that no personal identifiable information shall be collected, used, or shared except as necessary to fulfill the mission of the Agency and shall protect all data as defined in North Carolina General Statute 105-259.

Required Procedural Elements

Authority to Collect

NCDOR has the legal authority that permits the collection, use, maintenance and sharing of personally identifiable information per North Carolina General Statue 105-259.

Privacy Program Leadership

The NCDOR CIO has the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the Agency-wide privacy program.

Governance

NCDOR will develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, Resources, or technologies involving PII and in compliance with NCGS 105-259.

Privacy Impact and Risk Assessment

NCDOR will conduct privacy impact assessments for new Resources, major changes to Resources, or upon initiation of a new collection of PII that includes risks to the privacy of individuals resulting from the collection, sharing, storing, transmission, use, and disposal of PII.

Accounting of Disclosures

Per NCGS 105-259 an officer, an employee, or an agent of NCDOR who has access to tax information in the course of service to or employment by the State may not disclose the information to any other person except as provided in subsection 105-259(b).

Data Quality and Integrity

NCDOR will collect PII as needed regardless of the accuracy, relevance, timeliness, and completeness of that information.

NCDOR will limit the collection and retention of PII as required by NCGS105-259.

NCDOR will dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with an Agency-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

Program Management Policy

Purpose

The purpose of this policy is to ensure guidance is provided to Agency personnel for the creation and implementation of an information security program that meets and/or exceeds the requirements of Internal Revenue Code (IRC) § 6103 (p)(4) and guidance as provided by IRS Publication 1075.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that information security will follow a recognized regulatory framework that follows IRS guidance and adheres to all applicable regulatory requirements.

Required Procedural Elements

Information Security Program Leadership Role

NCDOR will appoint a senior Agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an Agency-wide information security program.

Information Security and Privacy Resources

NCDOR will include the Resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement.

NCDOR will prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards.

NCDOR will make available for expenditure, the planned information security and privacy Resources.

Plan of Action and Milestones Process

NCDOR will implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated Agency Resources which includes the following:

NCDOR will ensure that plans are developed and maintained.

NCDOR will document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to Agency operations and assets, individuals, other organizations, and the Nation.

NCDOR will report Plan of Actions and Milestones (POA&M) progress in accordance with established reporting requirements.

NCDOR will review plans of action and milestones for consistency with the Agency risk management strategy and Agency-wide priorities for risk response actions.

Resource Inventory

NCDOR will develop and update continually an inventory of Agency Resources.

NCDOR will establish, maintain, and update continually an inventory of all Resources and projects that process personally identifiable information.

Enterprise Architecture

NCDOR will develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to Agency operations and assets, individuals, other organizations, and the Nation.

NCDOR will review and update the security enterprise architecture data based on the enterprise architecture timeframes.

Risk Management Strategy

NCDOR will develop a comprehensive strategy to manage:

- Security risk to Agency operations and assets, individuals, other organizations, and the Nation associated with the operation and use of Agency Resources.
- Privacy risk to individuals resulting from the authorized processing of personally identifiable information.

NCDOR will implement the risk management strategy consistently across the Agency.

NCDOR will review and update the risk management strategy every three (3) years or as required, to address Agency changes.

Authorization Process

NCDOR will manage the security and privacy state of Agency Resources and the environments in which those Resources operate through authorization processes.

NCDOR will designate individuals to fulfill specific roles and responsibilities within the Agency risk management process.

NCDOR will integrate the authorization processes into an Agency-wide risk management program.

Insider Threat Program

NCDOR will implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Testing, Training and Monitoring

NCDOR will implement a process for ensuring that Agency plans for conducting security and privacy testing, training, and monitoring activities associated with Agency Resources:

Are developed and maintained; and

Continue to be executed; and

NCDOR will review testing, training, and monitoring plans for consistency with the Agency risk management strategy and Agency-wide priorities for risk response actions.

Privacy Program Plan

NCDOR will establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted

on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.

NCDOR will review and update the policy and procedures every three (3) years or when there is a significant change.

Privacy Program Leadership Role

NCDOR will appoint a senior Agency official for privacy with the authority, mission, accountability, and Resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the Agency-wide privacy program.

Accounting of Disclosures

NCDOR will develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

- Date, nature, and purpose of each disclosure.
- Name and address, or other contact information of the individual or organization to which the disclosure was made.

NCDOR will retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer.

NCDOR will make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Risk Management Program Leadership Roles

NCDOR will appoint a Senior Accountable Official for Risk Management to align Agency information security and privacy management processes with strategic, operational, and budgetary planning processes.

NCDOR will establish a Risk Executive (function) to view and analyze risk from an Agency-wide perspective and ensure management of risk is consistent across the organization.

Resource and Communications Protection Policy

Purpose

The purpose of this policy is to ensure that that information in transit internally and/or externally is protected.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that Resources will have protections in place to ensure that information transmitted internally and externally remains confidential.

Required Procedural Elements

Application Partitioning

NCDOR will separate user functionality, including user interface services, from Resource management functionality.

NCDOR will prevent the presentation of Resource management functionality at interfaces to non-privileged users.

Information in Shared System Resources

NCDOR will prevent unauthorized and unintended information transfer via shared system resources.

Boundary Protection

NCDOR will monitor and control communications at the external managed interfaces to the Resource and at key internal managed interfaces within the Resource.

NCDOR will implement subnetworks for publicly accessible Resource components that are physically and logically separated from internal Agency networks.

NCDOR will connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an Agency security and privacy architecture.

NCDOR will limit the number of external network connections to the Resource.

NCDOR will implement a managed interface for each external telecommunication service.

NCDOR will establish a traffic flow policy for each managed interface.

NCDOR will protect the confidentiality and integrity of the information being transmitted across each interface.

NCDOR will document each exception to the traffic flow policy with a supporting mission or business need and duration of that need.

NCDOR will review exceptions to the traffic flow policy at a minimum quarterly and remove exceptions that are no longer supported by an explicit mission or business need.

NCDOR will prevent unauthorized exchange of control plane traffic with external networks.

NCDOR will publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.

NCDOR will filter unauthorized control plane traffic from external networks.

NCDOR will deny network communications traffic by default and allow network communications traffic by exception on Resources where Agency Data is accessed, processed, stored, or transmitted.

NCDOR will prevent split tunneling for remote devices connecting to Agency Resources unless the split tunnel is securely provisioned using:

- Individual users shall not have the ability to configure split tunneling.
- Auditing must be performed semi-annually on each workstation with split tunneling enabled. Auditing must include:
    1. Only those users authorized for split tunneling have it enabled in their user profile or policy object.
    2. There is a continued need for split tunneling for the user.
    3. Only the correct and authorized split tunneling configurations are present on the workstation.
- Host Checking is enabled and configured on the VPN server:

1. Ensure the OS is supported.
2. Ensure that anti-malware is installed and up to date.
3. The most current hotfixes are applied.
4. Agency-defined additional parameters.

NCDOR will route internal communications traffic to external networks through authenticated proxy servers at managed interfaces.

NCDOR will detect and deny outgoing communications traffic posing a threat to external systems.

NCDOR will audit the identity of internal users associated with denied communications.

NCDOR will prevent the exfiltration of information.

NCDOR will conduct exfiltration tests at least semi-annually.

NCDOR will only allow incoming network communications from CISO authorized sources to be routed to CISO authorized destinations.

NCDOR will implement firewalls and intrusion detection systems at access points and end user equipment as appropriate.

NCDOR will route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

NCDOR will enforce adherence to protocol formats.

NCDOR will prevent Resources from entering unsecure states in the event of an operations failure of a boundary protection area.

NCDOR will implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary will be monitored and communications across each boundary will be controlled.

NCDOR will block known malicious sites (inbound or outbound), as identified to the Agency from US-CERT, MS-ISAC, or other sources, at each Internet Access Point (unless explicit instructions are provided to agencies not to block specific sites). NCDOR will block known malicious sites within two business days following release.

Transmission Confidentiality and Integrity

NCDOR will protect the confidentiality and integrity of transmitted information.

NCDOR will implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

NCDOR will ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over video and voice telecommunication and teleconferences.

Network Disconnect

NCDOR will terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

Cryptographic Key Establishment and Management

NCDOR will establish and manage cryptographic keys when cryptography is employed within the Resource in accordance with the following key management requirements: NIST SP 800-57, Recommendation for Key Management, for key generation, distribution, storage, access, and destruction.

Cryptographic Protection

NCDOR will determine the cryptographic uses needed to protect Agency Data in transit, storage, and rest.

NCDOR will implement the latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). NCDOR prohibits the use of SHA-1 for digital signatures.

Collaborative Computing Devices and Applications

NCDOR will prohibit remote activation of collaborative computing devices and applications with the following exceptions: users are notified by signage of the presence of such devices.

NCDOR will provide an explicit indication of use to users physically present at the devices.

NCDOR will provide an explicit indication of current participants in meetings that involve Agency Data.

Public Key Infrastructure Certificates

NCDOR will issue public key certificates under a CISO defined certificate authority or obtain public key certificates from an approved service provider.

NCDOR will include only approved trust anchors in trust stores or certificate stores managed by the Agency.

Mobile Code

NCDOR will define acceptable and unacceptable mobile code and mobile code technologies.

NCDOR will authorize, monitor, and control the use of mobile code within the Resource.

NCDOR will identify unacceptable mobile code and take corrective actions.

NCDOR will verify that the acquisition, development, and use of mobile code to be deployed in the Resource meets IRS Publication 1075 requirements.

Secure Name/Address Resolution Service (Authoritative Source)

NCDOR will provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

NCDOR will provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

NCDOR will provide data origin and integrity protection artifacts for internal name/address resolution queries.

Secure Name/Address Resolution Service (Recursive or Caching Resolver)

NCDOR will request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Architecture and Provisioning for Name/Address Resolution Service

NCDOR will ensure the Resources that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Session Authenticity

NCDOR will protect the authenticity of communications sessions.

NCDOR will invalidate session identifiers upon user logout or other session termination.

NCDOR will generate a unique session identifier for each session with session with policy defined randomness requirements and recognize only session identifiers that are system generated.

NCDOR will only allow the use of CISO approved certificate authorities for verification of the establishment of protected sessions.

Protection of Information at Rest

NCDOR will protect the confidentiality and integrity of Agency Data that is no longer accessed or requires an extended retention period.

NCDOR will implement cryptographic mechanisms to prevent unauthorized disclosure and modification of Agency Data at rest on end user Resources (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage.

External Malicious Code Identification

NCDOR will include Resource components that proactively seek to identify network-based malicious code or malicious websites.

Process Isolation

NCDOR will maintain a separate execution domain for each executing Resource process.

Resource Time Synchronization

NCDOR will synchronize Resource clocks within and between Resources and Resource components.

NCDOR uses state provided clocks.

NCDOR does not use internal Resource clocks.

Resource and Information Integrity Policy

Purpose

The purpose of this policy is to ensure Resources and information are monitored and evaluated to ensure overall integrity.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that Agency Data and Resources will be validated to ensure overall integrity from non-tampering, malicious damage, or human error.

Required Procedural Elements

Flaw Remediation

NCDOR will identify, report and correct Resource flaws.

NCDOR will test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

NCDOR will install security-relevant software and firmware updates promptly after the release of the updates.

NCDOR will incorporate flaw remediation into the Agency configuration management process.

NCDOR will determine if Resource components have applicable security relevant software and firmware updates installed using automated mechanisms at a minimum monthly, daily for networked workstations and malicious code protection.

NCDOR will measure the time between flaw identification and flaw remediation.

NCDOR will utilize the following benchmarks for taking corrective actions:

- Criticality of flaws and impact on the NCDOR architecture.

- Availability of stable fix or patch
- Impact of applying fix without prior testing

NCDOR will employ automated patch management tools to facilitate flaw remediation to all Agency Resources that includes but not limited to mainframes, workstations, applications, and network components.

NCDOR will install security-relevant software and firmware updates automatically to all Agency Resources.

NCDOR will remove previous versions of security relevant software and firmware components after updated versions have been installed.

NCDOR will ensure that, upon daily power up and connection to the Agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent Agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every 24 hours (excluding weekends, holidays, etc.)

Malicious Code Protection

NCDOR will implement signature-based and/or non-signature-based malicious code protection mechanisms at Resource entry and exit points to detect and eradicate malicious code.

NCDOR will automatically update malicious code protection mechanisms as new releases are available in accordance with Agency configuration management policy and procedures.

NCDOR will configure malicious code protection mechanisms to:

1. Perform periodic scans of the Resource and implement 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.
2. Either block or quarantine take and send alert to Resource Owners in response to malicious code detection.

NCDOR will address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the Resource.

NCDOR will scan removable media for malicious code upon introduction of the media into any Resource on the network and before users may access the media.

NCDOR will not less than daily, check for updates to malicious code scanning tools, including anti-virus (AV) and anti-spyware software and intrusion detection tools and when updates are available, implement them on all devices on which such tools reside.

Resource Monitoring

NCDOR will monitor the Resource to detect:

- Attacks and indicators of potential attacks in accordance with the following monitoring objectives:
    - Defined IT Security monitoring objectives; and
    - Unauthorized local, network, and remote connections.

NCDOR will identify unauthorized use of the Resource through a variety of techniques and methods.

NCDOR will invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the Resource to collect Agency-determined essential information.
2. At ad hoc locations within the Resource to track specific types of transactions of interest to the Agency.

NCDOR will analyze detected events and anomalies.

NCDOR will adjust the level of Resource monitoring activity when there is a change in risk to Agency operations and assets, individuals, other organizations, or the Nation.

NCDOR will obtain legal opinion regarding Resource monitoring activities.

NCDOR will provide the output from Resource monitoring to designated Agency officials at a minimum every two weeks or sooner if deemed necessary.

NCDOR will connect and configure individual intrusion detection tools into a Resource-wide intrusion detection system.

NCDOR will employ automated tools and mechanisms to support near real-time analysis of events.

NCDOR will determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.

NCDOR will monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.

Agency staff will alert the appropriate Agency personnel when the following Resource generated indications of compromise or potential compromise occur:

- Suspicious activity reported from firewalls.
- Intrusion detection Resources.
- Malware detection Resources.
- Endpoint protection Resources.
- Security Information Event Manager
- Third party event alerting solutions.

NCDOR will make provisions so that internal encrypted traffic and encrypted traffic being transmitted to external resources is visible to endpoint protection monitoring and relevant AI/Machine learning security solutions.

NCDOR will analyze outbound communications traffic at the external interfaces to the Resource and selected Agency defined interior points within the Resource to discover anomalies.

IT Security, IT Operations, the CIO, CISO, or designee will be alerted using automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur:

- Suspicious Activity Report
- Reports of potential insider threat
- Active intrusion detection
- Data loss or breach

NCDOR will analyze outbound communications traffic at external interfaces to the Resource and at the following interior points to detect covert exfiltration of information:

- At IT Security-defined interior points within the Resource.

IT Security will discover, collect, and distribute to the CIO or CISO indicators of compromise provided by government and non-government sources.

All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the Agency CISO.

Security Alerts, Advisories and Directives

NCDOR will receive Resource security alerts, advisories, and directives from third parties such as US-CERT, MS-ISAC, product vendors, etc. on an ongoing basis.

NCDOR will generate internal security alerts, advisories, and directives as deemed necessary.

NCDOR will disseminate security alerts, advisories, and directives to appropriate personnel with security responsibilities (e.g., system administrators, ISSOs, Resource Owners, incident response capabilities, etc.).

NCDOR will implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

Software, Firmware, and Information Integrity

NCDOR will employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: system kernels, drivers, firmware (e.g., BIOS, UEFI), software (e.g., OS, applications, middleware) and security attributes.

NCDOR will immediately disconnect the device from the network and notify designated Agency officials when unauthorized changes to the software, firmware, and information are detected.

NCDOR will perform an integrity check of software, firmware, and information at startup; at the identification of a new threat to which the Resource is susceptible; the installation of new hardware, software, or firmware; or at a minimum annually.

NCDOR will incorporate the detection of the following unauthorized changes into the Agency incident response capability:

- Unauthorized changes to baseline configuration setting; and
- Unauthorized elevation of Resource privileges.

NCDOR will verify the checksum of downloaded firmware to protect the integrity of boot firmware in the Resources where Agency Data is accessed, processed, stored, and transmitted.

NCDOR will employ spam protection mechanisms at Resource entry and exit points to detect and act on unsolicited messages.

NCDOR will update spam protection mechanisms when new releases are available in accordance with Agency configuration management policy and procedures.

NCDOR will automatically update spam protection mechanisms at a minimum quarterly.

Information Input Validation

NCDOR will check the validity of information inputs. (e.g., character set, length, numerical range, acceptable values).

Error Handling

NCDOR will generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

NCDOR will reveal error messages only to designated Agency officials.

Information Management and Retention

NCDOR will manage and retain information within the Resource and information output from the Resource in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

NCDOR will submit the DTR form for review and approval by the IRS Office of Safeguards to minimize the use of personally identifiable information for research, testing, or training.

Memory Protection

NCDOR will implement hardware-based or software-based data execution prevention to protect the Resource memory from unauthorized code execution.

Resource and Services Acquisition Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered when developing the Resource and service acquisition program and that assurances are in place that standards, guidelines, and procedures align with NCDOR's risk management strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that a service and resources acquisition process is implemented to ensure security and privacy controls are considered throughout the entire Resource life cycle.

Required Procedural Elements

Allocation of Resources

NCDOR will determine the high-level information security and privacy requirements for the Resource or Resource service in mission and business process planning.

NCDOR will determine, document, and allocate the resources required to protect the Resource or Resource service as part of the Agency capital planning and investment control process.

NCDOR will establish a discrete line item for information security and privacy in Agency programming and budgeting documentation.

System Development Life Cycle

NCDOR will acquire, develop, and manage the Resource using an Agency system development life cycle that incorporates information security and privacy considerations.

NCDOR will define and document information security and privacy roles and responsibilities throughout the system's development lifecycle (SDLC).

NCDOR will identify individuals having information security and privacy roles and responsibilities.

NCDOR will integrate the Agency information security and privacy risk management process into SDLC activities.

NCDOR will approve, document, and control the use of live data in preproduction environments for the Resource, Resource component, or Resource service.

NCDOR will protect preproduction environments for the Resource, Resource component, or Resource service at the same impact or classification level as any live data in use within the preproduction environments.

Acquisition Process

NCDOR will include the following requirements, descriptions, and criteria, explicitly or by reference, using State procurement contract language where provided and IRS Exhibit 7 or Agency equivalent of IRS Exhibit 7 in the acquisition contract for the Resource, Resource component, or Resource service.

NCDOR will require the developer of the Resource, Resource component, or Resource service to provide a description of the functional properties of the controls to be implemented.

NCDOR will require the developer of the Resource, Resource component, or Resource service to provide design and implementation information for the controls that includes:

- security-relevant external Resource interfaces
- high-level design; low-level design
- source code or hardware schematics
- design and implementation information for the security controls to be employed at sufficient level of detail to permit analysis and testing of controls.

NCDOR will require the developer of the Resource, Resource component, or Resource service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the Agency.

NCDOR will require the developer of the Resource, Resource component, or Resource service to identify the functions, ports, protocols, and services intended for Agency use.

NCDOR will include Agency Data ownership requirements in the acquisition contract.

NCDOR will require all Agency Data to be removed from the contractor's systems and returned to the Agency within 7 calendar days prior to contract termination.

NCDOR requires that Resources that receive, process, store, access, protect and/or transmit Agency Data must be located, operated, and accessed within the United States. When a contract developer is used, agencies must document, through contract requirements, that all Agency Resources (i.e., beyond commercial products used as components) are located within the United States and are developed physically within the United States by United States citizens or those with lawful resident status.

NCDOR will use common security configurations, when applicable, by (a) requiring vendors to configure IT with common security configurations (when available and applicable, e.g., Center for Internet Security benchmarks) prior to delivery or (b) configuring acquired IT to meet Agency-tailored, secure parameters (e.g., configurations that meet Publication 1075 and applicable SCSEM requirements) after delivery but prior to deployment.

Resource Documentation

NCDOR will obtain or develop administrator documentation for the Resource, Resource component, or Resource service that describes:

- Secure configuration, installation, and operation of the Resource, component, or service.
- Effective use and maintenance of security and privacy functions and mechanisms.
- Known vulnerabilities regarding configuration and use of administrative or privileged functions.

NCDOR will obtain or develop user documentation for the Resource, Resource component, or Resource service that describes:

- User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms.
- Methods for user interaction, which enables individuals to use the Resource, component, or service in a more secure manner and protect individual privacy.
- User responsibilities in maintaining the security of the Resource, component, or service and privacy of individuals.

NCDOR will document attempts to obtain Resource, Resource component, or Resource service documentation when such documentation is either unavailable or nonexistent and the CIO or COO will determine whether to accept the risk or not.
NCDOR will distribute documentation to designated Agency officials.

Security Engineering Principles

NCDOR will apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the Resource and Resource components:

- Resource upgrades and modifications.
- Layered protections.
- Security and Privacy Policies.
- Architecture and control design and development.
- Physical and logical security boundaries.
- Design patterns and compensating controls.

External System Services

NCDOR will require that providers of external system services comply with Agency security and privacy requirements and employ the following controls: the security and privacy requirements contained within this policy and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements.

NCDOR will define and document Agency oversight and user roles and responsibilities regarding external system services.

NCDOR will employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: continuous

monitoring activities (e.g., perform internal inspections, complete self-assessments using SCSEM, perform automated configuration compliance scans, etc.)

NCDOR will conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services.

NCDOR will verify that the acquisition or outsourcing of dedicated information security services is approved by a designated Agency official.

NCDOR will require providers of external information system services that process, store, or transmit Agency Data to identify the functions, ports, protocols, and other services required for the use of such services.

NCDOR will establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit Agency Data.

NCDOR will restrict the location of accessing, processing, storage, transmission of Agency Data to The U.S. and territories based on IRS Publication 1075 requirements.

NCDOR will maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

NCDOR will restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

Developer Configuration Management

NCDOR will require the developer of the Resource, Resource component, or Resource service to:

- Perform configuration management during Resource, Resource component, or Resource service: design, development, implementation, and operation and disposal.
- Document, manage, and control the integrity of changes to configuration items under configuration management.
- Implement only Agency-approved changes to the Resource, Resource component, or Resource service.

- Document approved changes to the Resource, Resource component, or Resource service and the potential security and privacy impacts of such changes.
- Track security flaws and flaw resolution within the Resource, Resource component, or Resource service and report findings to the designated Agency official.

NCDOR will require the developer of the Resource, Resource component, or Resource service to enable integrity verification of software and firmware components.

NCDOR will require the developer of the Resource, Resource component, or Resource service to enable integrity verification of hardware components.

NCDOR will require Agency designated security and privacy representatives to be included in the configuration change management and control process.

Developer Testing and Evaluation

NCDOR will require the developer of the Resource, Resource component, or Resource service, at all post-design stages of the system development life cycle, to:

- Develop and implement a plan for ongoing security and privacy assessments.
- Perform Resource testing/evaluation at the depth of one or more of the following: security-related functional properties, security-related externally visible interfaces, high-level design, low-level design and/or implementation representation (i.e., source code and hardware schematics) at all post-design phases of the SDLC.
- Produce evidence of the execution of the assessment plan and the results of the testing and evaluation.
- Implement a verifiable flaw remediation process.
- Correct flaws identified during testing and evaluation.

NCDOR will require the developer of the Resource, Resource component, or Resource service to employ static code analysis tools to identify common flaws and document the results of the analysis.

NCDOR will require the developer of the Resource, Resource component, or Resource service to perform a manual code review of Agency Data-related applications using the

following processes, procedures, and/or techniques: CISO defined manual review process.

NCDOR will require the developer of the Resource, Resource component, or Resource service to perform penetration testing:

- At the following level of rigor: at a minimum Whitebox testing.
- Under the following constraints: where Agency Data is processed, stored, or transmitted.

NCDOR will require the developer of the Resource, Resource component, or Resource service to perform attack surface reviews.

Development Process, Standards and Tools

NCDOR will require the developer of the Resource, Resource component, or Resource service to follow a documented development process that:

- Explicitly addresses security and privacy requirements.
- Identifies the standards and tools used in the development process.
- Documents the specific tool options and tool configurations used in the development process.
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

NCDOR will review the development process, standards, tools, tool options, and tool configurations at a minimum annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: IRS Publication 1075 security and privacy requirements.

NCDOR will require the developer of the Resource, Resource component, or Resource service to perform a criticality analysis:

- At the following decision points in the system development life cycle:
    1. Design
    2. Delivery
    3. Integration
    4. Maintenance
- At the following level of rigor: post-design phases of the SDLC.

Unsupported Resource Components

NCDOR will replace Resource components when support for the component is no longer available from the developer, vendor, or manufacturer.

NCDOR will provide the following options for alternative sources for continued support for unsupported components: Extended security support agreement that include security software patches and firmware updates from an external source for each unsupported component.

Resource Maintenance Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered when developing the Resource maintenance program and that assurances are in place that standards, guidelines, and procedures align with NCDOR's risk management strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency to establish controls for the maintenance, repair, and replacement of Resources within a secure and monitored environment.

Required Procedural Elements

Controlled Maintenance

NCDOR will schedule, document, and review records of maintenance, repair, and replacement on Resource components in accordance with manufacturer or vendor specifications and/or Agency requirements.

NCDOR will approve and monitor all maintenance activities, whether performed on site or remotely and whether Resource or Resource components are serviced on site or removed to another location.

NCDOR will require that designated Agency officials explicitly approve the removal of the Resource or Resource components from Agency facilities for off-site maintenance, repair, or replacement.

NCDOR will sanitize equipment to remove all information on the equipment sanitized prior to removal from Agency facilities for off-site maintenance, repair, or replacement.

NCDOR will check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions.

NCDOR will include the following information in the Agency's Agency maintenance records:

1. Date and time of maintenance.
2. Name of the individual performing the maintenance.
3. Name of escort, if necessary.
4. A description of the maintenance performed.
5. A list of equipment removed or replaced (including identification numbers, if applicable).

Maintenance Tools

NCDOR will approve, control, and monitor the use of Resource maintenance tools.

NCDOR will review previously approved Resource maintenance tools on an annual basis.

NCDOR will inspect maintenance tools to determine if the tools have been modified in an improper/unauthorized manner or to contain malicious code.

NCDOR will check media containing diagnostic and test programs for malicious code before the media are used in Agency Resources.

NCDOR will prevent the removal of maintenance equipment containing Agency Data by:

a. Verifying that there is no Agency Data contained on the equipment.
b. Sanitizing or destroying the equipment.
c. Retaining the equipment within the facility.
d. Obtaining an exemption from a designated Agency official(s) explicitly authorizing removal of the equipment from the facility.

NCDOR will restrict the use of maintenance tools to authorized personnel only.
NCDOR will monitor the use of maintenance tools that execute with elevated privilege.

Nonlocal Maintenance

NCDOR will approve and monitor nonlocal maintenance and diagnostic activities.

NCDOR will allow the use of nonlocal maintenance and diagnostic tools only as consistent with Agency policy and documented in the security plan for the Resource.

NCDOR will employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.

NCDOR will maintain records for nonlocal maintenance and diagnostic activities.

NCDOR will terminate sessions and network connections when nonlocal maintenance is completed.

NCDOR will log the following events for nonlocal maintenance and diagnostic sessions:

1. All accesses or attempts to access an Agency Resource, including the identity of each user and device.
2. Logoff activities.
3. Activities that might modify, bypass, or negate IT security safeguards.
4. Security-relevant actions associated with processing Agency Data.
5. User generation of reports and extracts containing Agency Data.
6. Any interaction with Agency Data through an application.
7. Password changes.
8. Creation or modification of groups.
9. Privileged user actions.
10. Access to the Resource.
11. Creating and deleting files.
12. Change of permissions or privileges.
13. Command line changes and queries.
14. Changes made to an application or database.
15. Resource and data interactions.
16. Opening and/or closing of files.
17. Program execution activities.

NCDOR will review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

NCDOR will protect nonlocal maintenance sessions by:

a. Employing multifactor authentication consistent with NIST 800-63 Digital Identity Guidelines requirements; and
b. Separating the maintenance sessions from other network sessions with the Resource by either:
    1. Physically separated communications paths.
    2. Logically separated communications paths.

NCDOR will implement cryptographic mechanisms for Virtual Private Network (VPN) connections to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

NCDOR will verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

Supplemental Guidance: Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. 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. Enforcing requirements in MA-4 is accomplished in part by other controls.

Maintenance Personnel

NCDOR will establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

NCDOR will verify that non-escorted personnel performing maintenance on the Resource possess the required access authorizations.

NCDOR will designate Agency personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

NCDOR will ensure that non-escorted personnel performing maintenance activities not directly associated with the Resource but in the physical proximity of the Resource, have required access authorizations.

Timely Maintenance

NCDOR will obtain maintenance support and/or spare parts for security-critical Resource components and/or key information technology components within the Recovery Time Objective/Recovery Point Objective (RTO/RPO) timelines and Maximum Tolerable Downtime (MTD) parameters agreed upon in the Resource Information System Contingency Plan (ISCP).

Risk Assessment Policy

Purpose

The purpose of this policy is to define the methods used to assess, mitigate, and treat security and privacy risks.

Scope

The policy applies to all Agency Resources and Data (physical and logical).

Policy

It is the policy of the Agency that risk assessments will be conducted to identify threats and vulnerabilities associated with Agency Resources and responses to risks will include a plan of action to mitigate in a timely manner.

Required Procedural Elements

Risk Assessment

NCDOR will conduct a risk assessment that:

1. Identifies threats to and vulnerabilities in the Resource.
2. Determines the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the Resource, the information it processes, stores, or transmits, and any related information.
3. Determines the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

NCDOR will integrate risk assessment and integrate risk assessment results and risk management decisions from the Agency and mission or business process perspectives with system-level risk assessments.

NCDOR will document risk assessment results in risk assessment plans and in the form of a registry that will be managed by an approved tracking Resource.

NCDOR will review risk assessment results at least annually.

NCDOR will disseminate risk assessment results to Resource Owners, IT Security, Business Operations, IT, the CIO, and the CISO.

NCDOR will update the risk assessment at least every three years or when there are significant changes to the Resource, its environment of operation, or other conditions that may impact the security or privacy state of the Resource.

NCDOR will assess supply chain risks associated with Agency Data and update the risk assessment every three (3 years), when there are significant changes to the relevant supply chain, or when changes to the Resource, environments of operation, or other conditions may necessitate a change in the supply chain.

Vulnerability Monitoring and Scanning

NCDOR will monitor and scan for vulnerabilities in the Resource and hosted applications every thirty (30) days, prior to placing a Resource on the Agency network, to confirm remediation actions, and when new vulnerabilities potentially affecting the Resource are identified and reported.

NCDOR will employ vulnerability monitoring 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.
2. Formatting checklists and test procedures.
3. Measuring vulnerability impact.

NCDOR will analyze vulnerability scan reports and results from vulnerability monitoring.

NCDOR will remediate legitimate vulnerabilities in accordance with an Agency assessment of risk.

NCDOR will share information obtained from the vulnerability monitoring process and control assessments with all NCDOR IT Security personnel to help eliminate similar vulnerabilities in other Resources.

NCDOR will employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

NCDOR will update the Resource vulnerabilities to be scanned at least every 30 days; prior to a new scan; when new vulnerabilities are identified and reported.

NCDOR will determine information about the Resource that is discoverable and take appropriate corrective actions.

NCDOR will implement privileged access authorization to all information Resource components for selected vulnerability scanning activities.

NCDOR will implement vulnerability management for Resources (including wireless networks) to complement the patch management process.

Risk Response

NCDOR will respond to findings from security and privacy assessments, monitoring, and audits in accordance with Agency risk tolerance.

NCDOR will mitigate risks by implementing new controls or strengthening existing controls; accepting the risk with appropriate justification or rationale; sharing or transferring the risk; or rejecting the risk.

Privacy Impact Assessment

NCDOR will Conduct privacy impact assessments for Resources, programs, or other activities before:

- Developing or procuring information technology that processes personally identifiable information.
- Initiating a new collection of personally identifiable information that:
    1. Will be processed using information technology.
    2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

NCDOR will conduct a privacy impact assessment for new Resources used to process, store, or transmit Agency Data.

Security Incident Response Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are implemented when developing the security incident response program and that assurances are in place that standards, guidelines, and procedures align with NCDOR's risk management strategy.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

NCDOR will ensure that measures are implemented for the timely reporting of any suspected unauthorized disclosure or breach within 24 hours of discovery.

NCDOR will utilize the required controls to offer assurances that employees, contractors, and relevant third-party services are aware of the actions needed to respond, mitigate, recover, and report a security or privacy related incident.

Required Procedural Elements

Security Incident Response Training

NCDOR will provide security incident response training to Resource users consistent with roles and responsibilities:

1. Within 30 days of assuming an incident response role or responsibilities or acquiring Resource access.
2. If changes to Resources may require it.
3. On an annual basis.

NCDOR will review and update security incident response training every 3 years and following major business and Resource changes that may impact the Agency Resource.

NCDOR will incorporate simulated events into training to facilitate the required response by personnel in crisis situations.

NCDOR will provide security incident response training on how to identify and respond to a breach, including NCDOR's process for reporting to a breach.

Security Incident Response Testing

NCDOR will test the effectiveness of the security incident response capability annually through tabletop exercises.

Testing will be coordinated with elements that might exist in all relevant plans that include the following:

- Business Continuity Plans
- Disaster Recovery Plans
- Communication Crisis Plans
- Critical Infrastructure Plans

NCDOR will use qualitative and quantitative data from testing to:

- Determine the effectiveness of security incident response processes.
- Continuously improve security incident response processes
- Provide security incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Security Incident Response Handling

NCDOR will implement handling capabilities for security incidents that are consistent with the security incident response plan and will include preparation detection and analysis, containment, eradication, and recovery.

NCDOR will coordinate security incident handling activities with contingency planning activities.

NCDOR will incorporate lessons learned from ongoing security incident handling activities into the security incident response procedures, training, and testing, and implement the results accordingly.

NCDOR will ensure rigor, intensity, scope, and results of security incident handling activities are comparable and predictable across all departments.

NCDOR will support the security incident handling process using automated solutions or mechanisms.

NCDOR will implement capabilities for security incidents involving insider threats.

NCDOR will coordinate with contractors, data centers, counties, and other agencies to correlate and share security incident information involving Agency Data to achieve a cross-organization perspective on security incident awareness and more effective security incident responses.

Security Incident Monitoring

NCDOR will track and document security incidents.

Security Incident Reporting

NCDOR will require personnel to report suspected security incidents to the Service Desk or by opening a security incident ticket immediately upon discovery.

NCDOR will report security incident information immediately, but no later than 24 hours after identification of a possible issue involving Agency Data.

NCDOR will report Resource vulnerabilities associated with reporting security incidents to the Service Desk.

NCDOR will provide security incident information to the provider of the product or service and other relevant organizations involved in the supply chain or supply chain governance for resources and resources related to the security incident.

Security Incident Response Assistance

NCDOR will provide a security incident response support resource, integral to the department response capability, which provides guidance to users of the Resources for the handling and reporting of security incidents.

NCDOR will provide the capability for security incident response automation to increase the capabilities of the security incident response process.

NCDOR will coordinate with external providers to establish a cooperative relationship between the security incident response capability and external providers of Resource protection capability. Additionally, NCDOR will communicate department security incident response team members to the external providers.

Security Incident Response Plan

NCDOR will develop a security incident response plan that includes the following:

1. A roadmap for implementing the security incident response capability.

2. The structure and description of the security incident response capability
3. A high-level description of the capability and how it fits into the overall department.
4. Is unique to the department in relation to the mission, size, structure, and functions.
5. Defines reportable security incidents.
6. Provides metrics for measuring the security incident response capability within the department.
7. Defines the Resources and management support needed to effectively maintain and mature a security incident response capability.
8. Addresses the sharing of security incident information.
9. Is reviewed and approved by designated Agency officials at a minimum on an annual basis.
10. Explicitly designates responsibility for security incident response to NCDOR IT Security personnel.

NCDOR will distribute copies of the security incident response plan to authorized incident response personnel and Agency personnel with access to Agency Data

NCDOR will update the security incident response plan to address Resource and Agency changes, or problems encountered during plan implementation, execution, or testing.

NCDOR will communicate security incident response plan changes to authorized security incident response personnel and Agency personnel with access to Agency Data.

NCDOR will protect the security incident response plan from unauthorized disclosure and modification.

NCDOR will document response measures in the NCDOR security incident response plan involving breaches related to PII that includes:

1. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.
2. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms.
3. Identification of applicable privacy requirements.

Information Spillage Response

NCDOR will respond to information spills by:

1. Assigning designated security incident response Agency personnel with responsibility for responding to information spills
2. Identifying the specific information involved in the Resource contamination.
3. Alerting designated Agency officials of the information spill using a method of communication not associated with the spill.
4. Isolating the contaminated Resource or Resource component
5. Eradicating the information from the contaminated Resource or component
6. Identifying other Resources or Resource components that may have been subsequently contaminated.
7. Performing the following additional actions when FTI is involved: Report security incident information to the appropriate special agent-in-charge, TIGTA and the IRS Office of Safeguards.

Supply Chain Risk Policy

Purpose

The purpose of this policy is to ensure that risks associated with the supply chain are mitigated through a formal plan, controls, and managed processes.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

NCDOR will manage the supply chain to reduce the exposure to cybersecurity risks and develop response strategies, policies, processes, and procedures.

Required Procedural Elements

Supply Chain Risk Management Plan

NCDOR will develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following system, system components or system services: Resources that process, store, or transmit Agency Data.

NCDOR will review and update the supply chain risk management plan every three (3) years or as required, to address threat, Agency, or environmental changes.

NCDOR will protect the supply chain risk management plan from unauthorized disclosure and modification.

NCDOR will establish a Supply Chain Risk Management Team (SCRMT) consisting of the following Agency personnel:

- Chief Information Officer
- Chief Information Security Officer
- IT PMO
- Chief Operating Officer
- Procurement

Supply Chain Controls and Processes

NCDOR will establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of Resources that access, process, store, or transmit Agency Data in coordination with the Supply Chain Risk Management Team or a subset of the team depending on the service/resource offering.

NCDOR will employ the following controls to protect against supply chain risks to the Resource, Resource component, or Resource service and to limit the harm or consequences from supply chain related events:

- Approved state vendors
- SLA and SOWs with predetermined maintenance schedules
- Resiliency and contingency plan review
- Trusted configurations and hardening methods

NCDOR will document the selected and implemented supply chain processes and controls in security and privacy plans; supply chain risk management plan; and/or any Agency supply chain plan documentation.

NCDOR will employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain:

- Avoid the purchase of custom or non-standardized configurations.
- Adhering to vendor approved lists vetted by the State of North Carolina.
- Follow pre-agreed maintenance schedules.

- Update and patch delivery mechanisms.
- Implement contingencies in case of adverse supply chain events.
- Utilize procurement carve outs that provide exclusions to commitments or obligations.
- Use diverse delivery options.
- Minimize time between purchase decisions and delivery.

NCDOR will ensure that the controls included in the contracts of prime contractors are also included in the contracts of sub-contractors.

Supplier Assessments and Reviews

NCDOR will assess and review the supply chain-related risks associated with suppliers or contractors and the Resource, Resource component, or Resource service they provide at a minimum annually.

Inspection of Systems and Components

NCDOR will inspect the following systems or system components at the time of receiving, upon delivery to detect tampering: hardware /software components that access, process, store, or transmit Agency Data.

Component Authenticity

NCDOR will develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the Resource and report counterfeit Resource components to source of counterfeit component.

NCDOR will train Agency personnel whose roles are specific to supply chain management on methods to detect counterfeit components.

NCDOR will maintain configuration control over Resource components that store Agency Data that are awaiting service or repair and serviced or repaired components awaiting return to service.

Transcript Delivery System (TDS) Policy

Purpose

The purpose of this policy is to ensure that authorization to the TDS is operated under a strict set of controls and that Agency personnel that are granted access adhere to all the requirements of the IRS MOU.

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that access to the TDS will be controlled by a formal authorization and approval process.

Required Procedural Elements

NCDOR will follow all guidance provided by the IRS in accessing the TDS.

NCDOR will require that if TDS is printed and/or duplicated, it is properly labeled and logged according to IRS requirements and Agency guidance. Employees that have access to the TDS are required to report any incidents related to the unauthorized access to FTI.

NCDOR will require that the user or user's manager notify the Disclosure Officer when access to the TDS is no longer required and must provide the date for termination of access. NCDOR will review logs of access for discrepancies or anomalies monthly.

FTI printed on paper must be stamped to identify the document(s) as containing Federal Tax Information, must be stored in a red folder which contains the Agency approved label, and must be always secured when not in use in an Agency approved container.

TDS stored digitally must be named using a standard naming convention in a manner to identify as containing FTI, must be stored in a secure location with restricted access granted to only those staff with a business need and need-to-know. Any transfer of FTI outside of the Agency secured perimeters or infrastructure require approval from the Disclosure Officer.

TDS may be transferred to DOJ for civil or criminal proceedings, may be sent to a taxpayer or duly authorized representative, and disclosed under court order without authorization from the Disclosure Officer.

Virtual Desktop Infrastructure (VDI) and Internet of Things (IoT) Policy

Purpose

The purpose of this policy is to ensure that security and privacy controls are considered when allowing the use of IoT devices and prior to deploying Agency VDI environments.,

Scope

This policy applies to all Agency Staff, Resources, and Data (both logical and physical).

Policy

It is the policy of the Agency that the authorized use of IoT and deployment of VDI will require secure application and device security. NCDOR will ensure that secure execution methods are implemented prior to deployment.

Required Procedural Elements

Virtual Desktop Infrastructure

The Agency allows connections from external information systems only in the event the Agency has configured a virtual desktop infrastructure (VDI) solution to receive, secure and manage remote connections.

Approval by the Agency CISO is required for connection of non-government furnished or contractor-owned IT devices (including USB-connected portable storage and mobile devices) to Agency Resources receiving, processing, storing, accessing, protecting and/or transmitting Agency Data. This requirement does not apply to networks and systems intended for use by the public.

Environment Segregation

NCDOR will segregate Virtual Desktop Components so that boundary protections can be implemented, and access controls are granulized.

Major VDI components such as databases, application servers and management software will be installed on dedicated platforms to prevent unauthorized access.

If a design validation farm or a pilot farm exists, NCDOR will ensure adequate separation for each environment.

If NCDOR decides to support more than one virtual environment, each virtual environment will be independent from each other to prevent a single point of failure.

The Virtual Desktop Tier must be protected in a logical enclave so that VDI Resources are protected and segregated from other enterprise IT Resources.

Devices that have access to Agency Data will be further segregated into a logical enclave to provide the most granular protection for Agency Data.

External facing Access Tier components such as web servers and interface servers will be placed behind filtering devices in a Demilitarized Zone (DMZ).

Access Control

All devices (laptops, computing platforms) will be evaluated for compliance (patches, anti-virus) prior to being allowed to attempt connection to the VDI.

- Access to each Resource will be granted explicitly to prevent unauthorized access, and
- Anonymous and public access will be disabled, and
- Administrative and monitoring traffic will originate from authorized IP address ranges, and
- Administrative consoles will be restricted to authorized personnel only.

NCDOR will implement Network Access Control (NAC), or device authentication ensure only authorized thin client devices are permitted to access the virtual desktop environment.

Secure Configurations

NCDOR will ensure the virtual desktop environment will be securely configured, patched for security vulnerabilities, and supported by the vendor.

The underlying Operating System (OS) will be securely configured as published by the IRS Office of Safeguards via the Safeguard Computer Security Evaluation Matrices (SCSEM).

NCDOR will Install anti-virus software on all platforms supporting the virtual environment.

NCDOR will reposition an existing firewall or add additional boundary protections, if needed, to adequately protect internal Resources.
NCDOR will change the default ports of the web server and remove any sample sites installed by the web server for web interfaces used by the virtual environment.

NCDOR will encrypt all web interfaces using HTTPS to ensure the confidentiality and integrity of web traffic to ensure that SSL certificates are current and that all encryption mechanisms are compliant with the latest version of FIPS 140.

Managing User Privileges

NCDOR will implement Role-Based Access Control (RBAC) to effectively manage user privileges.

Administrators will not be able to authenticate directly as root and must “sudo.”

NCDOR will restrict users from installing software in the virtual environment to prevent the use of unauthorized and malicious software.

NCDOR will only allow end users to have permissions sufficient for daily business operations unless a business justification is documented and approved by management.

NCDOR will implement restricted access to configuration files, log files and automated scripts that are placed on the virtual machine to virtual desktop administrators only.

NCDOR will prevent unauthorized access from end users with the use of access control list.

NCDOR will protect virtual machine files, snapshots and roll back files from unauthorized access.

Limit Functionality

NCDOR will disable Copy and clipboard functions such as the “Client clipboard redirection” to prevent unauthorized access and disclosure of Agency Data.

NCDOR will disable client drive mapping to prevent users from storing data on their local devices or on the virtual workstation.

NCDOR will disable file transfer to local device and USB.

NCDOR will disable shadowing to ensure sensitive data is limited to authorized users only for virtual desktop solutions that support shadowing.

NCDOR will disable unnecessary functionality such as the capability to deliver multimedia information and support of collaboration devices such as webcam and microphones.

NCDOR will disable printer configuration so that Agency Data cannot be printed locally.

NCDOR will configure the virtual desktop to prompt the user for credentials before attempting to resume the disconnected session after network disruption.

NCDOR will remove anonymous or public user accounts from the virtual environment. Published resources must be restricted to authorized users only.

NCDOR will disable snapshots and roll back functionality if they are not required.

Multi-factor Authentication

NCDOR will implement multi-factor authentication for remote access of Agency Data to ensure only authorized users have access to Agency Data.

Audit and Monitoring

NCDOR will configure the virtual desktop environment to record all privileged and administrative functions.

Session Confidentiality and Integrity

NCDOR will enable current FIPS 140 complaint encryptions for traffic with Agency Data in transit as well as management traffic and between Client Tier communications to the virtual desktop.

Internet of Things (IoT)

NCDOR will authorize the use of IoT upon approval and it is determined that the use of IoT technology is deemed as a business necessity or in support of the Agency's mission/strategy.

NCDOR will require that all connections to IoT devices are approved and monitored.

NCDOR will require unique logical identifiers for IoT devices to distinguish the device from others and allow for device management and monitoring.

NCDOR will require logical access privilege configuration to ensure the device meets the Agency's security requirements.

NCDOR will ensure that IoT devices that are approved for use have the capability to be centrally managed and configured to manage software settings, changes, and security settings.

NCDOR will require that IoT devices have protections in place to protect Agency data.

To ensure a third-party contractor system is not considered an external information system, the Agency must include IRS or state Exhibit 7 language in its contract with the service provider.