Security Policy Manual

May 31, 2016

Revision History

Author	Sections	Reason	Version
Dwayne Beamon **Rosita Lee**	All	Added 15 new security policies required by IRS Publication 1075 and NIST 800-53 Controls. Also added new data elements throughout policy manual, and Glossary of terms	01.1
David Roseberry	All	Rewrote the manual to match numbering and format of IRS 1075 and make it easier for staff to work with. New definitions added.	4/1/2015
David Roseberry	All	Revised per IRS Publication 1075 revisions Converted bullets to letters and numbers to make it easier to refer to Dropped confidentiality requirements as it is not applicable	7/24/2015
David Roseberry	All	Revised to add applicability of controls to Data classifications Public and Confidential for clarity	5/26/2016

Table of Contents

General Security Policies

Facilities Security Policies

Technical Security Policies

Overview

This document contains the policies of the North Carolina Department of Revenue (Agency) with respect to the security of our electronic information and computing resources. The purpose of this document is to set forth expectations of behavior in order to protect the electronic information and computing assets of 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 annually.

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 have access to the electronic information or computing assets of the Agency. No exceptions to these policies are permitted unless approved by the CIO. Any questions related to this document should be referred to your supervisor or the Chief Information Security Officer (CISO).

The intent of this manual is to establish the policies of the Agency that will fully comply with the most recent revision of IRS publication 1075 controls. It is also the intent of this manual to treat Data classified as Public or Confidential as equivalent to Data classified as Low Risk or Moderate Risk in NIST Special Publication 800-53 rev 4, respectively. In the case where a system may either store, process or transmit Data classified as Confidential and FTI, both sets of controls apply. In some cases, special policies or controls will be included to meet other standards and regulatory requirements that are placed on the Agency in order to fulfill its mission.

Secretary Name Jeff Epstein

Secretary Signature _____ **Date** 5.31.16

CIO Name David Roseberry

CIO Date _____ **Date** 5/26/2016

Definitions

Agency: The North Carolina Department of Revenue.

Staff: Anyone working on behalf of the Agency regardless of employment status and includes contractual relationships for 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.

Facilities: Broadly interpreted to refer to any physical location where Staff performs work on the behalf of the Agency without regard to the ownership of the physical property. This term includes alternate sites where the Agency has approved for the Staff to work (e.g. a private residence).

Resource: Broadly interpreted to refer to any computing device such as a server, pc, smart phone, tablet or any other such device that can process or transmit information digitally.

Data: Electronic information in any form, regardless of source, that is created or obtained by the Agency.

FTI: Data classified as Federal Tax Information as defined in the General Security Policies Manual.

Non-Public Data: Data that is classified as Confidential or as Federal Tax Information per the General Security Policies Manual.

Media: Anything that is capable of storing Data.

CISO: The Chief Information Security Officer who is responsible for the development, implementation and maintenance of the IT Security program for the Agency.

Major Incident: An event that has, or could, cause a significant loss of functionality and needs to be addressed urgently. Specifically, any incident in which the possibility exists that the integrity or confidentiality of Data classified as non-Public Data could be at risk is considered a Major Incident.

About This Document

Some policies have components that are applicable based on the Data classification that is involved. In order to determine applicability, most polices have a section that clearly defined what parts of the policy apply under what circumstances. If no such distinction is made, the entire policy statement applies.

General Security Policies

Staff Expectations Policy Family

(SE-1) Staff Responsibilities

Purpose

The purpose of the policy is to establish the responsibilities of all Staff as it relates to the security of Data or Resources owned or operated by the Agency.

Scope

This policy applies to all Staff.

It is the policy of the Agency that all Staff must actively participate in ensuring the security of Agency Data and Resources.

a) Compliance with all policies is a necessary condition of employment. Noncompliance or conduct unbecoming a state employee may result in disciplinary action, up to and including termination.
b) All work products including, but not limited to, programs, software, source code, and documentation generated on behalf of the Agency, are the sole property of the Agency without exception. The Agency owns all Data stored, created, transmitted, and received on behalf of the Agency. In the cases where received data is subject to a Memorandum of Understanding (MOU), then the Agency will ensure that the MOU is enforced. All Media received from an external source must be scanned prior to accessing the Data, using approved tools and methods.
c) Use of Resources to perform work on behalf of the Agency does not indicate an expectation of privacy. The Agency may audit, examine, inspect, or monitor, at any time without notice, any agency Resource or a non-Agency Resource that is connected to Agency networks. Use of Agency Resources for personal purposes is permitted provided that it is not used in a way that is illegal, could compromise security or causes an unauthorized cost to be incurred by the Agency (e.g. a long distance call). Authorization is determined by your immediate supervisor.
d) Staff must be observant of any action or occurrence that could violate security policies including unusual behaviors, unlawful activity, unauthorized disclosure of Data, or attempts to gain unauthorized access to Data or Resources. Staff must report loss or inappropriate disclosure of Data, loss or theft of Resources, or violation of security policy to the Service Desk within two hours of suspected loss or disclosure.
e) Staff must safeguard their logon ID and password to ensure it is used only for the purpose for which it is intended. If Staff suspects their password may have been compromised, they should change it, and notify the Service Desk and their immediate supervisor within 30 minutes.

f) Staff shall not attempt to access Data, Resources, or Media, that are not appropriate for their duties and responsibilities or for which they are not authorized. Staff must report any inappropriate level of access to Data, Resources or Media to the IT Service Desk and their immediate supervisor within two hours.
g) Staff shall not tamper with or change security configurations of Resources.
h) Staff shall not copy, distribute, or use in any manner Agency software that knowingly violates the licensing agreement.
i) Staff shall not install hardware or software that provides network services (e.g. wifi, hotspots, wireless access points, etc.). "Sniffing" or listening in on Agency owned networks, wired or wireless, is prohibited.
j) Electronic communications, such as text or email, shall not contain statements or content that is libelous, offensive, harassing, illegal, derogatory, or discriminatory. Foul, inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes are prohibited. Sexually explicit messages or images, cartoons, or jokes are prohibited. Messages for political fund raising, election campaigns, profit, or non-Agency approved fund raising are prohibited.
k) Staff must report any discovered access to Resources or Data that is inappropriate for themselves or others to the IT Service Desk immediately.

(SE-2) Data Classification

Control retired and replaced with RA-2

(SE-3) Internet Usage

Purpose

The purpose of the policy is to regulate the use of Agency provided Internet access.

Scope

This policy applies to all Staff or Resources accessing Agency provided Internet services or any non-Agency owned networks.

It is the policy of the Agency that access to the Internet is considered a privilege and Staff must use it responsibly and professionally, and make no intentional use of it in an illegal, malicious, or obscene manner.

a) Access to the Internet does not convey an expectation of privacy. The Agency may audit, examine, inspect, and monitor, at any time, the use of the Internet without notice.
b) No software shall be downloaded from the Internet onto Agency Resources without the approval of the CISO. The downloader is solely responsible for ensuring that the software is used in a manner consistent with all applicable software copyright and licensing laws. Violation of

copyright protection or licensing agreements may subject the downloader to civil and criminal liability.

c) All files downloaded from the Internet must be scanned using IT approved products prior to use.
d) No FTI or Confidential Information shall be transmitted over the Internet without prior approval of the CISO and must comply with all policies and procedures. Any questions regarding the appropriateness of transmitting information should be referred to the IT Service Desk.

(SE-4) Messaging Systems

Purpose

The purpose of this policy is to ensure the proper use of Agency provided messaging systems, such as email, text, instant messaging, or web conferencing tools, and prevent the unauthorized or inadvertent disclosure of information.

Scope

This policy applies to messaging services provided, owned, or funded in part or in whole by the Agency.

It is the policy of the Agency that all messages created, sent, received, or stored on the official messaging systems are the sole property of the Agency. Use of alternative messaging systems for the purpose of conducting Agency business is expressly prohibited including auto-forwarding of messages.

(SE-5) Social Media

Purpose

The purpose of this policy is to provide standards for the use of social media. Even though social media is frequently used to express personal views, it can directly or indirectly impact the Agency. Staff who view social media posts may not recognize, or fully appreciate, that the ideas, views, opinions or positions belong to the author rather than the Agency.

Scope

This policy applies to the use of online publishing or public communication services, broadly referred to as Social Media, and includes, but is not limited to, blogs, personal web pages, online journals, and interactive online social communication services such as Facebook and Twitter. Communications includes posting text, pictures, videos, links and any other material made accessible to others outside of the Agency. This policy applies to all Staff without regard to working hours or the ownership of the computing device used to communicate.

It is the policy of the Agency that the use of Social Media by Staff is subject to Agency standards and values. Staff should demonstrate respect for others and exercise good judgment when participating in Social Media.

a) Except as expressly authorized by the Secretary, Staff shall refrain from making any statements regarding the Agency and may not engage in communications that represents, or makes it appear they are representing, the Agency. Staff shall not use Agency trademarks, logos, letterhead, copyright materials or communicate information about the Agency that has not already been made public.
b) Staff shall not make offensive comments that have the purpose or effect of creating an intimidating or hostile environment such as the use of ethnic slurs, personal insults, profanity, or other offensive language. Staff shall not engage in communications that defame or violate the privacy or publicity rights of any party.

(SE-6) Password Sharing

Purpose

The purpose of the policy is to ensure that passwords are protected and not inadvertently compromised.

Scope

The scope of this policy applies to all Staff.

It is the policy of the Agency that passwords shall not be shared with, used by, or disclosed to others.

a) IT staff will never ask Staff for their password.
b) Passwords shall not be inserted into email messages or other forms of electronic communication.
c) Passwords shall not be embedded in automated programs, utilities, applications, documents, or other methods whereby they may be stored on the system.

(SE-7) Security of Mobile Resources

Purpose

The purpose of the policy is to secure mobile Resources.

Scope

The policy applies to all Agency mobile Resources.

It is the policy of the Agency to secure mobile Resources.

a) Staff are responsible for the security of any mobile Resources they have been issued. Staff should keep the mobile Resource in their possession at all times or stored securely when not in use. Mobile Resources that are stored in Agency operated facilities are considered secure unless otherwise indicated.
b) Outside of Agency owned facilities:
    1. Mobile Resources should be stored out of plain sight, when possible, under lock and key. The key should remain in the possession of the Staff.
    2. When traveling by common carrier (for example, air, trains, bus, boat, etc.), mobile Resources should not be checked as baggage.
c) The loss or theft of a mobile Resource must be reported to the IT Service Desk immediately.
d) The CISO will establish security standards, usage restrictions and implementation guidance for mobile Resources and authorize, monitor, and control access to Data. Whenever possible, all mobile Resources must be encrypted.

Facilities Security Policies

Facilities Security

(FS-1) Staff Responsibilities

Purpose

The purpose of the policy is to establish the responsibilities of all Staff as it relates to the security of Facilities.

Scope

This policy applies to all Staff.

It is the policy of the Agency that all Staff must actively participate in ensuring the security of Facilities.

All Staff must:

a) Observe surroundings.
b) Report to Security Guards any unusual activity.
c) Report any threats (actual or perceived) against the Agency or any Agency staff.
d) Safeguard their badge at all times, and wear it between the neck and waist.
e) Report a lost or stolen badge immediately to the Service Desk or Security Guard.
f) Not allow another individual to “piggyback” or “tailgate” through security checkpoints (e.g. doors with badge access).
g) Never share their badge.

(FS-2) Management Responsibilities

Purpose

The purpose of the policy is to establish the responsibilities of managers as it relates to the security of Facilities.

Scope

This policy applies to all Staff with supervisory or managerial responsibilities.

It is the policy of the Agency that managers actively participate in ensuring the security of Facilities.

a) Notify the Service Desk or Security Guards of Staff termination, so access badges can be immediately revoked.

b) Facility access must be terminated immediately and the manager can later submit approved access request form to remove all other system access of employee or contractor.

(FS-3) Threats

Purpose

The purpose of the policy is to ensure that threats are promptly and appropriately reported.

Scope

The policy applies to all Staff.

It is the policy that Staff is required to immediately report any threat, actual or perceived, against the Agency, Staff, or any other criminal threat to the Agency's Security Guards. Only Security Guards should attempt to deal with a physical threat.

(FS-4) Visitors

Purpose

The purpose of the policy is to ensure that visitors are properly controlled while in a Facility.

Scope

The policy applies to all Agency Staff and Facilities.

It is the policy of the Agency that access to Facilities is controlled.

a) Visitors must provide proof of identity before being granted access to areas where Resources reside or Data is transmitted, stored or processed. Visitors must be escorted at all times while in such areas.

(FS-5) Staff Background Screening

Purpose

The purpose of the policy is to ensure that background screens are performed and the screening process is administered consistently, equally and fairly to all Staff and prospective Staff.

Scope

This policy applies to Agency Human Resources Staff and affects all Staff.

It is the policy of the Agency that background checks will be required of all applicant finalists selected for new hire in regular full-time, regular part-time, time-limited, temporary, intermittent positions or contract services with the Agency.

Background screening of Agency employees, contractors and prospective employees shall have the objective and focus on the following:

a) Compliance with IRS Publication 1075 requirements (and protection of Data classified as Federal Taxpayer Information).
b) Compliance with PCI Data Security Standard requirements.
c) Compliance with all regulatory mandates and laws enforced by state and federal agencies.
d) Fulfilling other legal or contractual obligations.
e) Providing a safe work environment.
f) Protecting Agency assets.
g) Reducing risk of legal liabilities.

(FS-6) Minimum Protection of Data Classified as Federal Tax Information (FTI)

Purpose

The purpose of the policy is to ensure that the Agency establishes a uniform method of physically protecting Data and Resources as well as non-electronic forms of FTI.

Scope

The policy applies to all Agency Staff. Also applies to the protection of non-electronic forms of FTI (such as printed reports, correspondence, etc. that contain FTI).

It is the policy of the Agency that a minimum protection standard be established and maintained to inform Agency Staff as to what constitutes minimum protection of FTI per IRS regulations (IRS 1075, section 4.2).

IT Security Staff will:

a) Document, disseminate and review at least annually a Minimum Protection Standard for safeguarding FTI. The Minimum Protection Standards should cover the following subjects:
    1. Secured Perimeter
    2. Security Room
    3. Badged Staff
    4. Security Container

(FS-7) Restricted Area Access

Purpose

The purpose of the policy is to ensure that there are appropriate measures in place to prevent unauthorized access to Data by creating restricted areas where such Data resides.

Scope

The policy applies to all Business Operations management Staff and Agency Facilities.

It is the policy of the Agency to have procedures that ensure Data is protected by restricting physical access to areas (i.e. restricted areas) where such Data resides.

a) All restricted areas shall have at least two barriers of protection to deter, delay, or detect illegal or unauthorized entry.
b) Data must be containerized in areas where other than authorized Staff may have access after-hours.
c) Access to Restricted Areas must be monitored and records maintained of all persons entering these areas.
d) The Agency must establish procedures for restricted area access including:
    1. Protection of Data after normal business hours.
    2. Appropriate storage containers.
    3. Signs should be prominently posted.
    4. Visitor access log that complies with IRS 1075, section 4.3 “Restricted Area Access”.
    5. Visitor sign-in and validation of visitor’s identity.
    6. Use Authorized Access List.
    7. Control Access to Areas.
    8. Control and Safeguard Keys and Combinations
    9. Keep to a minimum physical keys (or knowledge of combination) to restricted areas
    10. Protect Data in Transit
e) Restrict physical access to Data or Resources that house cardholder data (“PCI data”).
    1. Including limiting and monitoring physical access to Resources in the cardholder data environment, developing procedures regarding badge access, and controlling access to restricted areas.
    2. Procedures should comply with PCI DSS v3.0, Requirement 9.

(FS-8) Physical Security of Resources & Data

Purpose

The purpose of the policy is to ensure that the Agency protects its Resources and Data.

Scope

The policy applies to all Agency Staff and Resources.

It is the policy of the Agency to have procedures that ensure basic security requirements are met for keeping Data protected.

The Agency must:

a) Keep in a secure area with restricted access Data and Resources that receive, process, store, or transmit Data.
b) In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, Resources must receive the highest level of protection practical, including full disk encryption.
c) All Resources that contain Data and are resident in an alternate work site must employ encryption mechanisms to ensure that the Data may not be accessed. If the computer is lost or stolen, it must be reported immediately to the employee's manager and to the IT Service Desk.
d) Basic security requirements must be met, such as keeping Resources and Media locked up when not in use.
e) When removable media contains FTI, it must be labeled as such.
f) All Resources and media containing Data must be kept in a secured area under the immediate protection and control of an authorized Staff or locked up. When not in use, the Media must be promptly returned to a proper storage area/container.
g) Inventory records of electronic Media must be maintained and reviewed semi-annually for control and accountability.
h) Physical access to transmission medium (e.g., cabling), should be protected and access restricted.

(FS-9) Media Off-site Storage Requirements

Purpose

The purpose of the policy is to ensure that the Agency protects its Media that contains Data.

Scope

The policy applies to all Staff and Media that contains Data.

It is the policy of the Agency that when using off-site storage Facilities, if the following conditions are met that no additional IRS safeguarding controls related to physical access will apply:

a) The Media is encrypted.
b) The Media is locked in a turtle case.
c) The Agency retains the key to the turtle case.

(FS-10) Alternative Work Locations

Purpose

The purpose of the policy is to ensure that the confidentiality and integrity of Data is protected.

Scope

The policy applies to all Staff and alternative work locations.

It is the policy of the Agency that all policies apply at telework sites (e.g. Staff homes)

The Agency must conduct periodic inspections of alternative work sites during the year to ensure compliance with all policies. The results of each inspection shall be fully documented.

Physical and Environmental Protection

(PE-1) Physical Security Environment Protection

Purpose

The purpose of the policy is to ensure that proper physical and environmental controls are in place to protect Staff and Resources.

Applicability

Public	Confidential	FTI
PE-1	PE-1	PE-1

Scope

The policy applies to all Agency Facilities and approved alternate work sites.

It is the policy of the Agency that procedures to facilitate the implementation of the physical security environment protection procedures must be documented, disseminated and reviewed at least annually.

(PE-2) Physical Access Authorizations

Purpose

The purpose of the policy is to ensure that physical access to Agency Facilities is restricted to authorized Staff.

Applicability

Public	Confidential	FTI
PE-2	PE-2	PE-2 (CE1)

Scope

The policy applies to all Agency facilities and Staff.

The Agency must:

a) Develop, approve, and maintain a list of Staff with authorized access to the Agency facilities where Resources and Data reside.
b) Issue authorization credentials for Agency facility access.
c) Review the access list detailing authorized Agency facility access by Staff, at least annually
d) Remove Staff from the facility access list when no longer required

Control Enhancement

CE1. Enforce physical access authorizations to Resources in addition to the physical access controls for the Facility where Data is received, processed, stored, or transmitted.

(PE-3) Physical Access Control

Purpose

The purpose of the policy is to ensure that physical access controls at the entry/exit points to Facilities where Agency Resources reside.

Applicability

Public	Confidential	FTI
PE-3	PE-3	PE-3

Scope

The policy applies to all Agency Facilities and Agency Staff.

It is the policy of the Agency to:

a) Enforce physical access authorizations at entry/exit points to Facilities by:
    1. Verifying individual access authorizations before granting access to the Facility; and
    2. Controlling ingress/egress to the Facility using physical access control systems/devices or guards.

b) Maintain physical access audit logs for entry/exit points;
c) Provide security safeguards to control access to areas within the Facility officially designated as publicly accessible;
d) Escort visitors and monitor visitor activity;
e) Secure keys, combinations, and other physical access devices;
f) Inventory physical access devices; and
g) Change combinations and keys when an employee who knows the combination retires, terminates employment, or transfers to another position or at least annually.

(PE-4) Access Control for Transmission Medium

Purpose

The purpose of the policy is to ensure that physical access to Agency Facilities is controlled.

Applicability

Public	Confidential	FTI
	PE-4	PE-4

Scope

The policy applies to all Facilities and Agency Staff.

Is the policy of the Agency to control physical access within Facilities.

(PE-5) Access Control for Output Devices

Purpose

The purpose of the policy is to ensure that physical access to Resources is controlled.

Applicability

Public	Confidential	FTI
	PE-5	PE-5

Scope

The policy applies to all Facilities and Agency Staff.

The Agency must control physical access to Resources to prevent unauthorized disclosure.

(PE-6) Monitoring Physical Access

Purpose

The purpose of the policy is to ensure that physical access to Facilities is monitored.

Applicability

Public	Confidential	FTI
PE-6	PE-6 (CE1)	PE-6 (CE1)

Scope

The policy applies to all Facilities where Resources reside.

It is the policy of the Agency to monitor physical access to the Facility where the Resources reside in order to detect and respond to physical security incidents. The Agency must:

a) Review physical access logs annually;
b) Coordinate results of reviews and investigations with the agency incident response capability; and
c) Monitor physical intrusion alarms and surveillance equipment.

(PE-8) Visitor Access Records

Purpose

The purpose of the policy is to ensure that records of visitors are maintained and reviewed.

Applicability

Public	Confidential	FTI
PE-8	PE-8	PE-8

Scope

The policy applies to all Facilities.

It is the policy of the Agency to maintain visitor access records to the facility where Resources reside and review visitor access records at least annually.

(PE-9) Power Equipment and Cabling

Purpose

The purpose of the policy is to determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to Agency facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

Applicability

Public	Confidential	FTI
	PE-9	

Scope

The policy applies to all environments, regardless of ownership, where Agency Resources reside.

It is the policy of the Agency to protect power equipment and power cabling for the Resource from damage and destruction.

(PE-10) Emergency Shutoff

Purpose

This policy applies primarily to facilities containing concentrations of Resources including, for example, in data centers or server rooms.

Applicability

Public	Confidential	FTI
	PE-10	

Scope

The policy applies to all environments, regardless of ownership, where Agency Resources reside.

It is the policy of the Agency to:

a. Provide the capability of shutting off power to the Resource;

b. Place emergency shutoff switches or devices in any location where Agency Resources are permanently located, to facilitate safe and easy access for personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

(PE-11) Emergency Power

Purpose

The purpose of the policy is sustaining operations of Resources in the event of loss of power.

Applicability

Public	Confidential	FTI
	PE-11	

Scope

The policy applies to all Resources.

It is the policy of the Agency to provide a short-term uninterruptible power supply to facilitate either an orderly shutdown of the Resource or transition of the Resources to long-term alternate power in the event of a primary power source loss.

(PE-12) Emergency Lighting

Purpose

This policy applies primarily to facilities containing concentrations of Resources including, for example, in data centers or server rooms.

Applicability

Public	Confidential	FTI
PE-12	PE-12	

Scope

The policy applies to all Resources.

It is the policy of the Agency to employ and maintains automatic emergency lighting for the Resource that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

(PE-13) Fire Protection

Purpose

The purpose of the policy is to protect Resources.

Applicability

Public	Confidential	FTI
PE-13	PE-13 (CE3)	

Scope

The policy applies to facilities containing concentrations of Resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

It is the policy of the Agency to employ and maintain fire suppression and detection devices/systems for the Resources that are supported by an independent energy source.

(PE-14) Temperature and Humidity Controls

Purpose

The purpose of the policy is to provide stable environmental conditions conducive to the operation of the Resource.

Applicability

Public	Confidential	FTI
PE-14	PE-14	

Scope

The policy applies to facilities containing concentrations of Resources, for example, data centers, server rooms, and mainframe computer rooms.

It is the policy of the Agency to:

a. Maintain temperature and humidity levels within the facility where the Resource resides at; and

b. Monitor temperature and humidity levels.

(PE-15) Water Damage Protection

Purpose

The purpose of the policy is to protect Resources from water damage.

Applicability

Public	Confidential	FTI
PE-15	PE-15	

Scope

The policy applies to facilities containing concentrations of Resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

It is the policy of the Agency to protect the Resource from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

(PE-16) Delivery and Removal

Purpose

The purpose of the policy is to ensure that Resource components entering and exiting the Facilities are controlled.

Applicability

Public	Confidential	FTI
PE-16	PE-16	PE-16

Scope

The policy applies to all Facilities.

It is the policy of the Agency to authorize, monitor and control Resource components entering and exiting the Facility and maintain records of those items.

(PE-17) Alternate Work Site

Purpose

The purpose of the policy is to ensure that Data & Resources are protected at alternate work sites.

Applicability

Public	Confidential	FTI
	PE-17	PE-17

Scope

The policy applies to all Facilities.

It is the policy of the Agency to employ Office of Safeguards requirements at alternate work sites. The Agency must:

a) Assess, as feasible, the effectiveness of security controls at alternate work sites; and
b) Security incidents or problems must be immediately reported to the IT Service Desk.

(PE-18) Location of Resource Components

Purpose

The purpose of the policy is to ensure that Resources are physically placed as to minimize potential damage from environmental hazards.

Applicability

Public	Confidential	FTI
		PE-18

Scope

The policy applies to all Resources.

It is the policy of the Agency to position Resources within the Facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Technical Security Policies

Access Control Policy Family

(AC-1) Access Control Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the access control policy family.

Applicability

Public	Confidential	FTI
AC-1	AC-1	AC-1

Scope

This policy applies to all access control procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the access control processes must be documented, disseminated and reviewed at least annually.

(AC-2) Account Management

Purpose

The purpose of the policy is to ensure that the confidentiality and integrity of Data is protected by appropriately managing accounts.

Applicability

Public	Confidential	FTI
AC-2	AC-2 (CE1) (CE2) (CE3) (CE4)	AC-2 (CE-3)

Scope

This policy applies to all Staff, Resources and Data.

It is the policy of the Agency to restrict Staff access to Data and Resources appropriate to their duties and responsibilities. The IT Business Support Services (BSS) Department is responsible for account management.

a) BSS will identify and select the types of accounts to support organizational missions/business functions.
b) BSS will identify an account manager for each Resource and manage all accounts in accordance to account management procedures;
c) The account manager is responsible for establishing conditions for group and role membership and the related privileges and other attributes for each account;
d) BSS will require approval of the account manager for requests to create accounts. Access to Resources or Data is not permitted unless specifically requested and approved by the account manager. Additional approvals may be required before access is granted. The CIO or CISO may deny, restrict or revoke access to any Resource or Data for any Staff without notice in order to preserve the integrity and confidentiality of Data;
e) The Human Resources Department must notify the IT Service Desk when Staff are separated or transfers to another department. Those supervising or sponsoring contractual Staff must report when contractors start, change work assignments, or end their assignment. BSS must then restrict access accordingly. Internal transfers will be treated as a separation from the originating department and a new hire in the department that the Staff transferred to;
f) Resources must log the use of accounts; and
g) The IT Security Department will review accounts for compliance with account management requirements annually, at a minimum, for accounts with general privileges and quarterly, at a minimum, for accounts with elevated privileges.

Control Enhancements

CE1. The Agency employs automated mechanisms to support the management of accounts.
CE2. The Resource automatically removes or disables temporary and emergency accounts after a defined time period for each type of account.
CE3. Accounts that are inactive for 120 days are disabled
CE4. The Resource automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies IT Security.

(AC-3, 4) Access & Information Flow Enforcement

Purpose

The purpose of the policy is to establish requirements related to access control policies.

Control Applicability

Public	Confidential	FTI
AC-3,4	AC-3,4	AC-3,4

Scope

This policy applies to all Resources.

It is the policy of the Agency that all Resources enforce approved authorizations:

a) For logical access to Data in accordance with applicable access control policies (AC-3); and
b) For controlling the flow of information within the Resource and between interconnected Resources based on applicable information flow control policies (AC-4).

(AC-5) Separation of Duties

Purpose

The purpose of the policy is to address the potential for abuse of privileges and the risk of malevolent activity without collusion.

Control Applicability

Public	Confidential	FTI
	AC-5	AC-5

Scope

This policy applies to all Staff who have sufficient access to Resources or Data and that the potential of malevolent activity is feasible.

It is the policy of the Agency that:

a) All duties of Staff are separated & documented to prevent harmful activity without collusion. For example:
    1. Dividing mission functions and Resource support functions among different individuals;

2. Conducting Resource support functions with different individuals such as Resource management, programming, configuration management, quality assurance & testing, and network security; and
3. Ensuring security personnel administering access control functions do not also administer audit functions.

b) Resource access authorizations are defined to support separation of duties.

(AC-6) Least Privilege

Purpose

The purpose of the policy is to establish the use of the principle of “least privilege”.

Applicability

Public	Confidential	FTI
	AC-6 (CE1) (CE2) (CE5) (CE9) (CE10)	AC-6 (CE1) (CE2) (CE5) (CE9) (CE10)

Scope

This policy applies to all Staff and Resources.

It is the policy of the Agency that Staff, or processes acting on behalf of Staff, is only authorized access necessary to accomplish assigned tasks in accordance with required business functions.

Control Enhancements

CE1. The Agency explicitly authorizes access to Data classified as Confidential or FTI.

CE2. The Agency requires that users of accounts, or roles, with access to Confidential Data or FTI use non-privileged accounts or roles when accessing non-security functions. (i.e. A system administrator account should not be used for non-security related work).

CE5. The Agency restricts privileged accounts on the Resource to a limited number of Staff with a need to perform security or administrative duties.

CE9. The resource must log the execution of privileged functions.

CE10. The resource must prevent non-privileged Staff from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

CE11.A privileged account must be in addition to the non-privileged account which is used for day to day tasks.

(AC-7) Unsuccessful Logon Attempts

Purpose

The purpose of the policy is to limit invalid logon attempts.

Applicability

Public	Confidential	FTI
AC-7	AC-7	AC-7 (FTI1)(FTI2)

Scope

This policy applies to all Resources that enforce authentication.

The Resource must:

a) Enforces a limit of consecutive invalid logon attempts by a user during a defined time period; and
b) Automatically locks the account for a defined time period; locks the account until released by an administrator; delays next logon prompt when the maximum number of unsuccessful attempts is exceeded.

Control Enhancements

FTI1. Resources enforce a limit of three consecutive invalid logon attempts within a 120-minute period

FTI2. Resources automatically lock the account until released by the Resource administrator.

(AC-8) Resource Use Notification

Purpose

The purpose of the policy is to establish the use of warning banners.

Applicability

Public	Confidential	FTI
AC-8	AC-8	AC-8

Scope

This policy applies to all Resources where Data is stored, processed or transmitted.

It is the policy of the Agency that for all Resources:

a) Before granting access to Staff, the Resource must display a use notification message that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
    1. The Staff are accessing a restricted Resource;
    2. Usage may be monitored, recorded, and subject to audit;
    3. Unauthorized use of the Resource is prohibited and subject to criminal and civil penalties; and
    4. Use of the Resource indicates consent to monitoring and recording.
b) Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the Resource; and
c) For publicly accessible Resources:
    1. Displays use information before granting further access;
    2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such Resources that generally prohibit those activities; and
    3. And includes a description of the authorized uses of the Resource.

(AC-11) Session Lock

Purpose

The purpose of the policy is to prevent unintended access.

Applicability

Public	Confidential	FTI
	AC-11	AC-11

Scope

This policy applies only to Resources where Data classified as Confidential or FTI is stored, processed or transmitted.

It is the policy of the Agency that Resources prevent access by initiating a session lock after 15 minutes of inactivity and maintains the lock until the Staff reestablishes access using established identification and authentication procedures.

(AC-12) Session Termination

Purpose

The purpose of the policy is to prevent unintended access.

Applicability

Public	Confidential	FTI
	AC-12	AC-12

Scope

This policy applies only to logical sessions on Resources where Data classified as Confidential or FTI is stored, processed or transmitted. A logical session (for local, network, and remote access) is initiated whenever Staff, or process acting on behalf of Staff, accesses a Resource. Such sessions can be terminated without terminating network sessions. Session termination terminates all processes associated with the Staff's logical session except those processes that are specifically created by the session owner to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, 15 minutes of user inactivity, targeted responses to certain types of incidents or time-of-day restrictions on Resource use.

It is the policy of the Agency that Resources automatically terminate Staff-initiated logical sessions after 15 minutes of inactivity.

(AC-14) Permitted Actions without Identification or Authentication

Purpose

The purpose of the policy is to addresses situations in which it is determined that no identification or authentication is required for a Resource.

Applicability

Public	Confidential	FTI
AC-14	AC-14	AC-14

Scope

This policy applies to all Resources in which it is determined that no identification or authentication is required including, for example, when Staff access public websites, use mobile phones to receive calls, or when facsimiles are received. This policy does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred.

It is the policy of the Agency that Data may not be disclosed without identification and authentication. For those Resources on which it is determined that no identification or authentication is required, the specific actions that can be performed must not include the disclosure of inappropriate Data.

(AC-17) Remote Access

Purpose

The purpose of the policy is to establish the requirements needed to access Resources and Data from a remote location.

Applicability

Public	Confidential	FTI
AC-17	AC-17 (CE1) (CE2) (CE3) (CE4)	AC-17 (CE1) (CE2) (CE3) (CE4) (FTI1) (FTI2) (FTI3) (FTI4)

Scope

This policy applies to access of the Data or Resources by Staff (or processes acting on behalf of Staff) via non-Agency controlled networks regardless of method (e.g. dial-up, broadband, and wireless). This policy does not apply to Resources designed for public access such as web servers. This policy addresses authorization prior to allowing access.

It is the policy of the Agency that for each type of remote access allowed, procedures must:

a) document usage restrictions, configuration/connection requirements and implementation guidance, and;
b) Authorizes remote access to the information system prior to allowing such connections

Control Enhancements

CE1. IT Security must monitor and control remote access methods

CE2. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

CE3. All remote access should be routed through the fewest number of managed network access control points as is practical

CE4. There are no special restrictions to the use of privileged commands or access to security-relevant information based solely on the access being remote

FTI1. Remote access requires identification and multifactor authorization prior to allowing access (IA-2, CE1, CE2, CE11);

FTI2. Multifactor authentication must be implemented such that one of the factors is provided by a device separate from the Resource gaining access. NIST SP 800-63 allows the use of software tokens (IA-2, CE11);

FTI3. Remote access is prohibited for Staff located outside of United States. Further, no Data may be received, processed, stored, transmitted or disposed of by Resources located outside of the United States;

FTI4. All remote access must be encrypted using a cryptographic module that is FIPS 140-2 compliant (CE2, IA-7);

(AC-18) Wireless Access

Purpose

The purpose of the policy is to prohibit the use of wireless technologies to directly access Resources.

Applicability

Public	Confidential	FTI
AC-18	AC-18 (CE1)	AC-18 (CE1) (FTI1) (FTI2)

Scope

This policy applies to the use of technologies that do not require a physical connection (e.g. microwave, UHF/VHF radio, 802.11x, Bluetooth, Near Field Communications, etc.).

It is the policy of the Agency to:

a) Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
b) Authorize wireless access to the Resource prior to allowing such connections.

Control Enhancements

CE1. The information system must protect wireless access to the system using authentication and encryption.

FTI1. To use FTI in an 802.11 WLAN the agency must meet the following requirements:

a) The agency should have WLAN management controls that include security policies and procedures, a complete inventory of all wireless network components, and standardized security configurations for all components.

b) WLAN hardware (access points, servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, Secure Storage—IRC 6103(p)(4)(B).
c) Each system within the agency's network that transmits FTI through the WLAN is hardened in accordance with the requirements in this publication.
d) The WLAN is architected to provide logical separation between WLANs with different security profiles and from the wired LAN.
e) WLAN infrastructure that receives, processes, stores, or transmits FTI must comply with the Institute of Electrical and Electronic Engineers 802.11i wireless security standard and perform mutual authentication for all access to FTI via 802.1X and extensible authentication protocol.
f) Vulnerability scanning should be conducted as part of periodic technical security assessments for the organization's WLAN.
g) Wireless intrusion detection is deployed to monitor for unauthorized access, and security event logging is enabled on WLAN components in accordance with IRS publication 1075 Section 9.3.3, Audit and Accountability.
h) Disposal of all WLAN hardware follows media sanitization and disposal procedures in IRS publication 1075 Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization.

FTI2. IT Security must employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential breaches to Resources.

(AC-19) Access Control for Mobile Resources

Purpose

The purpose of the policy is to clarify the use of highly portable Resources.

Applicability

Public	Confidential	FTI
AC-19	AC-19 (CE5)	AC-19 (CE5) (AC-7 CE2) (FTI1)

Scope

This policy applies to the use of Resources that are portable by an individual, designed to operate without the need of a physical connection to a network, possess local Data storage and a self-contained power source. This policy applies only to such Resources that store, transmit or process Data.

It is the policy of the Agency to:

a) Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b) Authorize the connection of mobile devices to organizational Resources.

Control Enhancements

CE5. Mobile Resources must use a cryptographic module that is FIPS 140-2 compliant to protect confidentiality and integrity of local Data.

CE2. Mobile Resources must automatically purge/wipe Data from mobile Resources based on 10 consecutive, unsuccessful logon attempts. Laptop computers are excluded from this specific requirement.

FTI1. In addition, Mobile Resources must also meet the following requirements (IRS 1075 October 2014 - 9.4.8):

a) Mobile Resource management controls must be in place including security policies and procedures, inventory, and standardized security configurations for all Resources;
b) An annual risk assessment must be conducted of the security controls in place on all Resources in the mobile environment;
c) Protection mechanisms must be in place in case a mobile Resource is lost or stolen—all Data stored internally on the Resource or via removable media, must be encrypted using a cryptographic module that is FIPS 140-2 compliant;
d) The Agency must control the ability to download only authorized applications to the Resource and must limit access to Data by only authorized applications;
e) All mobile device management servers that receive, store or transmit Data must be hardened in accordance to this policy manual.
f) A centralized mobile Resource management solution must be used to authenticate Agency-issued and personally owned mobile Resources prior to allowing access to the internal network;
g) Security events must be logged for all mobile Resource and related management Resources;
h) The Agency must disable wireless personal area networks that allow a mobile Resource to connect to other Resources via Bluetooth or near field communication (NFC);
i) Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, must be disabled to the extent practical; and
j) Disposal of all mobile Resource component hardware follows media sanitization and disposal procedures.

(AC-20) Use of External Resources

Purpose

This control addresses the use of external Resources for the processing, storage, or transmission of Data from external Resources. External Resources are outside of the authorization boundary established by Agency and which the Agency has no direct supervision and authority over the application of required security controls or the assessment of control effectiveness.

The Agency establishes terms and conditions (i.e. MOUs, contracts, etc.) for the use of external Resources in accordance with Agency security policies and procedures. If terms and conditions with the owners of external Resources cannot be established, the Agency may impose restrictions on Agency personnel using those external Resources.

Applicability

Public	Confidential	FTI
AC-20	AC-20 (CE1) (CE2)	AC-20 (CE2) (CE3)

Scope

This policy applies to the intended use of non-Agency owned Resources or external access to Data.

The Agency establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external Resources, allowing authorized individuals to:

a) Access the Resource from external Resources; and
b) Process, store, or transmit organization-controlled Data using external Resources.

Control Enhancements

CE1. The Agency permits authorized Staff to use an external Resource to access the Resource or to process, store, or transmit organization-controlled Data only when the Agency:

a) Verifies the implementation of required security controls on the external Resource as specified in the NCDOR Security Policy Manual and Security Plan; or
b) Retains approved Resource connection or processing agreements with the organizational entity hosting the external Resource.

CE2. The Agency restricts the use of portable storage devices in external Resources to authorized individuals for Data classified as Public or Confidential. For Data classified as FTI, it is the policy of the Agency that unless approved by the IRS Office of Safeguards:

a) Access to FTI from external Resources is prohibited; and
b) Use of non-Agency owned Resources to receive, process, store or transmit FTI is prohibited.

CE3. Usage of any non-Agency owned Resource requires notification to the IRS Office of Safeguards 45 days prior to implementation (See Section 7.4 45-Day Notification Reporting Requirements).

(AC-21) Data Sharing

Purpose

The purpose of the policy is to restrict inappropriate redisclosure of information.

Applicability

Public	Confidential	FTI
	AC-21	AC-21

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that sharing or redisclosure of Data classified as Confidential or FTI is strictly prohibited to only those authorized.

For FTI, authorization is defined in Internal Revenue Code 26 U.S.C. § Section 6103 - *Confidentiality and disclosure of returns and return information* and approved by the IRS Office of Safeguards.

(AC-22) Publicly Accessible Content

Purpose

The purpose of the policy is to establish the requirements around making information available for the general public.

Applicability

Public	Confidential	FTI
AC-22	AC-22	AC-22

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information and publicly accessible Resources.

It is the policy of the Agency that only the Public Information Officer (PIO), or his authorized delegate, may post information onto a publicly accessible Resource.

a) The PIO must ensure that publically accessible information does not contain Data;
b) The PIO must review the proposed content of Data prior to posting onto the publicly accessible Resource; and
c) The PIO must review the information on any publically accessible Resource for Data, at least quarterly, and remove it if discovered.

Awareness and Training Policy Family

(AT-1) Security Awareness and Training Policy & Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the awareness and training policy family.

Applicability

Public	Confidential	FTI
AT-1	AT-1	AT-1

Scope

This policy applies to all awareness and training procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the awareness and training procedures must be documented, disseminated and reviewed at least annually.

(AT-2) Security Awareness and Training

Purpose

The purpose of the policy is to establish the parameters for security awareness training.

Applicability

Public	Confidential	FTI
AT-2	AT-2 (CE2)	AT-2 (CE2)

Scope

This policy applies to all Staff.

It is the policy of the Agency that prior to granting Staff access to Data and Resources they must certify their understanding of the Agency's security policy and procedures for safeguarding information. Staff may not access Resources and Data unless certification, or recertification, has been completed. Security awareness and training is provided to Staff:

a) As part of initial training for new Staff;
b) When required by changes to Resources; and
c) Annually thereafter.

Control Enhancement

CE2. Training and certification must include the following provisions:

d) Include security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat training should bring awareness of the potential for Staff to use insider knowledge of sensitive Agency information to perform malicious actions, which could include the unauthorized access or redisclosure of Data; and
e) If the Data is classified as FTI, then per IRS 1075 IRC 6103(p)(4)(D)(6.3):
    1. Staff must be advised of the provisions of IRCs 7431, 7213, and 7213A;
    2. Training must also cover the incident response policy and procedure for reporting unauthorized disclosures and Data breaches;
    3. During this training, Staff must be made aware that disclosure restrictions and the penalties apply even after employment with the Agency has ended;
    4. Staff must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements; and
    5. Training certification must be documented and placed in the Agency's files for review and retained for at least five years.

(AT-3) Role-Based Security Training

Purpose

The purpose of the policy is to establish the need for training on this manual.

Applicability

Public	Confidential	FTI
AT-3	AT-3	AT-3

Scope

This policy applies to all Staff with roles related to information technology or information security. This includes, but is not limited to, enterprise architects, developers, software developers, acquisition/procurement officials, Resource managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to Resource-level software.

It is the policy of the Agency that Staff must be provided training on the content of the Technical Policies Manual:

a) As part of initial training for new Staff;
b) When required by changes to Resources; and
c) Annually thereafter.

(AT-4) Security Training Records

Purpose

The purpose of the policy is to establish the requirements to maintain records related to security training.

Applicability

Public	Confidential	FTI
AT-4	AT-4	AT-4

Scope

This policy applies to all Staff.

It is the policy of the Agency that IT Security documents and monitors individual security training activities including general security training and training related to specific Resources. Training records must be retained for five years.

Audit and Accountability Policy Family

(AU-1) Audit and Accountability Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the Audit and Accountability policy family.

Applicability

Public	Confidential	FTI
AU-1	AU-1	AU-1

Scope

This policy applies to all Audit and Accountability procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the audit and accountability procedures must be documented, disseminated and reviewed at least annually.

(AU-2) Audit Events

Purpose

The purpose of the policy is to establish the procedure requirements for audit events.

Applicability

Public	Confidential	FTI
AU-2	AU-2 (CE3)	AU-2 (CE3)

Scope

This policy applies to all Resources that contain Data.

It is the policy of the Agency that security-relevant events must enable the detection of unauthorized access to Data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of Data by each unique Staff member.

For each Resource:

a) Determine that it is capable, at a minimum, of auditing the following event types:

1. Log onto system;
2. Log off of system;
3. Change of password;
4. All Resource administrator commands, while logged on as Resource administrator;
5. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS);
6. Creation or modification of super-user groups;
7. Subset of security administrator commands, while logged on in the security administrator role;
8. Subset of Resource administrator commands, while logged on in the user role;
9. Clearing of the audit log file;
10. Startup and shutdown of audit functions;
11. Use of identification and authentication mechanisms (e.g., user ID and password);
12. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
13. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the Resource;
14. Changes made to an application or database by a batch file;
15. Application-critical record changes;
16. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
17. All Resource and Data interactions; and
18. Access to Data must be audited at the operating system, software, and database levels. Software and platforms have differing audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific Office of Safeguards SCSEM, which is available on the IRS Office of Safeguards website.

b) Coordinate the security audit function with other Agency entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; and
c) Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

Control Enhancement

CE3. Review and update the audited events at a minimum, annually.

(AU-3) Content of Audit Records

Purpose

The purpose of the policy is to establish the content for audit records.

Applicability

Public	Confidential	FTI
AU-3	AU-3 (CE1)	AU-3 (CE1)

Scope

This policy applies to all Resources.

It is the policy of the Agency that each Resource must:

a) Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any accounts associated with the event.

Control Enhancement

CE1. Generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject.

(AU-4) Audit Storage Capacity

Purpose

The purpose of the policy is to establish the requirements for retention of audit records.

Applicability

Public	Confidential	FTI
AU-4	AU-4	AU-4

Scope

This policy applies to all Resources.

It is the policy of the Agency to allocate sufficient storage capacity in order to retain records for seven years.

(AU-5) Response to Audit Processing Failures

Purpose

The purpose of the policy is to ensure that the appropriate Staff knows when an auditing process fails.

Applicability

Public	Confidential	FTI
AU-5	AU-5	AU-5 (CE1)

Scope

This policy applies to all Resources.

It is the policy of the Agency that all Resources must:

a) Alert IT Security in the event of an audit processing failure;
b) Monitor Resource operational status using operating system or Resource audit logs and verify functions and performance of the Resource. Logs shall be able to identify where Resource process failures have taken place and provide information relative to corrective actions to be taken by the Resource administrator.

Control Enhancement

CE1. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.

(AU-6) Audit Review, Analysis and Reporting

Purpose

The purpose of the policy is to ensure that audit logs are reviewed.

Applicability

Public	Confidential	FTI
AU-6	AU-6 (CE1)	AU-6

Scope

This policy applies to the logs being collected for Resources.

It is the policy of the Agency that IT Security Staff:

a) Review and analyze Resource audit records at least weekly for indications of unusual activity related to potential unauthorized access; and
b) Report findings according to the Agency security incident response policy. If the finding involves a potential unauthorized disclosure of Data classified as Federal Tax Information, the Agency

Disclosure Officer must be notified immediately who will then notify the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards.

Control Enhancement

CE1. The Agency employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

(AU-7) Audit Reduction and Report Generation

Purpose

The purpose of the policy is to ensure that audit logs can be easily reviewed and analyzed.

Applicability

Public	Confidential	FTI
	AU-7 (CE1)	AU-7

Scope

This policy applies to the logs being collected for Resources that store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that the Security Event Information Management (SEIM) Resource used by the Agency must provide an audit reduction and report generation capability that:

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

Control Enhancement

CE1. The SEIM provides the capability to process audit records for events of interest based on the content of specific audit record fields including, identities of individuals, event types, event times, event dates, Resources involved or IP addresses involved.

(AU-8) Time Stamps

Purpose

The purpose of the policy is to ensure that audit logs have accurate time stamps.

Applicability

Public	Confidential	FTI
AU-8	AU-8 (CE1)	AU-8 (CE1)

Scope

This policy applies to the logs being collected for all Resources.

It is the policy of the Agency that all Resources:

a) Use internal Resource clocks to generate time stamps for audit records; and
b) Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

Control Enhancement

CE1. All Resources compare and synchronize the internal Resource clocks to approved authoritative time sources (e.g., NIST, Naval Observatory)

(AU-9) Protection of Audit Information

Purpose

The purpose of the policy is to ensure that audit logs have accurate time stamps.

Applicability

Public	Confidential	FTI
AU-9	AU-9 (CE4)	AU-9 (CE4)

Scope

This policy applies to the logs being collected for all Resources.

It is the policy of the Agency that the Resources must protect audit information and audit tools from unauthorized access, modification, and deletion.

Control Enhancement

CE4. The Agency must authorize access to manage audit functionality only to IT Security Staff. Resource and network administrators must not have the ability to modify or delete audit log entries.

(AU-11) Audit Record Retention

Purpose

The purpose of the policy is to ensure that audit logs are kept for a sufficient amount of time.

Applicability

Public	Confidential	FTI
AU-11	AU-11	AU-11

Scope

This policy applies to the logs being collected for all Resources.

It is the policy of the Agency that audit records must be retained for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and Agency information retention requirements.

(AU-12) Audit Generation

Purpose

The purpose of the policy is to ensure that audit logs capture particular events.

Applicability

Public	Confidential	FTI
AU-12	AU-12	AU-12

Scope

This policy applies to the logs being collected for all Resources.

It is the policy of the Agency that Resources must:

a) Provide audit record generation capability for the auditable events defined in the policy Audit Events (AU-2);
b) Allow IT Security Staff to select which auditable events are to be audited by specific components of the Resource; and
c) Generate audit records for the events with the content defined in the policy Content of Audit Records (AU-3).

(AU-16) Cross Agency Auditing

Purpose

The purpose of the policy is to ensure that audit information is protected when working with service providers outside of the Agency.

Applicability

Public	Confidential	FTI
		AU-16

Scope

This policy applies to outsourced data centers or cloud providers who are providing Resources that store, transmit or process Data classified as Federal Tax Information (FTI). The provider must be held accountable to protect and share audit information with the Agency through the contract.

It is the policy of the Agency to coordinate the access and protection of audit information among external organizations when audit information is transmitted across Agency boundaries.

a) For cloud computing environments see IRS 1075 section 9.4.1 Cloud Computing Environments for mandatory requirements; and
b) For consolidated data centers see IRS 1075 5.4.2 Contractor- or Agency-Shared Facility—Consolidated Data Centers for mandatory requirements.

Security Assessment and Authorization Policy Family

(CA-1) Security Assessment and Authorization Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the security assessment and authorization policy family.

Applicability

Public	Confidential	FTI
CA-1	CA-1	CA-1

Scope

This policy applies to all security assessment and authorization procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the security assessment and authorization procedures must be documented, disseminated and reviewed at least annually.

(CA-2) Security Assessments

Purpose

The purpose of the policy is to establish the requirements for security assessments. Security assessments ensure that information security is built into organizational Resources; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions as part of security authorization processes; and ensure compliance to vulnerability mitigation procedures.

Applicability

Public	Confidential	FTI
CA-2	CA-2 (CE1)	CA-2

Scope

This policy applies to IT Security.

It is the policy of the Agency that the IT Security Department must:

a) Develop a security assessment plan that describes the scope of the assessment, including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities.
b) Assess the security controls in the Resource and its environment at a minimum on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
c) Produce a security assessment report that documents the results of the assessment;
d) Provide the results of the security control assessment to the Agency's Chief Information Officer and Chief Information Security Officer; and
e) Security assessments on Resources that store, process or transmit Data classified as Federal Tax Information is required immediately upon implementation and a minimum of every three years thereafter.

For Capabilities that will store, process or transmit Data classified as Public or Confidential as described in the DOR Security Policy, it is recommended that the Security Plan shall use the publication NIST 800-53A as the basis for the plan. The Data classification Public will equate to the NIST classification of Low Risk. The Data classification Confidential will equate to the NIST classification of Moderate Risk. (See NIST Special Publication 800-53A, web: irs.gov/uac/Safeguards-Program)

For Capabilities that will store, process or transmit Data classified as FTI as described in the DOR Security Policy, it is recommended that the Security Plan shall use the IRS Computer Security Compliance References including the Management, Operation and Technical for administrative controls and applicable Computer Security Evaluation Matrices for specific Databases, operating systems, etc. (see IRS Management, Operation and Technical and Web:irs.gov/pub/irs-utl/safeguards-scsem-mot.xls IRS Computer Security Compliance References, web:irs.gov/uac/Safeguards-Program)

It is recommended to use the NIST SP 800-115 Technical Guide to Information Security and Testing and Assessment for consistency and thoroughness.

Control Enhancement

CE1. The organization employs impartial assessors or assessment teams to conduct security control assessments. Impartiality is defined as assessors that are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results.

(CA-3) Resource Interconnections

Purpose

The purpose of the policy is to ensure that the Agency carefully consider the risks that may be introduced when Resources are connected to other Resources with different security requirements and security controls, both within organizations and external to organizations.

Applicability

Public	Confidential	FTI
CA-3	CA-3 (CE5)	CA-3 (CE5)

Scope

This policy applies to dedicated connections between Resources and does not apply to transitory, user-controlled connections such as email and website browsing.

It is the policy of the Agency that the CIO must authorize connections from the Resource to Resource.

a) To connect to an external Resource there must be an Interconnection Security Agreement. The agreement must document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. The Agency may also incorporate Interconnection Security Agreement information into Memorandums of Understanding (MOUs) for interconnections established between state agencies;
b) If interconnecting systems are within the Agency, the Interconnection Security Agreement is not needed and may simply describe the interface characteristics between those interconnecting Resources in their respective security plans; and
c) IT Security must review and update the system interconnection or Resource security plan on an annual basis and the CIO must reauthorize the connection.

Control Enhancement

CE5. The connection must employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit Data classified as Federal Tax Information to connect to external information systems.

(CA-5) Plan of Action and Milestones

Purpose

The purpose of the policy is to ensure that the Agency documents remedial actions.

Applicability

Public	Confidential	FTI
CA-5	CA-5	CA-5

Scope

This policy applies to any known weakness or deficiency identified by self-assessments, internal inspections, external audits and any other vulnerabilities identified for all Resources.

It is the policy of the Agency the Plan of Action and Milestones (POA&M) is reflected in the IT tracking systems JIRA to track vulnerabilities identified. The POA&M will be updated quarterly, at a minimum.

a) Each issue will be identified by the portfolio segment type "Compliance" and be assigned a value based on the combination of Impact (Severity) and the level of effort that will be required to remediate the issue;
b) All items in JIRA will be processed according to the portfolio management procedures;
c) Remediation plans will be documented as part of the Service Design process;
d) Remediation and testing will be executed as defined by the Service Transition process; and
e) All remediation items will be audited by IT Security once the item has been moved into Service Operations and results documented in the tool.

(CA-6) Security Authorization

Purpose

The purpose of the policy is to authorize all Resources prior to being implemented for use.

Applicability

Public	Confidential	FTI
CA-6	CA-6	CA-6

Scope

This policy applies to all Resources.

It is the policy of the Agency that the CIO is the authorizing official for all Resources and must provide authorization before commencing operations. In addition, all Resource authorizations must be approved again every three years or if there is a significant change to the Resource. In order to submit for authorization the following information must be provided to the CIO:

a) The CTO must approve that the architecture adheres to the established standards, or approve the exception; and
b) The CISO must approve that the Resource meets all relevant security policies and controls or approve the exception.

(CA-7) Continuous Monitoring

Purpose

The purpose of the policy is to ensure that Resources are monitored to protect confidentiality and integrity of Data appropriately.

Applicability

Public	Confidential	FTI
CA-7	CA-7 (CE1)	CA-7

Scope

This policy applies to all Resources.

It is the policy of the Agency that IT Security must implement a continuous monitoring strategy and implement a continuous monitoring program that includes defined metrics to be monitored annually, ongoing security control assessments and continual security status monitoring.

Control Enhancement

CE1. The organization employs impartial assessors or assessment teams that to monitor the security controls in the Resource on an ongoing basis. Impartiality is defined as assessors that are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results.

Configuration Management Policy Family

(CM-1) Configuration Management Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the configuration management policy family.

Applicability

Public	Confidential	FTI
CM-1	CM-1	CM-1

Scope

This policy applies to all configuration management procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the configuration management procedures must be documented, disseminated and reviewed at least annually.

(CM-2) Baseline Configuration

Purpose

The purpose of the policy is to ensure that baseline configurations are maintained.

Applicability

Public	Confidential	FTI
CM-2	CM-2 (CE1) (CE3)(CE7)	CM-2 (CE1)

Scope

This policy applies to all Resources.

It is the policy of the Agency to develop, document, and maintain under configuration control, a current baseline configuration of the Resource.

Control Enhancements

CE1. The Agency must review and update the baseline configuration of the Resource:

a) At a minimum annually;
b) When required due to system upgrades, patches, or other significant changes; and
c) As an integral part of Resource component installations and upgrades.

For Data classified as FTI, the Agency must use SCSEMs provided on the Office of Safeguards website for developing a Resource baseline configuration.

CE3. The Agency retains at least 1 previous configuration version to support rollback.

CE7. The Agency may choose to:

a) Issues mobile devices with special configurations to individuals traveling to locations that the Agency deems to be of significant risk; and
b) Applies standard configurations to the devices when the individuals return.

(CM-3) Configuration Change Control

Purpose

The purpose of the policy is to ensure that changes to Resources are controlled, documented and that security is properly considered.

Applicability

Public	Confidential	FTI
	CM-3 (CE2)	CM-3 (CE2)

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that changes to Resources is methodical. The Agency will;

a) Determine the types of changes to Resources that are configuration controlled;
b) Review proposed configuration-controlled changes and approve or disapprove such changes with explicit consideration for security impact analyses;
c) Document configuration change decisions;
d) Implement approved configuration-controlled changes;
e) Retain records of configuration-controlled changes to the Resource for the life of the system;
f) Audit and review activities associated with configuration-controlled changes; and
g) Coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur.

Control Enhancement

CE2. The Agency will also test, validate, and document changes to the Resource before implementing the changes on the operational system.

(CM-4) Security Impact Analysis

Purpose

The purpose of the policy is to ensure that configuration changes to Resources must be reviewed to prevent negative impact to security.

Applicability

Public	Confidential	FTI
CM-4	CM-4	CM-4

Scope

This policy applies to all Resources.

It is the policy of the Agency that prior to implementing changes being made to resources that IT Security must analyze the proposed changes for security impacts.

(CM-5) Access Restrictions for Change

Purpose

The purpose of the policy is to ensure that the Staff who can make changes to Resources is limited.

Applicability

Public	Confidential	FTI
	CM-5	CM-5

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency to define, document, approve and enforce physical and logical access restriction associated with change to Resources.

(CM-6) Configuration Settings

Purpose

The purpose of the policy is to ensure that Resource configuration changes are properly documented.

Applicability

Public	Confidential	FTI
CM-6	CM-6	CM-6

Scope

This policy applies to all Resources.

It is the policy of the Agency that for all Resources configuration settings must be documented using IRS Office of Safeguardsapproved compliance requirements (e.g. SCSEMs, assessment tools) that reflect the most restrictive mode consistent with operational requirements.

a) Implement approved configuration settings;
b) Identify, document and approve any deviations from established configuration settings; and
c) Monitor and control changes to the configuration settings.

(CM-7) Least Functionality

Purpose

The purpose of the policy is to ensure that Resources are configured with only the functionality that is required, and no more.

Applicability

Public	Confidential	FTI
CM-7	CM-7 (CE1) (CE2) (CE4)	CM-7

Scope

This policy applies to all Resources.

It is the policy of the Agency for all Resources that they are configured with only essential capabilities.

a) Restrict or prohibit the use of functions, ports, protocols or services. For Data classified as FTI, restrict or prohibit the use of functions, ports, protocols or services as defined in the IRS Office of Safeguards-approved compliance requirement (e.g. IRS SCSEMs, assessment tools);
b) Review the Resource as part of the vulnerability assessments to identify unnecessary or non-secure functions, ports, protocols, and services per Vulnerability Scanning (RA-5); and
c) Disable defined functions, ports, protocols, and services within the Resource deemed to be unnecessary or non-secure.

Control Enhancements

CE1. The Agency:

a) Reviews the Resource annually to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
b) Disables defined functions, ports, protocols, and services within the Resource deemed to be unnecessary or non-secure.

CE4. The Agency IT Security Department:

a) Identifies software programs not authorized to execute on Resources;
b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the Resource; and
c) Reviews and updates the list of unauthorized software programs annually.

(CM-8) Resource Component Inventory

Purpose

The purpose of the policy is to ensure that Resource component inventory is properly maintained.

Applicability

Public	Confidential	FTI
CM-8	CM-8 (CE1) (CE3) (CE5)	CM-8 (CE1)

Scope

This policy applies to all Resources.

It is the policy of the Agency for all Resources:

a) That there is an inventory of components that:
    1. Accurately reflects the current state;
    2. Includes all components;

3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes information deemed necessary to achieve effective Resource component accountability.

b) Review and update the component inventory through periodic manual inventory checks or network monitoring tool that automatically maintains inventory;
c) All additional requirements for maintaining a Resource component inventory are provided in NIST SP 800-70 Rev 2 Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers.

Control Enhancements

CE1. The Agency updates the inventory of Resource components as an integral part of component installations, removals and updates.

CE3. The Agency:

a) Employs automated mechanisms weekly to detect the presence of unauthorized hardware, software, and firmware components within the authorization boundary of the capability; and
b) Disables network access by such components; isolates the components; notifies the CISO and CIO.

CE5. The Agency verifies that all components within the authorization boundary of the Resource are not duplicated in other Resource component inventories.

(CM-9) Configuration Management

Purpose

The purpose of the policy is to set forth the requirements for a configuration management plan.

Applicability

Public	Confidential	FTI
	CM-9	CM-9

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency to develop, document and implement a configuration management plan for all Resources that:

a) Addresses roles, responsibilities, and configuration management processes and procedures;
b) Establishes a process for identifying configuration items throughout the system development lifecycle (SDLC) and for managing the configuration of the configuration items;
c) Defines the configuration items for the information system and places the configuration items under configuration management; and
d) Protects the configuration management plan from unauthorized disclosure and modification.

(CM-10) Software Usage Restrictions

Purpose

The purpose of the policy is to make sure that software is licensed properly.

Applicability

Public	Confidential	FTI
CM-10	CM-10	CM-10 (CE1)

Scope

This policy applies to all software.

It is the policy of the Agency that all software must be used in accordance with contract agreements and copyright laws.

a) All software usage must be tracked and improper copying or distribution is strictly prohibited
b) Peer-to-peer file sharing technology is prohibited in order to prevent unauthorized distribution, display, performance or reproduction of copyrighted work.

Control Enhancement

CE1. Open source software must be legally licensed, approved for use by the CISO and adhere to a secure configuration baseline checklist from the U.S. Government or industry.

(CM-11) User-Installed Software

Purpose

The purpose of the policy is to make sure that software installed by non-IT Staff does not violate contracts, copyright laws or create security issues.

Applicability

Public	Confidential	FTI
CM-11	CM-11	CM-11

Scope

This policy applies to all software that is installed by Staff outside of the IT Department.

It is the policy of the Agency that software may not be installed by non-IT Staff unless specifically authorized by the CIO. Software installation must be prohibited, and compliance monitored, through automated methods when practical.

Contingency Planning Policy Family

(CP-1) Contingency Planning Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the contingency planning policy family.

Applicability

Public	Confidential	FTI
CP-1	CP-1	CP-1

Scope

This policy applies to all contingency planning procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the contingency planning procedures must be documented and disseminated and reviewed at least annually.

(CP-2) Contingency Plan

Purpose

The purpose of the policy is to develop plans to ensure that Data and Resources are available, based on the risk assessment.

Applicability

Public	Confidential	FTI
CP-2	CP-2 (CE1) (CE3)(CE8)	CP-2

Scope

This policy applies to all Resources.

It is the policy of the Agency that each Resource:

a) Must have a contingency plan that:
    1. Identifies essential missions and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
    5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    6. Is reviewed and approved by the CIO.
b) Distributes copies of the contingency plan to key contingency personnel, at a minimum;
c) Coordinates contingency planning activities with incident handling activities;
d) Reviews the contingency plan for the Resource annually;
e) Updates the contingency plan to address changes to the organization, Resources, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f) Communicates contingency plan changes to key contingency personnel, at a minimum; and
g) Protects the contingency plan from unauthorized disclosure and modification.

Control Enhancements

CE1. The Agency coordinates contingency plan development with organizational elements responsible for related plans.
CE3. The Agency plans for the resumption of essential missions and business functions within the stated recovery objective of each capability after contingency plan activation.
CE8. The Agency identifies critical information system assets supporting essential missions and business functions.

(CP-3) Contingency Training

Purpose

The purpose of the policy is to make sure that Staff who could be involved in the recovery of Resources is trained to execute contingency plans.

Applicability

Public	Confidential	FTI
CP-3	CP-3	CP-3

Scope

This policy applies to all Resources.

It is the policy of the Agency that contingency training is provided to Resource users consistent with assigned roles and responsibilities prior to assuming a contingency role or responsibility. Training should be refreshed in the event of a major change to the Resource and annually thereafter.

(CP-4) Contingency Plan Testing

Purpose

The purpose of the policy is to make sure that contingency plans are tested.

Applicability

Public	Confidential	FTI
CP-4	CP-4 (CE1)	CP-4

Scope

This policy applies to all Resources.

It is the policy of the Agency that prior to any Resource being released into production for general use that the contingency plan is tested and then, at a minimum, annually thereafter.

a) The plan should be tested for effectiveness to ensure that the Agency is ready to execute it if needed; and
b) Contingency plan testing results should be reviewed and corrective actions implemented if needed.

Control Enhancement

CE1. The Agency coordinates contingency plan testing with organizational elements responsible for related plans.

(CP-6) Alternate Storage Site

Purpose

The purpose of the policy is to endure the recovery of backup information in the event of a disaster.

Applicability

Public	Confidential	FTI
	CP-6 (CE1)(CE3)	CP-6

Scope

This policy applies to all backup information on Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency to

a) Establish an alternative storage site, including necessary agreements to permit the storage and retrieval of Resource backup information; and
b) Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site. If the Resource backup information contains Data classified as Federal Tax Information, the Agency must ensure that the alternative storage site provides information security safeguards that meet the IRS Publication 1075 revision October 2015 Section 4.2 – Minimum Protection Standards and the disclosure provisions of Internal Revenue Code § 6103 Confidentiality and disclosure of returns.

Control Enhancements

CE1. The Agency identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
CE3. The Agency identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(CP-7) Alternate Processing Site

Purpose

The purpose of the policy is to make sure that normal operations are resummed in the event of a disaster.

Applicability

Public	Confidential	FTI
	CP-7 (CE1)(CE2)(CE3)	CP-7

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency to establish an alternative processing site including necessary agreements to permit the transfer and resumption of Resources for essential missions/business functions within the recovery period identified for the Resource (See CP-2).

a) Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the time period defined in the contingency plan for transfer/resumption; and
b) Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site. In the event that the Resource stores, processes or transmits Data classified as Federal Tax Information, the alternate processing site must provide information security safeguards that meet the minimum protection standards and the disclosure provisions of Internal Revenue Code § 6103 Confidentiality and disclosure of returns.

Control Enhancements

CE1. The Agency identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
CE2. The Agency identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
CE3. The Agency develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

(CP-9) Resource Backup

Purpose

The purpose of the policy is to ensure the backup of Agency information.

Applicability

Public	Confidential	FTI
CP-9	CP-9 (CE2)	CP-9

Scope

This policy applies to all Resources.

It is the policy of the Agency to conduct backups of user-level information, system-level information, and security-related documentation consistent with the defined frequency in the Resource contingency plan. In the event that the backup contains Data classified as Federal Tax Information, the confidentiality of backup information at storage locations will be protected pursuant to Internal Revenue Code § 6103 *Confidentiality and disclosure of returns* requirements.

(CP-10) Resource Recovery and Reconstitution

Purpose

The purpose of the policy is to ensure the Agency can recover from a disaster.

Applicability

Public	Confidential	FTI
CP-10	CP-10 (CE2)	CP-10

Scope

This policy applies to all Resources.

It is the policy of the Agency to provide for the recovery and reconstitution of the Resource to a known state after a disruption, compromise, or failure.

Control Enhancement

CE2. The Resource implements transaction recovery if it is transaction-based.

Identification and Authentication Policy Family

(IA-1) Identification and Authentication Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the identification and authentication policy family.

Applicability

Public	Confidential	FTI
IA-1	IA-1	IA-1

Scope

This policy applies to all identification and authentication procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the identification and authentication procedures must be documented, disseminated and reviewed at least annually

(IA-2) Identification and Authentication (Staff)

Purpose

The purpose of the policy is to make sure that Staff can be uniquely identified and authenticated prior to accessing a Resource.

Applicability

Public	Confidential	FTI
IA-2 (CE1)(CE12)	IA-2 (CE1) (CE2) (CE3) (CE8) (CE11) (CE12)	IA-2 (CE1)(CE2) (CE11)

Scope

This policy applies to all Resources.

It is the policy of the Agency that each Resource must be able to uniquely identify and authenticate Staff or processes acting on behalf of Staff (i.e. Staff may not share accounts).

Control Enhancements

CE1. The Resource implements multifactor authentication for network access to privileged accounts.

CE2. The Resource implements multifactor authentication for network access to non-privileged accounts.

CE3. The information system implements multifactor authentication for local access to privileged accounts.

CE8. The Resource implements replay-resistant authentication mechanisms for network access to privileged accounts.

CE11. The Resource implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. Note: NIST SP 800-63-2 allows the use of software tokens.

CE12. The Resource accepts and electronically verifies Personal Identity Verification (PIV) credentials.

(IA-3) Identification and Authentication (Devices)

Purpose

The purpose of the policy is to make sure that devices are uniquely identified.

Applicability

Public	Confidential	FTI
	IA-3	IA-3

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that each Resource must be able to uniquely identify and authenticate devices before establishing a connection.

(IA-4) Identifier Management

Purpose

The purpose of the policy is to make sure that Resource identifiers are properly managed. Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers.

Applicability

Public	Confidential	FTI
IA-4	IA-4	IA-4

Scope

This policy applies to all Resource identifiers. Management of individual identifiers is not applicable to shared Resource accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the Resource accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This policy also addresses individual identifiers not necessarily associated with Resource accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to Resources). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

It is the policy of the Agency that Resource identifiers must be managed by:

a) Receiving authorization from the CIO to assign an individual, group, role, or Resource identifiers;
b) Selecting an identifier that identifies Staff, group, role, or Resource;
c) Assigning the identifier to the intended Staff, group, role, or Resource;
d) Preventing reuse of identifiers; and
e) Disabling the identifier after 120 days.

(IA-5) Authenticator Management

Purpose

The purpose of the policy is to make sure that authenticators are properly managed.

Applicability

Public	Confidential	FTI
IA-5 (CE1) (CE11)	IA-5 (CE1) (CE2) (CE3) (CE11)	IA-5 (CE1)

Scope

This policy applies to all Resource authenticators. Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual

authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within Resources (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges).

It is the policy of the Agency that we manage Resource authenticators by:

a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b) Establishing initial authenticator content for authenticators defined by the Agency. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length);
c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators ;
e) Changing default content (e.g., the initial password) of authenticators prior to information system installation;
f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g) Changing/refreshing authenticators;
h) Protecting authenticator content from unauthorized disclosure and modification;
i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j) Changing authenticators for group/role accounts when membership to those accounts changes.

Control Enhancements

CE1. For password-based authentication the Resource must:

a) Enforce minimum password complexity of:
    1. Eight characters;
    2. At least one numeric and at least one special character;
    3. A mixture of at least one uppercase and at least one lowercase letter; and
    4. Storing and transmitting only encrypted representations of passwords.
b) Enforce password minimum lifetime restriction of one day;
c) Enforce non-privileged account passwords to be changed at least every 90 days;
d) Enforce privileged account passwords to be changed at least every 60 days;
e) Prohibit password reuse for 24 generations;
f) Allow the use of a temporary password for system logons requiring an immediate change to a permanent password; and
g) Password-protect system initialization (boot) settings.

CE2. The information system, for PKI-based authentication:

a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b) Enforces authorized access to the corresponding private key;
c) Maps the authenticated identity to the account of the individual or group; and
d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

CE5. The Agency requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.
CE11. For hardware token-based authentication, the Resource employs mechanisms that satisfy Agency specifics such as working with a particular PKI.

(IA-6) Authenticator Feedback

Purpose

The purpose of the policy is to make sure that passwords aren't seen by others.

Applicability

Public	Confidential	FTI
IA-6	IA-6	IA-6

Scope

This policy applies to all Resources.

It is the policy of the Agency that the Resource obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

(IA-7) Cryptographic Module Authentication

Purpose

The purpose of the policy is to make sure that encryption is strong enough.

Applicability

Public	Confidential	FTI
IA-7	IA-7	IA-7

Scope

This policy applies to all encryption used to protect Data classified as Federal Tax Information (FTI).

It is the policy of the Agency that all Resources must implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Validation provides assurance that when the Agency implements cryptography to protect FTI, the encryption functions have been examined in detail and will operate as intended.

All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information.

(IA-8) Identification and Authentication (non-Staff)

Purpose

The purpose of the policy is to make sure that non-Staff can be uniquely identified and authenticated prior to accessing a Resource.

Applicability

Public	Confidential	FTI
IA-8(CE2)(CE3)(CE4)	IA-8(CE1) (CE2)(CE3)(CE4)	IA-8

Scope

This policy applies to all Resources.

It is the policy of the Agency that each Resource must be able to uniquely identify and authenticate non-Staff or processes acting on behalf of non-Staff (i.e. Staff is strictly prohibited from sharing accounts).

Control Enhancements

CE1. The Resource accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4

CE2. The Resource accepts only FICAM-approved third-party credentials.

Supplemental Guidance: This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.

CE3. The Agency employs only FICAM-approved Resource components to accept third-party credentials.

Supplemental Guidance: This control enhancement typically applies to Resources that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.

CE4. The Resource conforms to FICAM-issued profiles.

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.

Major Incident Response Policy Family

(IR-1) Major Incident Response Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the Major Incident response policy family.

Applicability

Public	Confidential	FTI
IR-1	IR-1	IR-1

Scope

This policy applies to all Major Incident response procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the Major Incident response procedures must be documented, disseminated and reviewed at least annually.

a) The procedures must also include a definition and examples of what a Major Incident; and
b) The NIST Special Publication 800-61 Revision 2 should be used as a guide for incident response procedures.

(IR-2) Major Incident Response Training

Purpose

The purpose of the policy is to ensure that Staff are trained in Major Incident response processes.

Applicability

Public	Confidential	FTI
IR-2	IR-2	IR-2

Scope

This policy applies to all Staff involved in Major Incident response processes.

It is the policy of the Agency that Staff are trained in their Major Incident response roles prior to assuming a Major Incident response role or responsibility, when a change occurs in a Major Incident response process for a Resource and annually thereafter.

(IR-3) Major Incident Response Testing

Purpose

The purpose of the policy is to ensure that Major Incident responses are tested annually.

Applicability

Public	Confidential	FTI
	IR-3(CE2)	IR-3

Scope

This policy applies to all Staff involved in Major Incident response processes as they relate to Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that Major Incident response processes are tested annually.

a) The Agency must perform a tabletop exercise using scenarios that would be classified as a Major Incident including a breach of Data classified as Federal Tax Information (FTI);
b) All Staff with significant Major Incident response capabilities, including those responsible for maintaining consolidated data centers and off-site storage, must be included in the tabletop exercise; and
c) Each exercise must produce and after-action report to improve the process.

For Major Incidents where FTI is involved:

d) The Agency must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the Agency Disclosure Officer must contact TIGTA and the IRS immediately. The Agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the Major Incident;
e) The Office of Safeguards will coordinate with the Agency regarding appropriate follow-up actions required to be taken by the Agency to ensure continued protection of FTI;
f) Once the Major Incident has been addressed, the Agency will conduct a post-action review to ensure the Major Incident response policies and procedures provide adequate guidance;
g) Any identified deficiencies in the Major Incident response policies and procedures should be resolved immediately; and
h) Additional training on any changes to the Major Incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.

Control Enhancement

CE2. The Agency coordinates incident response testing with organizational elements responsible for related plans.

(IR-4) Major Incident Handling

Purpose

The purpose of the policy is to ensure that Major Incident processes are coordinated and improved over time.

Applicability

Public	Confidential	FTI
IR-4	IR-4 (CE1)	IR-4

Scope

This policy applies to the Major Incident response process.

It is the policy of the Agency that Major Incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery

a) Coordinate Major Incident handling activities with contingency planning activities; and
b) Incorporate lessons learned from ongoing Major Incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

Control Enhancement

CE1. The Agency employs automated mechanisms to support the incident handling process.

(IR-5) Major Incident Monitoring

Purpose

The purpose of the policy is to ensure that Major Incidents are documented.

Applicability

Public	Confidential	FTI
IR-5	IR-5	IR-5

Scope

This policy applies to the Major Incidents.

It is the policy of the Agency that Major Incidents are tracked and documented.

(IR-6) Major Incident Reporting

Purpose

The purpose of the policy is to ensure that Major Incidents are reported timely and to all required parties .

Applicability

Public	Confidential	FTI
IR-6	IR-6 (CE1)	IR-6

Scope

This policy applies to the Major Incidents.

It is the policy of the Agency that Staff report suspected security incidents to the Service Desk upon discovery of the incident. The Service Desk will notify IT Security. If the security incident may involve Data classified as Federal Tax Information, IT Security will notify the Disclosure officer.

Control Enhancement

CE1. The Agency employs automated mechanisms to assist in the reporting of security incidents.

(IR-7) Incident Response Assistance

Purpose

The purpose of the policy is to ensure that Major Incidents are reported.

Applicability

Public	Confidential	FTI
IR-7	IR-7 (CE1)	IR-7

Scope

This policy applies to the Major Incidents.

It is the policy of the Agency that IT Security will provide an incident response support resource, integral to the Agency incident response capability that offers advice and assistance to users of Resources for the handling and reporting of security incidents.

Control Enhancement

CE1. The Agency employs automated mechanisms to increase the availability of incident response-related information and support.

(IR-8) Incident Response Plan

Purpose

The purpose of the policy is to ensure that there is a Major Incidents response plan.

Applicability

Public	Confidential	FTI
IR-8	IR-8	IR-8

Scope

This policy applies to the Major Incidents.

It is the policy of the Agency that the there is a process for dealing with Major Incidents.

a) The process:
    1. Provides the Agency with a process for implementing its Major Incident response capability;
    2. Describes the structure of the Major Incident response capability;
    3. Provides a high-level approach for how the Major Incident response process fits into the overall Agency;
    4. Meets the unique requirements of the Agency, which relate to mission, size, structure, and functions;
    5. Defines Major Incidents that are reportable to IRS of Safeguards;
    6. Provides metrics for measuring the Major Incident response capability within the Agency;
    7. Defines the resources and management support needed to effectively maintain and mature a Major Incident response process; and
    8. Is reviewed and approved by CIO.
b) Distribute copies of the Major Incident response process to authorized Major Incident response personnel;

c) Review the Major Incident response process at a minimum on an annual basis or as an after-action review;
d) Update the Major Incident response process to address system/Agency changes or problems encountered during plan implementation, execution, or testing;
e) Communicate Major Incident response process changes to authorized Major Incident response personnel; and
f) Protect the Major Incident response procedure from unauthorized disclosure and modification.

(IR-9) Data Spillage Response

Purpose

The purpose of the policy is to ensure that if Data is mishandled, that there is a process to address it.

Applicability

Public	Confidential	FTI
		IR-9

Scope

This policy applies to mishandled Data. Spillage refers to instances where Data categorized as Federal Tax Information (FTI) is inadvertently placed on a Resource that is not authorized to process such Data. Such spills often occur when Data that is initially thought to be classified as Public is transmitted to an appropriate Resource and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required.

It is the policy of the Agency that the there is a process for dealing with Data spillage. The process must respond to spills by:

a) Identifying the specific Data involved in the Resource contamination;
b) Alerting authorized Major Incident response personnel of the spill using a method of communication not associated with the spill;
c) Isolating the contaminated Resource or component;
d) Eradicating the Data from the contaminated Resource or component; and
e) Identifying other Resources or components that may have been subsequently contaminated.

Maintenance Policy Family

(MA-1) Resource Maintenance Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the maintenance policy family.

Applicability

Public	Confidential	FTI
MA-1	MA-1	MA-1

Scope

This policy applies to all resource maintenance procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the maintenance procedures must be documented, disseminated and reviewed at least annually.

(MA-2) Controlled Maintenance

Purpose

The purpose of the policy is to ensure that maintenance activities on Resources are managed.

Applicability

Public	Confidential	FTI
MA-2	MA-2	MA-2

Scope

This policy applies to all Resources.

It is the policy of the Agency to:

a) Schedule, perform, document, and review records of maintenance and repairs on Resources and components in accordance with manufacturer or vendor specifications and Agency requirements;
b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the Resource is serviced on site or removed to another location;

c) Require that the CIO explicitly approve the removal of the Resource or components from Agency facilities for off-site maintenance or repairs;
d) Sanitize Resources to remove all Data classified as Data from associated media prior to removal from Agency facilities for off-site maintenance or repairs; and
e) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions and update Agency maintenance records accordingly.

(MA-3) Maintenance Tools

Purpose

The purpose of the policy is to ensure that maintenance tools are appropriate.

Applicability

Public	Confidential	FTI
	MA-3 (CE1) (CE2)	MA-3

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that the CISO must approve, control, and monitor Resource maintenance tools.

Control Enhancements

CE1. The Agency inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

CE2. The Agency checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

(MA-4) Non-Local Maintenance

Purpose

The purpose of the policy is to ensure that maintenance that is provided remotely doesn't compromise the confidentiality or integrity of Data or Resources.

Applicability

Public	Confidential	FTI
MA-4	MA-4 (CE2)	MA-4 (CE2)

Scope

This policy applies to all Resources.

It is the policy of the Agency that the CISO must:

a) Approve and monitor non-local maintenance and diagnostic activities;
b) Allow the use of non-local maintenance and diagnostic tools only as consistent with Agency policy and documented in the security plan for the Resource;
c) Employ multi-factor authenticator in the establishment of non-local maintenance and diagnostic sessions;
d) Maintain records for non-local maintenance and diagnostic activities; and
e) Terminates session and network connections when non-local maintenance is completed.

Control Enhancement

CE2. The Agency documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(MA-5) Maintenance Staff

Purpose

The purpose of the policy is to ensure that maintenance Staff is properly tracked.

Applicability

Public	Confidential	FTI
MA-5	MA-5	MA-5

Scope

This policy applies to all Staff performing maintenance on Resources.

It is the policy of the Agency the CISO

a) Establish a process for maintenance Staff authorization and maintain a list of authorized maintenance organizations or personnel;

b) Ensure that non-escorted Staff performing maintenance on the Resource have required access authorizations; and
c) Designate Agency Staff with required access authorizations and technical competence to supervise the maintenance activities of Staff who do not possess the required access authorizations.

Media Protection Policy Family

(MP-1) Media Protection Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the media protection policy family.

Applicability

Public	Confidential	FTI
MP-1	MP-1	MP-1

Scope

This policy applies to all Media protection procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the Media protection procedures must be documented, disseminated and reviewed at least annually.

(MP-2) Media Protection

Purpose

The purpose of the policy is to ensure that Data is properly handled and unauthorized disclosure is prevented.

Applicability

Public	Confidential	FTI
MP-2	MP-2	MP-2

Scope

This policy applies to all Media.

It is the policy of the Agency that all Media is protected by:

a) Restricting access to Media to only authorized individuals;
b) Protecting Media during transport outside of controlled areas; and
c) Sanitizing Media prior to disposal or release for reuse.

(MP-3) Media Marking

Purpose

The purpose of the policy is to ensure that Data is properly handled and unauthorized disclosure is prevented.

Applicability

Public	Confidential	FTI
	MP-3	MP-3

Scope

This policy applies to all Media that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that all Media must be labeled as the most restrictive Data Classification as is stored on the Media.

a) Any Media that contains any Data classified, as Federal Tax Information must be labeled as "Federal Tax Information".
    1. The Agency must label removable Media and Resource output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.
b) Any Media that contains no Data classified as FTI, but does have Data classified as Confidential must be labeled as "DOR Confidential;" and
c) Any Media that contains no Data classified as FTI or Confidential must be labeled as "DOR Public".

(MP-4) Media Storage

Purpose

The purpose of the policy is to ensure that Data is properly stored.

Applicability

Public	Confidential	FTI
	MP-4	MP-4

Scope

This policy applies to all Media that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that all Media must be:

a) Physically controlled and securely stored; and
b) Protected until it is destroyed or sanitized using approved equipment, techniques, and procedures.

For Data classified as Federal Tax Information, see IRS Publication 1075 Revision October 2014 - Section 4.0, Secure Storage—IRC 6103(p)(4)(B), on additional secure storage requirements.

(MP-5) Media Transport

Purpose

The purpose of the policy is to ensure that the confidentiality of Data is maintained during transport.

Applicability

Public	Confidential	FTI
	MP-5 (CE4)	MP-5 (CE4)

Scope

This policy applies to all Media that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that:

a) All Media must be protected and controlled during transport outside of controlled areas;
b) Accountability for the Media is maintained during transport outside of controlled areas; and
c) The Agency must document activities associated with the transport of Media:
    1. For Data classified as Federal Tax Information (FTI) the Agency must use transmittal forms (transmittals) or an equivalent tracking method to ensure FTI reaches its intended

destination. See IRS Publication 1075 Rev October 2014, Section 4.4, FTI in Transit, for more information on transmittals and media transport requirements.

d) The Agency restricts the activities associated with the transport of Media to authorized personnel.

Control Enhancement

CE4. The Resource must implement a cryptographic mechanism that is FIPS 140-2 compliant to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

(MP-6) Media Sanitization

Purpose

The purpose of the policy is to ensure that the confidentiality of Data is maintained through sanitization.

Applicability

Public	Confidential	FTI
MP-6	MP-6	MP-6 (CE1)

Scope

This policy applies to all Media.

It is the policy of the Agency that:

a) Sanitizes all media prior to disposal, release out of organizational control, or release for reuse using IRS-approved sanitization techniques in accordance with applicable federal and organizational standards and policies; and
b) Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Control Enhancement

CE1.Processes should be in place to review, approve, track, document, and verify media sanitization and disposal actions. For Data classified as FTI:

a) Processes should be in place to ensure that the review and approval of media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing Staff who reviewed and approved sanitization and disposal actions, types of Media sanitized, specific files stored on the media, sanitization methods used, date and time of

the sanitization actions, personnel who performed the sanitization, verification actions taken, Staff who performed the verification, and disposal action taken;

b) The procedures must include the verification that the sanitization of the Media was effective prior to disposal (see Information Handling and Retention (SI-12));

c) The use of Media on Resources that receive, store, process or transmit FTI must be restricted using physical or automated controls; and

d) Additional requirements for protecting FTI during Media sanitization are provided in IRS Publication 1075 Revision October 2014 - Exhibit 10, *Data Warehouse Security Requirements* and Section 9.4.7, *Media Sanitization*.

Planning

(PL-1) Security Planning Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the security planning policy family.

Applicability

Public	Confidential	FTI
PL-1	PL-1	PL-2

Scope

This policy applies to IT Security.

It is the policy of the Agency that procedures to facilitate the implementation of the security planning procedures must be documented, disseminated and reviewed at least annually.

(PL-2) Resource Security Plan

Purpose

The purpose of the policy is to ensure that every resource has a security plan.

Applicability

Public	Confidential	FTI
PL-2	PL-2(CE3)	PL-2

Scope

This policy applies to all Resources.

It is the policy of the Agency that every Resource must have a Resource Security Plan.

Each Resource that is being implemented or undergoing a major modification, must have a Resource Security Plan, prior to being placed into general production, that:

a) Is consistent with the organization's enterprise architecture;
b) Explicitly defines the authorization boundary for the system and is documented with a Technical Architecture diagram;
c) Describes the operational context of the Resource in terms of missions and business processes as documented by business process diagrams;
d) Provides the security categorization of the Resource including supporting rationale. Categorizations are based on the most restrictive Data classification that the Resource will store, process or transmit as defined in the General Security Policies Manual;
e) Describe the operational environment for the Resources and relationships with or connections to other information systems as documented in a Solution Architecture;
f) Provides an explanation of the security requirements, control by control, for the Resource as approved by the Chief Information Security Officer;
g) Is reviewed and approved by the Chief Information Officer prior to the Resource being placed into general production; and
h) The Resource Security Plan should be developed using the NIST Special Publication 800-18 Revision 1.

Control Enhancement

CE3. The Agency plans and coordinates security-related activities affecting the Resource with the Resource Owner before conducting such activities in order to reduce the impact on other organizational entities.

(PL-4) Rules of Behavior

Purpose

The purpose of the policy is to make sure Staff understands their responsibilities as it relates to Resource usage and Data security.

Applicability

Public	Confidential	FTI
PL-4	PL-4 (CE1)	PL-4 (CE1)

Scope

This policy applies to all Staff.

It is the policy of the Agency that all Staff be trained on their responsibilities as it relates to the use of Data and Resources. IT Security must:

a) Establish and make readily available to Staff requiring access to Resources, the rules that describe their responsibilities and expected behavior with regard to Data and Resource usage;
b) Receive a signed acknowledgement from such Staff, indicating that they have read, understand, and agree to abide by the applicable policies, before authorizing access to Data and the Resources;
c) Review the policies at least annually;
d) Require Staff who signed a previous version of the rules of behavior to read and re-sign when the applicable policies are revised/updated.

Control Enhancement

CE1. Include in the applicable policies, explicit restrictions on the use of social media/networking sites and posting Agency information on public websites. The Office of Safeguards prohibits sharing FTI using any social media/networking sites.

(PL-8) Information Security Architecture

Purpose

The purpose of the policy is to make sure security architecture is considered for all Resources that store, process or transmit Data classified as Confidential.

Applicability

Public	Confidential	FTI
	PL-8	

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential.

It is the policy of that Agency to:

a) Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
b) Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture; and
c) Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Personnel Security

(PS-1) Personnel Security Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the personnel security policy family.

Applicability

Public	Confidential	FTI
PS-1	PS-1	PS-1

Scope

This policy applies to the personnel security procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the personnel security procedures must be documented, disseminated and reviewed at least annually.

(PS-2) Position Risk Designation

Purpose

The purpose of the policy is to ensure Staff are screened according to risk levels.

Applicability

Public	Confidential	FTI
PS-2	PS-2	PS-2

Scope

This policy applies to all Staff.

It is the policy of the Agency that all positions are assigned a risk designation. Screening criteria must be established for each position risk designation and they are reviewed at least annually.

(PS-3) Personnel Screening

Purpose

The purpose of the policy is to ensure Staff are screened.

Applicability

Public	Confidential	FTI
PS-3	PS-3	PS-3

Scope

This policy applies to all Staff.

It is the policy of the Agency that all Staff are screened prior to authorizing access to Resources and rescreened if deemed necessary.

(PS-4) Termination

Purpose

The purpose of the policy is to ensure that the confidentiality and integrity of Data and Resources is maintained when Staff are terminated.

Applicability

Public	Confidential	FTI
PS-4	PS-4	PS-4

Scope

This policy applies to the IT Service Desk.

It is the policy of the Agency that upon termination of Staff that the IT Service Desk:

a) Disable Resource access;
b) Terminate/revoke any authenticators/credentials associated with the Staff;
c) Conduct exit interviews, as needed;
d) Retrieve all security-related Agency Resource–related property;
e) Retain access to Agency Data and Resources formerly controlled by the terminated Staff; and
f) Notify appropriate Staff of the termination.

(PS-5) Personnel Transfer

Purpose

The purpose of the policy is to ensure that the confidentiality and integrity of Data and Resources is maintained when Staff is transferred.

Applicability

Public	Confidential	FTI
PS-5	PS-5	PS-5

Scope

This policy applies to the IT Service Desk.

It is the policy of the Agency that upon transfer of Staff that the IT Service Desk:

a) Review and confirm ongoing operational need for current logical and physical access authorizations to Resources/facilities when Staff are reassigned or transferred to other positions within the Agency;
b) Initiate transfer or reassignment actions following the formal transfer action;
c) Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and
d) Notify designated Agency personnel, as required.

(PS-6) Access Agreements

Purpose

The purpose of the policy is to ensure that access agreements are in place prior to Staff accessing Data classified as Federal Tax Information (FTI).

Applicability

Public	Confidential	FTI
PS-6	PS-6	PS-6

Scope

This policy applies to all Staff accessing Data. Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that Staff have read, understand, and agree to abide by the constraints associated with Resources to which access is authorized. Electronic signatures for acknowledge of access agreements is permitted.

It is the policy of the Agency that prior to Staff accessing Data, IT Security must:

a) Develop and document access agreements for Agency Resources;
b) Review and update the access agreements, at least annually; and
c) Ensure that Staff requiring access to Agency Data and Resources:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to Agency Resources when access agreements have been updated or at least annually.
d) Review Resource administrator Accounts, every 3 months as required by the NC Statewide Information Security Manual - Chapter 2, section 020101.

(PS-7) Third-Party Personnel Security

Purpose

The purpose of the policy is to ensure that all Staff, including third-party personnel, has defined security requirements.

Applicability

Public	Confidential	FTI
PS-7	PS-7	PS-7

Scope

This policy applies to all third-party Staff.

It is the policy of the Agency that third-party Staff:

a) Have defined personnel security requirements, including security roles and responsibilities;
b) Comply with all security policies and procedures;
c) Notify the Agency of any personnel transfers or terminations who possess Agency credentials or badges or who have access to Resources or Data; and
d) IT Security will monitor provider compliance.

(PS-8) Personnel Sanctions

Purpose

The purpose of the policy is to ensure that the policies regarding personnel sanctions are adhered to.

Applicability

Public	Confidential	FTI
PS-8	PS-8	PS-8

Scope

This policy applies to personnel sanction policies.

It is the policy of the Agency that all policies and procedures regarding personnel sanctions are adhered to.

Risk Assessment

(RA-1) Risk Assessment Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the risk assessment policy family.

Applicability

Public	Confidential	FTI
RA-1	RA-1	RA-1

Scope

This policy applies to the risk assessment procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the risk assessment procedures must be documented, disseminated and reviewed at least annually.

(RA-2) Security Categorization

Purpose

The purpose of the policy is to ensure that Data is properly handled and unauthorized disclosure is prevented.

Applicability

Public	Confidential	FTI
RA-2	RA-2	RA-2

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information and Resources.

It is the policy of the Agency that all Data may only be disclosed to appropriate individuals and only to the extent allowed by the classification. All Data must be classified and handled accordingly. A willful, unauthorized disclosure of Data will be prosecuted under all applicable statutes. If Data is comingled then the more restrictive classification shall apply.

It is the policy of the Agency to:

a) Categorize Data and the Resource in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b) Document the security categorization results (including supporting rationale) in the security plan for the information system; and
c) Ensures that the Agency CIO reviews and approves the security categorization decision.

Staff will classify all Data as one of the following:

Federal Tax Information

Federal Taxpayer Information (FTI) is defined by Internal Revenue Service Publication 1075.

a) Federal regulations require FTI be maintained separately from other Data whenever possible. If FTI is combined or commingled with other information and can no longer be identified specifically as FTI, then the commingled information must all be treated as FTI.
b) Any Staff disclosing FTI must ensure that it is authorized under IRC, Section 6103.
c) Only approved Resources may be used to process or store FTI.
d) No FTI shall be transmitted to a non-Agency email address using non-Agency IT approved methods without prior approval of the CISO.

Confidential Information

Confidential Information is non-FTI Data that is exempted from public records requests defined by NC G.S. 132-1. Confidential Information includes, but is not limited to:

e) Information that pertains to the security of our information systems as defined in G.S. 132-6.1(c).
f) Information that pertains to the physical security of our public buildings such as detailed plans of public buildings and infrastructure facilities as defined in G.S. 132-1.7.
g) State Taxpayer Information (STI) as defined by G.S. 105-259(B).
h) Payment Card Industry (PCI) Data Security Standard data.
i) Personally Identifiable Information (PII) as defined in G.S. 75-61, G.S. 75-66, G.S. 132-1.10, G.S. 14-113.20.
j) National Automated Clearing House Association (NACHA).

Public Information

k) All electronic information that is not classified as FTI or Confidential Information is considered Public Information as defined by the North Carolina General Statute G.S. 132-1 and is subject to public records requests.
l) All public records requests must be submitted to the Public Information Officer (PIO). The PIO will coordinate the Agency response to public records requests.

(RA-3) Risk Assessment

Purpose

The purpose of the policy is to establish the procedure requirements for risk assessment.

Applicability

Public	Confidential	FTI
RA-3	RA-3	RA-3

Scope

This policy applies to all Resources.

It is the policy of the Agency that for every Resource, prior to implementation, the Chief Information Security Office (CISO) must perform an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the Resource and the Data it stores, processes or transmits.

The CISO must:

a) Document risk assessment results in a risk assessment report;
b) Review risk assessment results at least annually;
c) Disseminate risk assessment results to the Resource owner, Chief Information Officer and the Chief Technology Officer; and
d) Update the risk assessment report at least every three years or whenever there are significant changes to the Resource or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the Resource.
e) The risk assessment should take into account NIST SP 800-37 rev 1 - *Guide for Applying the Risk Management Framework to Federal Information Systems*.

(RA-5) Vulnerability Scanning

Purpose

The purpose of the policy is to ensure that Resources are protected from vulnerabilities.

Applicability

Public	Confidential	FTI
RA-5	RA-5 (CE1)(CE2)(CE5)	RA-5(CE1)

Scope

This policy applies to all Resources.

It is the policy of the Agency that all Resources are protected from vulnerabilities. IT Security must:

a) Scan for vulnerabilities in the Resource and hosted applications at a minimum of monthly for all Resources and when new vulnerabilities potentially affecting the Resources are identified and reported; and
b) Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact.
c) Analyze vulnerability scan reports and results from security control assessments;
d) Remediate legitimate vulnerabilities in accordance with an assessment of risk; and
e) Share information obtained from the vulnerability scanning process and security control assessments with designated Agency officials to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Control Enhancements

CE1. Employ vulnerability scanning tools that include the capability to readily update the Resource vulnerabilities to be scanned.
CE2. The Agency updates the Resource vulnerabilities scanned weekly.
CE5. The Resource implements privileged access authorization to IT Security Staff or to a specified system account for vulnerability scanning activities.

Resource and Service Acquisition Policy Family

(SA-1) Resource and Service Acquisition

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the system and service acquisition policy family.

Applicability

Public	Confidential	FTI
SA-1	SA-1	SA-1

Scope

This policy applies to the system and service acquisition procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the system and service acquisition procedures must be documented, disseminated and reviewed at least annually.

(SA-2) Allocation of Resources

Purpose

The purpose of the policy is to ensure that information security is planned for the life of the Resource.

Applicability

Public	Confidential	FTI
SA-2	SA-2	SA-2

Scope

This policy applies to all Resources.

It is the policy of the Agency that all Resources have sufficient funding to ensure the confidentiality and integrity of Data and Resources commensurate with their defined risk level. The Chief Information Security Officer (CISO) must:

a) Determine information security requirements for the Resource or service in mission/business process planning;

b) Determine, document, and allocate the resources required to protect the Resource or service as part of the budget planning and investment control process; and
c) Establish a discrete line item for information security in Agency programming and budgeting documentation.

(SA-3) Resource Development Lifecycle

Purpose

The purpose of the policy is to ensure that security is considered during the development and maintenance of Resources.

Applicability

Public	Confidential	FTI
SA-3	SA-3	SA-3

Scope

This policy applies to all Resources.

It is the policy of the Agency to manage Resources using a System Development Life Cycle (SDLC) that incorporates information security considerations.

a) Define and document information security roles and responsibilities throughout the SDLC;
b) Identify Staff having information security roles and responsibilities; and
c) Integrate the Agency information security risk management process into SDLC activities.

(SA-4) Acquisition Process

Purpose

The purpose of the policy is to ensure that security requirements are included in any acquisition of a Resource or service.

Applicability

Public	Confidential	FTI
SA-4 (CE10)	SA-4 (CE1)(CE2)(CE9)(CE10)	SA-4 (CE1)

Scope

This policy applies to all Resources or services being procured.

It is the policy of the Agency that the following requirements, descriptions, and criteria, explicitly or by reference, is included in the acquisition contract for the Resource, component, or service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a) Security functional requirements;
b) Security strength requirements;
c) Security assurance requirements;
d) Security-related documentation requirements;
e) Requirements for protecting security-related documentation;
f) Description of the Resource development environment and environment in which it is intended to operate; and
g) Acceptance criteria.

Control Enhancements

CE1. The Agency requires the developer of the Resource, component, or service to provide a description of the functional properties of the security controls to be employed.
CE2. The Agency requires the developer of the Resource, component, or service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces, high-level design at sufficient detail to satisfy the Service Design process and as approved by the Service Design lifecycle manager.
CE9. The agency requires the developer of the Resource, component, or service to identify early in the Service Design lifecycle, the functions, ports, protocols, and services intended for organizational use.
CE10. The Agency employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

(SA-5) Resource Documentation

Purpose

The purpose of the policy is to ensure that adequate system documentation is obtained for all Resources procured by the Agency.

Applicability

Public	Confidential	FTI
SA-5	SA-5	SA-5

Scope

This policy applies to all Resources and/or services being procured.

It is the policy of the Agency that for all Resources and/or services being procured the Agency must:

a) Obtain administrator documentation for the Resource, component, or service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security functions/mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
b) Obtain Staff (i.e. user) documentation for the Resource, component, or service that describes:
    1. Staff-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
    2. Methods for Staff interaction, which enable Staff to use the Resource, component, or service in a more secure manner; and
    3. Staff responsibilities in maintaining the security of the Resource, component, or service.
c) Document attempts to obtain Resource, component, or service documentation when such documentation is either unavailable or nonexistent;
d) Protect documentation, as required; and
e) Distribute documentation to designated Agency officials.

(SA-8) Security Engineering Principals

Purpose

The purpose of the policy is to ensure that security is properly considered in the specification, design, development, implementation, and modification of Resources.

Applicability

Public	Confidential	FTI
	SA-8	SA-8

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency to apply Resource security engineering principles in the specification, design, development, implementation, and modification of the Resource. Specifically NIST Publication 800-27 Revision A - Engineering Principles for IT Security should be considered where appropriate.

(SA-9) External Information System Services

Purpose

The purpose of the policy is to ensure that security is properly considered when outsourcing services.

Applicability

Public	Confidential	FTI
SA-9	SA-9(CE2)	SA-9(CE5)

Scope

This policy applies to all external information system services.

It is the policy of the Agency that providers of external services comply with Agency information security requirements and employ to include (at a minimum) security requirements contained within applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements. For external services that will receive, store, process or transmit Data classified as Federal Tax Information (FTI), the external provider must comply with IRS 1075 Revision October 2014.

The related contract for services must:

a) Define government oversight and user roles and responsibilities with regard to external services if the service will receive, store, process or transmit FTI;
b) Monitor security control compliance by external service providers on an ongoing basis;
c) Restrict the location of Resources that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations (SA-9 CE5); and
d) Prohibit the use of non-Agencyowned Resources that receive, process, store, or transmit FTI unless explicitly approved by the Office of Safeguards. (For notification requirements, refer to IRS 1075 Revision October 2014 - Section 7.4.5 Non-AgencyOwned Information Systems). The contract for the acquisition must contain Exhibit 7 language, as appropriate (see IRS 1075 Revision October 2014 - Exhibit 7 Safeguarding Contract Language).

(SA-10) Developer Configuration Management

Purpose

The purpose of the policy is to ensure that security is considered during the development, implementation or operation of a Resource, component, or service.

Applicability

Public	Confidential	FTI
	SA-10	SA-10

Scope

This policy applies to all Resources under development, implementation or operation that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that any developer of a Resource, component, or service must:

a) Perform configuration management during Resource, component, or service development, implementation, and operation;
b) Document, manage, and control the integrity of changes to the Resource, component, or service;
c) Implement only Agency-approved changes to the Resource, component, or service;
d) Document approved changes to the Resource, component, or service and the potential security impacts of such changes; and
e) Track security flaws and flaw resolution within the Resource, component, or service and report findings to IT Security.

(SA-11) Developer Security Testing and Evaluation

Purpose

The purpose of the policy is to ensure that all developers of Agency Resources plan for security testing and evaluation.

Applicability

Public	Confidential	FTI
	SA-11	SA-11

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency that any developer of a Resource, component, or service must:

a) Create and implement a security assessment plan;
b) Perform security testing/evaluation;
c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d) Implement a verifiable flaw remediation process; and
e) Correct flaws identified during security testing/evaluation.

(SA-22) Unsupported Resource Components

Purpose

The purpose of the policy is to ensure that the Agency has continued support for Resources, components and services.

Applicability

Public	Confidential	FTI
		SA-22

Scope

This policy applies to all Resources, components and services that may store, process or transmit Data classified as Federal Tax Information.

It is the policy of the Agency to replace Resource components when support for the components is no longer available from the developer, vendor, or manufacturer.

Resource and Communication Protection Policy Family

(SC-1) Resource and Communication Protection Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the Resource and communication protection policy family.

Applicability

Public	Confidential	FTI
SC-1	SC-1	SC-1

Scope

This policy applies to the system and communication protection procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the Resource and communication protection procedures must be documented, disseminated and reviewed at least annually.

(SC-2) Application Partitioning

Purpose

The purpose of the policy is to make sure that privileged accounts are not being used for work that can be done with a less privileged account.

Applicability

Public	Confidential	FTI
SC-2	SC-2	SC-2

Scope

This policy applies to all Resources. Resource management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged Staff access. The separation of Staff functionality from Resource management

functionality can be achieved by physical and/or logical methods. Organizations implement separation of system management-related functionality from Staff functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for Staff of any other Resource resources. Separation of system and Staff functionality may include isolating administrative interfaces on different domains and with additional access controls.

It is the policy of the Agency that all Resources must separate Staff functionality (including Staff interface services) from Resources management functionality.

(SC-4) Data in Shared Resources

Purpose

The purpose of the policy is to ensure that residual Data is protected even when objects are reused.

Applicability

Public	Confidential	FTI
	SC-4	SC-4

Scope

This policy applies to all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information. This policy prevents Data, including encrypted representations of Data, produced by the actions of prior Staff/roles (or the actions of processes acting on behalf of prior Staff/roles) from being available to any current Staff/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released. The control of Data in shared Resources is also commonly referred to as object reuse and residual Data protection. This control does not address:

(i) Information remanence which refers to residual representation of Data that has been nominally erased or removed;

(ii) Covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; and

(iii) Components within information systems for which there are only single Staff/roles.

It is the policy of the Agency that all Resources must prevent unauthorized and unintended transfer of Data via shared system resources.

(SC-5) Denial of Service Protection

Purpose

The purpose of the policy is to ensure that Resources are protected from a Denial of Service attack.

Applicability

Public	Confidential	FTI
SC-5	SC-5	SC-5

Scope

This policy applies to all Resources.

It is the policy of the Agency that the Resource must protect against or limit the effects of denial of service attacks. Refer to NIST SP 800-61 R2 - *Computer Security Incident Handling Guide*, for additional information on denial of service.

(SC-7) Network Boundary Protection

Purpose

The purpose of the policy is to ensure managed interfaces for boundary protection of Resources are employed, monitored, audited and controlled.

Applicability

Public	Confidential	FTI
SC-7	SC-7 (CE3)(CE4)(CE5)(CE7)	SC-7 (CE3)(CE4)(CE5)(CE7)

Scope

This policy applies to any Resources and connection to an external network and key internal boundaries.

It is the policy of the Agency that managed interfaces for boundary protection of Resources are employed, monitored, audited and controlled at connection points to external networks using security devices (e.g. firewalls, routers, encrypted tunnels) in accordance with Agency enterprise architecture.

The Resource must:

a) Monitor and control communications at the external boundary of the Resource and at key internal boundaries within the Resource;

b) Implement sub-networks for publicly accessible Resource components that are physically and logically separated from internal Agency networks; and
c) Connect to external networks or Resource only through managed interfaces consisting of boundary protection devices arranged in accordance with Agency security architecture requirements. Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected sub-networks).

Control Enhancements

CE3. The Agency must limit the number of external network connections to the Resource.

CE4. The Agency must:
a) Implement a secure managed interface for each external telecommunication service;
b) Establish a traffic flow policy for each managed interface;
c) Protect the confidentiality and integrity of the Data being transmitted across each interface;
d) Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need, and accept the associated risk; and
e) Review exceptions to the traffic flow policy at a minimum annually, and remove exceptions that are no longer supported by an explicit mission/business need.

CE5. The Resource at managed interfaces must deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

CE7. The Resource must, in conjunction with a remote device, prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e. bridging).

Additional requirements for protecting FTI on networks are provided in IRS Publication 1075 Revision October 2014 - Section 9.4.10 - Network Protections.

(SC-8) Transmission Confidentiality and Integrity

Purpose

The purpose of the policy is to establish the proper transmission of Data to ensure the integrity and confidentiality of the Data.

Applicability

Public	Confidential	FTI
	SC-8 (CE1)	SC-8 (CE1)

Scope

This policy applies to both internal and external networks and all types of Resources components from which Data can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

It is the policy of the Agency that the Resource protects the confidentiality and integrity of transmitted information commiserate with the Data classification (RA-2)

Control Enhancement

CE1. The Resource implements cryptographic mechanisms to prevent unauthorized disclosure of information during transmission using FIPS 140-2 compliant cryptographic mechanisms.

a) If encryption is infeasible or impractical, the CISO may approve mitigating safeguards such as implementing vLANs to segregate network traffic or the use of physical security safeguards;
b) The Agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized Agency Staff; and
c) Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic.

(SC-10) Network Disconnect

Purpose

The purpose of the policy is to ensure the integrity and confidentiality of Data by terminating connections that are not being actively used.

Applicability

Public	Confidential	FTI
	SC-10	SC-10

Scope

This policy applies to the termination of network connections that are associated with communications sessions (i.e., network disconnect) in contrast to user-initiated logical sessions in AC-12.

It is the policy of the Agency that all Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information must terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

(SC-12) Cryptographic Key Management

Purpose

The purpose of the policy is to ensure that cryptographic keys are properly managed.

Applicability

Public	Confidential	FTI
SC-12	SC-12	SC-12

Scope

This policy applies to any Resource that stores, transmits or processes Data and utilizes cryptographic keys.

It is the policy of the Agency to establish and manage cryptographic keys for required cryptography employed within the Resource. Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures.

(SC-13) Cryptographic Protection

Purpose

The purpose of the policy is to ensure that cryptographic keys are properly managed.

Applicability

Public	Confidential	FTI
SC-13	SC-13	SC-13

Scope

This policy applies to any Resource that stores, transmits or processes Data and utilizes cryptographic keys.

It is the policy of the Agency that all Resources using cryptographic modules must implement them in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

(SC-15) Collaborative Computing Resources

Purpose

The purpose of the policy is to establish the appropriate use of collaborative computing devices.

Applicability

Public	Confidential	FTI
SC-15	SC-15	SC-15

Scope

This policy applies to all collaborative computing devices such as networked white boards, cameras, and microphones.

It is the policy of the Agency that the Resource must prohibit remote activation of collaborative computing devices and the Resource must provide an explicit indication of its use to Staff physically present at the devices.

(SC-17) Public Key Infrastructure Certificates

Purpose

The purpose of the policy is to ensure that certificates are supplied by a reputable source.

Applicability

Public	Confidential	FTI
	SC-17	SC-17

Scope

This policy applies to all public key infrastructure certificates.

It is the policy of the Agency to issue public key infrastructure certificates or obtain public key infrastructure certificates from an approved service provider.

(SC-18) Mobile Code

Purpose

The purpose of the policy is to define the use of mobile code technologies.

Applicability

Public	Confidential	FTI
	SC-18	SC-18

Scope

This policy applies to mobile code on Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information. Mobile code includes Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.

It is the policy of the Agency that the use of mobile code technology is permitted with the exception of some internet client usage. Mobile code technologies that exhibit functionality allowing unmediated access to host and remote system services, Resources and Data will be blocked or disabled via web proxy with content filtering for Internet browsing sessions.

(SC-19) Voice over Internet Protocol

Purpose

The purpose of the policy is to make sure that Data integrity and confidentiality is maintained when transmitting voice over the network.

Applicability

Public	Confidential	FTI
	SC-19	SC-19

Scope

This policy applies to all implementations of VoIP that may store, process or transmit Data classified as Confidential or as Federal Tax Information.

It is the policy of the Agency to establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and authorizes, monitors, and controls the use of VoIP within the Resource.

In order to use a VoIP network that provides information classified as Federal Tax Information (FTI) to a customer, the following requirements must be met:

a) VoIP traffic that contains FTI should be segmented off from non-VoIP traffic through segmentation. If complete segmentation is not feasible, the Agency must have compensating controls in place and properly applied that restrict access to VoIP traffic that contains FTI;
b) When FTI is in transit across the network (either Internet or Agency's network), the VoIP traffic must be encrypted using a cryptographic module that is FIPS 140-2 compliant;
c) Each Resource within the Agency's network that transmits FTI to an external customer through the VoIP network should be subject to frequent vulnerability testing;
d) VoIP-ready firewalls must be used to filter VoIP traffic on the network;
e) Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter;
f) VoIP phones must be logically protected, and agencies must be able to track and audit all FTI-applicable conversations and access; and
g) VoIP network Resources (e.g. servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security (see See IRS Publication 1075 IRC 6103(p)(4)(B) Section 4.2 – Minimum Protection Standards).

(SC-23) Session Authenticity

Purpose

The purpose of the policy is to ensure that communications sessions are valid.

Applicability

Public	Confidential	FTI
	SC-23	SC-23

Scope

This policy addresses communications protection at the session level versus the packet level (e.g., sessions in service-oriented architectures providing Web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

It is the policy of the Agency that Resources that may store, process or transmit Data classified as Confidential or as Federal Tax Information must protect the authenticity of communications sessions.

(SC-28) Data at Rest

Purpose

The purpose of the policy is to ensure that Data classified as Confidential or Federal Tax Information (FTI) is properly handled so that the confidentiality and integrity is maintained and unauthorized disclosure is prevented. Data at rest could be located on storage devices as specific components of Resources.

Applicability

Public	Confidential	FTI
	SC-28	SC-28

Scope

This policy applies to all Data classified as Confidential or as Federal Tax Information at rest. At rest refers to the state of Data when it is located on storage devices as specific components of Resources.

It is the policy of the Agency that all Resources must protect the confidentiality and integrity of Data classified as Confidential or as Federal Tax Information at rest.

a) The Agency may employ different mechanisms to achieve confidentiality and integrity protections, including encryption using a cryptographic module that is FIPS 140-2 compliant, file share scanning, and integrity protection. The Agency may also employ other security controls, including for example, secure offline storage in lieu of online storage, when adequate protection of Data at rest cannot otherwise be achieved or when continuously monitoring to identify malicious code at rest;
b) The confidentiality and integrity of Data at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms that are FIPS 140-2 compliant;
c) Data stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology; and
d) Mobile devices do require encryption at rest (see AC-19).

Resource and Data Integrity

(SI-1) Resource and Data Integrity Procedures

Purpose

The purpose of the policy is to establish the procedure requirements for the effective implementation of the Resource and Data integrity policy family.

Applicability

Public	Confidential	FTI
SI-1	SI-1	SI-1

Scope

This policy applies to the Resource and Data integrity protection procedures.

It is the policy of the Agency that procedures to facilitate the implementation of the Resource and Data integrity procedures must be documented, disseminated and reviewed at least annually.

(SI-2) Flaw Remediation

Purpose

The purpose of the policy is to ensure that Resources are patched to ensure the confidentiality and integrity of Data.

Applicability

Public	Confidential	FTI
SI-2	SI-2 (CE2)	SI-2 (CE1)

Scope

This policy applies to all Resources. Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

It is the policy of the Agency that for all Resources that IT Security:

a) Identify, report, and correct Resource flaws;
b) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c) Install security-relevant software and firmware updates based on severity and associated risk to the confidentiality of Data; and
d) Incorporate flaw remediation into the Agency configuration management process.

Control Enhancement

CE1. Centrally manage the flaw remediation process.

(SI-3) Malicious Code Protection

Purpose

The purpose of the policy is to ensure Resources are protected against malicious code.

Applicability

Public	Confidential	FTI
SI-3	SI-3 (CE1) (CE2)	SI-3 (CE1) (CE2)

Scope

This policy applies to the malicious code protection including antivirus software, antimalware and intrusion detection systems. Resource entry and exit points include, for example, firewalls, electronic mail servers, Web servers, proxy servers, remote access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files or hidden in files using steganography. Malicious code can be transported by

different means, including, for example, Web accesses, electronic mail, electronic mail attachments, and portable storage devices.

It is the policy of the Agency that malicious code protection mechanisms are employed at Resource entry and exit points to detect and eradicate malicious code.

a) Malicious code protection mechanisms must be updated whenever new releases are available in accordance with Agency configuration management policy and procedures; and
b) Malicious code protection mechanisms must be configured to:
    1. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with Agency security policy; and
    2. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection.
c) False positives must be addressed during malicious code detection and eradication and the resulting potential impact on the availability of the Resource.

Control Enhancements

CE1. Malicious code protection mechanisms must be centrally managed by IT Security.

CE2. The Resource must automatically update malicious code protection mechanisms.

(SI-4) Resource Monitoring

Purpose

The purpose of the policy is to ensure that Resources are constantly monitored for malicious activity.

Applicability

Public	Confidential	FTI
SI-4	SI-4 (CE2)(CE4)(CE5)	SI-4 (CE4)(CE5)(CE7) (CE11)(CE23)

Scope

This policy applies to all Resources. Resource monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the Resource boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the Resource.

Resource monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software).

Strategic locations for monitoring devices include, for example, selected perimeter locations and nearby server farms supporting critical applications, with such devices typically being employed at the managed interfaces.

It is the policy of the Agency to monitor all Resources.

IT Security will:

a) Monitor all Resources to detect:
    1. Attacks and indicators of potential attacks; and
    2. Unauthorized local, network, and remote connections.
b) Identify unauthorized use of Resources; and
c) Deploy monitoring devices:
    1. Strategically within the Resources to collect essential information; and
    2. At ad hoc locations within the Resource to track specific types of transactions of interest to the Agency.
d) Protect Data obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e) Heighten the level of Resource monitoring activity whenever there is an indication of increased risk to Agency operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information;
f) Provide Resource monitoring information to the CISO as needed; and
g) Analyze outbound communications traffic at the external boundary of the Resource and selected interior points within the network (e.g., sub-networks, subsystems) to discover anomalies—anomalies within Agency Resources include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

Control Enhancements

CE2. The Agency employs automated tools to support near real-time analysis of events.

CE4. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. *This is also a requirement for PCI data in PCI DSS 3.0 section 10.6.1, which calls for at least daily IDS/IPS monitoring of security events and system logs.*

CE5. Alert designated Agency Staff when indications of compromise or potential compromise occur—alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms intrusion detection or prevention mechanisms; or boundary protection Resources, such as firewalls, gateways, and routers and alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Agency Staff on the notification list can include, for example, system administrators, mission/business owners, system owners, or Resource security officers.

CE7. Notify designated Agency officials of detected suspicious events and take necessary actions to address suspicious events.

CE11. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications.

CE23. Implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on Resources.

(SI-5) Security Alerts, Advisories and Directives

Purpose

The purpose of the policy is to ensure that the Agency is receiving security alerts.

Applicability

Public	Confidential	FTI
SI-5	SI-5	SI-5

Scope

This policy applies to IT Security.

It is the policy of the Agency that IT Security:

a) Receive security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b) Generate internal security alerts, advisories, and directives as deemed necessary;
c) Disseminate security alerts, advisories, and directives to designated Agency officials; and
d) Implement security directives in accordance with established time frames or notify the issuing Agency of the degree of noncompliance.

(SI-7) Software, Firmware and Information Integrity

Purpose

The purpose of the policy is to prevent unauthorized changes to software, firmware, and Data due to errors or malicious activity. Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Data includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications

Applicability

Public	Confidential	FTI
	SI-7 (CE1)(CE7)	

Scope

This policy applies to all Resources that store, process or transmit Data classified as Confidential.

It is the policy of the Agency to employs integrity verification tools to detect unauthorized changes to software, firmware and Data.

Control Enhancements

CE1. The Resource performs an integrity check of software, firmware and Data at startup.

CE7. The Agency incorporates the detection of unauthorized changes to the Resource into the organizational incident response capability.

(SI-8) Spam Protection

Purpose

The purpose of the policy is to prevent spam.

Applicability

Public	Confidential	FTI
	SI-8 (CE1)(CE2)	SI-8

Scope

This policy applies to IT Security.

It is the policy of the Agency that IT Security employ spam protection mechanisms at Resource entry and exit points to detect and take action on unsolicited messages. In addition, they should update spam protection mechanisms when new releases are available in accordance with Agency configuration management policy and procedures.

(SI-10) Data Input Validation

Purpose

The purpose of the policy is to ensure that all Resources have some form of quality control around Data inputs and to prevent unauthorized or inappropriate input.

Applicability

Public	Confidential	FTI
	SI-10	SI-10

Scope

This policy applies to all Resources.

It is the policy of the Agency that all Resources must check the validity of Data inputs.

(SI-11) Error Handling

Purpose

The purpose of the policy is to make sure that all Resources can generate error notices.

Applicability

Public	Confidential	FTI
	SI-11	SI-11

Scope

This policy applies to all Resources.

It is the policy of the Agency that all Resources must:

a) Generate error messages that provide Data necessary for corrective actions without revealing Data that could be exploited by adversaries; and
b) Reveal error messages only to designated Agency officials.

(SI-12) Data Handling and Retention

Purpose

The purpose of the policy is to ensure that Staff properly handles Data.

Applicability

Public	Confidential	FTI
SI-12	SI-12	SI-12

Scope

This policy applies to all Staff.

It is the policy of the Agency that Staff must handle and retain Data within the Resource and Data output from the Resource in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

(SI-16) Memory Protection

Purpose

The purpose of the policy is to ensure that all Resources protect their memory.

Applicability

Public	Confidential	FTI
	SI-16	SI-16

Scope

This policy applies to all Resources. Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

It is the policy of the Agency that all Resources must implement safeguards to protect its memory from unauthorized code execution.

Program Management

(PM-2) Senior Information Security Officer

Purpose

The purpose of the policy is to establish the Chief Information Security Officer.

Applicability

Public	Confidential	FTI
		PM-2

Scope

This policy applies to the Agency. The security officer described in this policy is an Agency official. This official is the Chief Information Security Officer.

It is the policy of the Agency that the Agency appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an Agency-wide information security program.