S FOR POLICY

223.01 Information Security (INFOSEC)

Table of Contents

Introduction

The Alabama Community College System (ACCS) and its member colleges provide quality educational services to the citizens of Alabama in a cost-effective manner. ACCS views the entire Alabama population as a potential student that can enrich their lives through the advancements available to them thanks to ACCS. The assessment and mitigation of risks that threaten the ACCS way of life is a key asset in reducing costs and passing those savings to the students. Proper risk

that will consume, retain, distribute, and report security and privacy documentation to aid ACCS in clearly understanding the risk provided to its mission by its information resources.

PM-1: Program Management Policy & Procedures

ACCS:

a. Develops and disseminates an organization-wide information security program plan that:
    1. Provides an overview of the requirements for the Security Program and a description of the Security Program management controls and Common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    3. Reflects the coordination among organizational entities responsible for information security; and
    4. Is approved by a senior official with the responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the State.
b. Reviews the organization-

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-5: System Inventory

ACCS develops and maintains an inventory of organizational systems.

PM-6: Measures of Performance

ACCS develops, monitors, and reports on the results of information security and privacy measures of performance.

PM-7: Enterprise Architecture

ACCS develops an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations, assets, individuals, other organizations, and the State.

PM-8: Critical Infrastructure Plan

ACCS addresses information security and privacy issues in the development, documentation, and updating of critical infrastructure and key resources protection plan.

PM-9: Risk Management Strategy

ACCS:

a. Develops a comprehensive strategy to manage:
    1. Security risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of organizational systems;
    2. Privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information; and
    3. Supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the Risk Management Strategy annually or as required, to address organizational changes.

PM-10: Authorization Process

ACCS:

a. Manages the security and privacy state of organizational systems and the environments in which those systems operate through the authorization process;
b. Designates individuals to fulfill specific roles and responsibilities within the organization risk management process; and
c. Integrates the authorization process into an organization-wide risk management program.

PM-11: Mission & Business Process Definition

ACCS:

PM-18: Privacy Program Plan

ACCS:

a. Develops and disseminates an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:
    1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
    2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
    3. Includes the role of the Senior Agency Official for Privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
    4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
    5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
    6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the State; and
b. Updates the plan to address changes in privacy laws & policy, organizational changes, and problems identified during plan implementation or privacy control assessments.

PM-19: Privacy Program Roles

ACCS appoints a Senior ACCS Official for Privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

PM-20: Systems of Records Notice

ACCS:

a. Publishes System of Records notices in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information.
b. Keeps System of Records Notices current.

PM-21: Dissemination of Privacy Program Information

ACCS:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its Senior Agency Official for Privacy;
b. Ensure that organizational privacy practices are publicly available through organizational websites or otherwise; and
c. Employ publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

PM-22: Accounting of Disclosures

ACCS:

a. Develops and maintains an accounting of disclosures of personally identifiable information held in each system of records under its control, including:
    1. Date, nature, and purpose of each disclosure of a record; and

2. Name and address of the person or organization to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon request.

PM-23: Data Quality Management

ACCS issues guidelines ensuring and maximizing the quality, utility, objectivity, integrity, impact determination, and de-identification of personally identifiable information across the information life cycle.

PM-24: Data Management Board

ACCS:

a. Will establish a written charter for a Data Management Board;
b. Will establish the Data Management Board consisting of organization-defined roles with the following responsibilities:
    1. Develop and implement guidelines supporting data modeling, quality, integrity, and de-identification needs of personally identifiable information across the information life cycle;
    2. Review and approve applications to release data outside of the organization, archim on

a. Mechanisms that are easy to use and readily accessible by the public;
b. All information necessary for successfully filing complaints; and
c. Tracking mechanisms to ensure all complaints received are reviewed and appropriately addressed in a timely manner.

PM

Access Control

POLICY 223.01 INFOSEC Minimum Protection Requirement for AC

ACCS will limit information system access to authorized users, processes acting on behalf of authorized users, or devices

When accounts are no longer required;
When users are terminated or transferred; and
When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:
   A valid access authorization;
   Intended system usage; and
   Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements
   For Moderate systems at least every 90 days
   For Low systems at least every 365 days; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
l. Aligns account management processes with personnel termination and transfer processes.

AC

a. The receiving system, system component, or entity provides the req

b. Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
    a. Display system use information when appropriate, before granting further access;
    b. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    c. Include a description of the authorized uses of the system.

Before granting access to an ACCS system that receives, processes, stores, transmits, or disposes of Federal Tax Information, the system (and each applicable system component – i.e. application, database, operating system, and network devices) displays to users an IRS-approved warning banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. The system contains U.S. Government information
2. Users actions are monitored and audited
3. Unauthorized use of the system is prohibited
4. Unauthorized use of the system is subject to criminal and civil sanctions

Further, the system (and applicable system components) must Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

The agency does not make Federal Tax Information publicly available through its systems.

AC-11: Device Lock

ACCS Systems:

a. Prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and
b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

AC-12: Session Termination

ACCS systems automatically terminate a user session after 30 minutes of inactivity.

AC-14: Permitted Actions Without Identification or Authentication

ACCS:

a. Identifies specific user actions that can be performed on the information system without identification or authentication;
b. Documents and provides supporting rationale in the system security plan for the information system, user actions not requiring identification or authentication; and
c. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Federal Tax Information may not be disclosed to individuals on the information system without identification and authentication.

AC-17: Remote Access

ACCS:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

ACCS systems protect wireless access to the system using encryption, and authentication of both users and devices.

ACCS systems disable, when not intended for use, wireless networking capabilities internally embedded within system components prior to issuance and deployment.

ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information must employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Detailed mandatory requirements for using FTI on an 802.11 wireless LAN can be found in section 9.4.18 of IRS Publication 1075.

AC-19: Access Control for Mobile Devices

ACCS:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices;
b. CIO or his/her designee authorizes the connection of mobile devices to organizational information systems; and
c. Protects and control mobile devices when outside of controlled areas.

ACCS employs (FIPS 140-2 validated module) full-device encryption or container encryption to protect the confidentiality and integrity of information on approved mobile devices.

ACCS systems that use mobile devices (as defined by the Security Program - Glossary – excluding Laptops) to receive, process, store, transmit, or dispose of Federal Tax Information must purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Detailed mandatory requirements for using FTI on mobile devices can be found in section 9.4.8 of IRS Publication 1075.

AC-20: Use of External Systems

ACCS

f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

ACCS permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when ACCS:

a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

ACCS restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.

With respect to receiving, processing, storing, transmitting, or disposing of Federal Tax Information, the agency does not permit:

a. Access to FTI from external information systems, other than through a virtual desktop infrastructure;
b. The use of ACCS-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems;
c. The use of non-ACCS-owned information systems; system components; or devices to process, store, or transmit FTI; any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation.

AC-21: Information Sharing

ACCS:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and
b. Employs automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

ACCS restricts the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the IRS Office of Safeguards.

AC-22: Publicly Accessible Content

ACCS:

a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency:

a. Trains authorized individuals to ensure that publicly accessible information does not contain FTI;
b. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included; and
c. Reviews the content on the publicly accessible information system for FTI, at a minimum, quarterly and removes such information, if discovered.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, Section 6.3 Disclosure Awareness Training in IRS Publication 1075 is required in order for author

AU-6: Audit, Review, Analysis, & Reporting

ACCS:

a.

NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi)
State or Agency designated internal NTP time servers; and

b. Synchronizes the internal clocks to the authoritative time source when the time difference is greater than one hundred (100) milliseconds

AU-9: Protection of Audit Information

ACCS systems protect audit information and audit tools from unauthorized access, modification, and deletion.

The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system. System and network administrators must not have the ability to modify or delete audit log entries.

AU-11: Audit Generation

ACCS Systems:

a. Provide audit record generation capability for the following auditable events defined in AU-2: Audit Events:
    a. All successful and unsuccessful authorization attempts;
    b. All changes to logical access control authorities (e.g., rights, permissions);
    c. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
    d. The audit trail, which must capture the enabling or disabling of audit report generation services; and
    e. The audit trail must capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).
b. Allows Security Operations Center personnel, Systems Administrator personnel, or other applicable personnel or roles to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the list of events defined in AU-2: Audit Events with the content defined in AU-3: Content of Audit Records.

AU-16: Cross-ACCS Auditing

ACCS employs mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, this requirement applies to outsourced data centers or cloud providers. The provider must be held accountable to protect and share audit information with the agency through the contract.

Assessment and Authorization

d. Produces an assessment report that documents the results of the assessment; and
e. Provides the results of the security and privacy control assessment within sixty (60) days after its completion to the Authorizing Official, Chief Information Officer, Chief Information Security Officer, Program Manager responsible for the system, and the Information Security Office Governance, Risk, & Compliance Management team.

ACCS employs assessors or assessment teams with agency CISO level of independence to conduct security control assessments.

CA-3: System Interconnections

ACCS:

a. Authorizes connections from the information system to other information systems using Interconnection Security Agreements (ISA) or other comparable agreements (such as MOU/MOA, SLA, or specific contractual clause, so long as the appropriate interconnection detail is provided therein);
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated;
c. Reviews and updates the interconnection agreements no less often that once every year and/or whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement as a verification of enforcement of security requirements; and
d. Only activates a system interconnection (including testing) when a signed interconnection agreement is in place.

ACCS employs a deny-all, permit-by-exception, policy for allowing agency information systems to connect to external information systems, except for client workstations connecting to internet resources – which employs a permit-all, deny-by-exception policy.

CA-5: Plan of Action & Milestones

ACCS:

a. Develops a plan of action and milestones for the system to document the planned remedial actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones monthly based on the findings from control assessments, impact analyses, and continuous monitoring activities.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, the POA&M must be comprised of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI.

CA-6: Authorization

ACCS:

a. Assigns a senior-level executive or manager as the authorizing official for the system and for any common controls inherited by the system;
b. Ensure that the authorizing official, before commencing operations:
    1. Authorizes the system for processing; and
    2. Authorizes the common controls inherited by the system; and
c. Updates the security authorization:

    Within every three (3) years;

    When significant changes are made to the system;

    When changes in requirements result in the need to process data of a higher sensitivity;

    When changes occur to authorizing legislation or federal requirements that impact the system;

    After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and

    Prior to expiration of a previous security authorization.

CA-7: Continuous Monitoring

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of the following metrics monitored based on the organization security goals and objectives:

    Compliance Percentage

    PoA&M items open & PoA&M items closed

    Security Incidents opened & closed

    Threats observed/stopped

    Vulnerability metrics
b. Establishment of the following frequencies, to correlate with Configuration Management practices & accommodate the assessments (defined in CA-2: Assessments), for monitoring and ongoing assessment of security and privacy control effectiveness:

    Review one-half (1/2) of minimum baseline controls annually;

    Review all controls every two years;

    Review potentially affected controls as part of the Configuration Management processes;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of the metrics define in CA-7a in accordance with the organizational continuous monitoring strategy;
e.

Configuration Management

POLICY 223.01 INFOSEC Minimum Protection Requirement for CM

ACCS will: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

CM-1: Configuration Management Policy & Procedures

ACCS:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A Configuration Management Policy that:
        a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designates the Chief Information Security Officer to manage the configuration management policy and procedures;
c. Reviews and updates the current configuration management:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the configuration management procedures implement the configuration management policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the configuration management policy.

CM-2: Baseline Configuration

ACCS develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

ACCS reviews and updates the baseline configuration of the information system:

a. At least annually;
b. When configuration settings change due to critical security patches, upgrades, and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades;
c. As an integral part of:
    1. information system component installations;
    2. upgrades; and
    3. updates to applicable governing standards; and
d. Supporting baseline configuration documentation to reflect ongoing implementation of operational baseline configuration updates, either directly or by policy.

ACCS employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

d. Receives automated updates from a trusted source.

CM-8: System Component Inventory

ACCS:

a. Develops and documents an inventory of information system components that:
    1. Accurately reflects the current information system;
    2. Include all components within the authorization boundary of the information system;
    3. Are at the level of granularity deemed necessary for tracking and reporting; and
    4. Includes:
        Each component's unique identifier and/or serial number;
        Information system of which the component is a part;
        Type of information system component (e.g., server, desktop, application);
        Manufacturer/model information;
        Operating system type and version/service pack level;
        Presence of virtual machines;
        Application software version/license information;
        Physical location (e.g., building/room number);
        Logical location (e.g., IP address, position with the information system [IS] architecture);
        Media access control (MAC) address;
        Ownership;
        Operational status;
        Primary and secondary administrators; and
        Primary user.
b. Reviews and updates the information system component inventory annually.

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

ACCS:

a. Employs automated mechanisms no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
b. Takes the following actions when unauthorized components and/or provisioned configurations are detected:
    1. Isolate the identified component;
    2. Notify the Security Operations Center;
    3. Notify Systems Administrators; and
    4. Notify the responsible actor(s) – the individual and/or the individual's supervisor

CM-9: Configuration Management Plan

ACCS develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b.

ACCS systems use automated tools to identify moderate or high categorized information and the specific system components on which the information resides to ensure adequate security and privacy controls are in place to protect organizational information and individual privacy.

Contingency Planning

POLICY 223.01 INFOSEC

ACCS coordinates contingency plan development with organizational elements responsible for related plans.

ACCS plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

ACCS identifies critical system assets supporting essential missions & business functions.

CP-3: Contingency Training

ACCS provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities:

a. Within ninety (90) days of assuming a contingency role or responsibility;
b. When

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

CP-7: Alternate Processing Site

ACCS Systems:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of critical system operations for essential missions/business functions within the Maximum Tolerable Downtime (MTD) as specified by the system contingency plan or COOP for the business function(s) supported by the system when the primary processing capabilities are unavailable;
b. Ensures 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 Maximum Tolerable Downtime (MTD) for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

ACCS identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

ACCS identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives) for system operations in support of critical business functions; and
b. When applicable, request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the prim

Identification and Authentication

POLICY 223.01 INFOSEC Minimum Protection Requirement for IA

ACCS will identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

IA-3: Device Identification & Authentication

ACCS systems uniquely identify and authenticate specific or types of devices, as specified in the applicable System Security Plan, before establishing local, remote, or network connections.

IA-4: Identifier Management

ACCS manages information system identifiers by:

a. Receiving authorization from Agency Systems Administrators to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;

a) Enforces minimum password complexity of at least one character from each of the four character categories (A-Z, a-z, 0-9, special characters) with a length of 8 characters for non-privileged accounts and 15 characters for privileged accounts;
b) Enforces at least a minimum of six (6) characters change when new passwords are created;
c) Stores and transmits only cryptographically-protected passwords;
d)

IA-8: Identification and Authentication (Non-Organizational Users)

ACCS systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to agency systems and networks.

Incident Response

POLICY 223.01 INFOSEC Minimum Protection Requirement for IR

ACCS will: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

IR-1: Incident Response Policy & Procedures

ACCS:

1. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    a. An Incident Response Policy that:
        i.

IR-4: Incident Handling

ACCS:

a. Implements an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities;
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly; and
d. Ensures the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

ACCS employs automated mechanisms to support the incident handling process.

IR-5: Incident Monitoring

The organization tracks and documents all physical, information security, and privacy incidents.

IR-6: Incident Reporting

ACCS:

a. Requires personnel to report actual or suspected security and privacy incidents to the agency helpdesk or Security Operations Center and the Privacy Office immediately upon discovering a suspected security incident; and
b. Reports security incident information to authorities defined in the Incident Response plan.

b.

ACCS prohibits the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Physical and Environmental

POLICY 223.01 INFOSEC Minimum Protection Requirement for PE

ACCS will: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

PE-1: Physical & Environmental Protection Policy & Procedures

ACCS:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A Physical & Environmental Protection Policy that:
        a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Verifying individual access authorizations before granting access to the facility; and

Controlling ingress and egress to the facility using physical access control systems/devices and/or guards;

b. Maintains physical access audit logs for all public entry and exit points;
c. Provides physical access control systems/devices and guards to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity while inside areas not officially designated as publicly accessible;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices, such as keys, badges/cards, card readers, and locks biennially;
g. Changes:

Combinations – annually, when compromised, or when individuals using the combination are transferred or terminated

Keys - when keys are lost or compromised/improperly duplicated

PE-4: Access Control for Transmission

ACCS controls physical access to telephone closets and information system distribution and transmission lines within organizational facilities using physical/key locks, cameras, and/or locking equipment racks.

PE-5: Access Control for Output Devices

ACCS controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

PE-6: Monitoring Physical Access

ACCS:

a. Monitorsiphreyeay2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2ey2e4.000(, c)-7 Tm(ividu)5(als u)3(sin)5(g)4(t)

a. Provides the capability of shutting off power within data centers to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

PE-11: Emergency Power

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to a long-term alternate power source in the event of a primary power source loss.

PE-12: Emergency Lighting

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.

PE-13: Fire Protection

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

PE-14: Temperature and Humidity Controls

ACCS:

a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-specified levels;
b. Monitors temperature and humidity level regularly; and
c. Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.

PE-15: Water Damage Protection

ACCS protects the information system 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

ACCS authorizes, monitors, and controls the flow of all information system-related components entering and exiting the facility and maintains records of those items.

PE-17: Alternate Work Site

ACCS:

a.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet the requirements listed in Section 4.7 Telework Locations for off-site locations such as other government facilities or private residences of employees.

PE-18: Location of Information System Components (Additional IRS 1075 Requirements)

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Planning

POLICY 223.01 INFOSEC Minimum Protection Requirement for PL

ACCS will develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

PL-1: Planning Policy & Procedures

ACCS:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A Security Planning Policy that:
        a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the Security Planning policy and the associated Planning controls;
b. Designates the Chief Information Security Officer to manage the Security Planning policy and procedures;
c. Reviews and updates the current Security Planning:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Security Planning procedures implement the Security Planning policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Security Planning policy.

PL-2: System Security Plan

ACCS:

a. Develops security and privacy plans for agency systems that:
    1. Are consistent with the organization's Enterprise Architecture;
    2. Explicitly define the authorization boundary for the system;
    3.

PL-4: Rules of Behavior

ACCS:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior regarding information and information system usage;
b. Receives an acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior annually; and
d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated and at least annually;

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

ACCS prohibits, and makes explicit this

a.

Personal Security

POLICY 223.01 INFOSEC Minimum Protection Requirement for PS

PS-8: Personnel Sanctions

ACCS:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies the individual's chain of command, Human Resources, Helpdesk, the Information Security Office, and other applicable personnel and roles within seven calendar days when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

e. Disseminates risk assessment results to the Authorizing Official, Program Managers (as related to the scope of the risk assessment), the Chief Information Security officer, the Chief Information Officer, and other affected stakeholders as necessary;
f. Updates the risk assessment every two years or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-5: Vulnerability Scanning

ACCS:

a. Scans for vulnerabilities in its systems and hosted applications at least monthly, randomly, or when new vulnerabilities potentially affecting systems are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures;
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from control assessments'
d. Remediates legitimate vulnerabilities within 30 days for high or critical vulnerabilities, 60 days for moderate vulnerabilities, and 180 days for low vulnerabilities in accordance with an organizational assessment of risk;
e. Shares information obtained from the vulnerability scanning process and control assessments with Authorizing Officials, Information Owners, System Owners, the Chief Information Officer, and the Chief Information Security Officer to help eliminate similar vulnerabilities in other systems; and
f. Employs vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.

ACCS updates the system vulnerabilities to be scanned daily and when new vulnerabilities are identified or reported.

ACCS implements privileged access authorization to operating

System and Services Acquisitions

POLICY 223.01 INFOSEC Minimum Protection Requirement for SA

ACCS will: (i) allocate

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

ACCS:

a.

b. Obtains user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
    3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexis

a. Perform configuration management during system, component, or service development, implementation, and operation;
b.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, without exception, ACCS must replace information system components (specifically security patches and/or product updates) when support for the components is no longer available from the developer, vendor, or manufacturer.

System and Communications Protection

POLICY 223.01 INFOSEC Minimum Protection Requirement for SC

ACCS will: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response

SC-1: System and Communications Protection Policy & Procedures

ACCS:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A System and Communications Protection Policy that:
        a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; a

1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
2. Forcibly disconnects:
    i. inactive remote client-based connections (including VPN connections) after thirty (30) minutes or less of inactivity,
    ii. inactive communications sessions (including stateful firewall sessions) after 60 minutes, and

b. Terminate or suspend network connections (i.e., a system to system interconnection) upon issuance of an order by the ACCS Chancellor, Authorizing Official, CIO, CISO, or Privacy Officer.

SC-12: Cryptographic Key Establishment and Management

ACCS systems establish and manage cryptographic keys for required cryptography employed within the information system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

SC-13: Cryptographic Protection

ACCS systems implement, for sensitive information, FIPS-validated cryptography or other laws, Executive Orders, directives, policies, regulations, and standards as applicable.

SC-15: Collaborative Computing Devices and Applications

ACCS:

a. Prohibits remote activation of collaborative computing devices except where explicitly permitted by the Authorizing Official or CIO; and
b. Provides an explicit indication of use to users physically present at the devices.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, or when Federal Tax Information is discussed over Collaborative Computing Devices and Applications, the agency:

Prohibits remote activation of collaborative computing devices; and

Provides an explicit indication of use to users physically present at the devices.

SC-17: Public Key Infrastructures

ACCS issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.

SC-18: Mobile Code

ACCS:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

SC-19: Voice Over Internet Protocol

ACCS:

a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously;
b. Authorizes, monitors, and controls the use of VoIP within the information system; and

c. Ensures VoIP equipment used to transmit or discuss sensitive information is protected with agency encryption requirements.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, or when Federal Tax Information is discussed over a Voice over IP telephone system, ACCS meets the requirements listed in Section 9.4.15 VoIP Systems of IRS Publication 1075.

SC-20: Secure Name / Address Resolution Service (Authoritative Source)

ACCS Systems:

a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-21: Secure Name / Address Resolution Service (Recursive or Caching Resolver)

ACCS systems requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22: Architecture and Provisioning for Name / Address Resolution Service

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

SC-23: Session Authenticity

ACCS systems protect the authenticity of communications sessions.

SC-28: Protection of Information at Rest

ACCS systems protect the confidentiality and integrity of sensitive information at rest regardless of storage media.

ACCS systems implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information when at rest on system components.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Information, the confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms. Federal Tax Information stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.

ACCS does not store Federal Tax Information on Mobile Devices.

SC-39: Process Isolation

The information system maintains a separate execution domain for each executing process.

b. iModerate/Medium – 180 calendar days
c. Low – 365 calendar days

d. Incorporates flaw remediation into the organizational configuration management process.

ACCS centrally manages the flaw remediation process.

ACCS employs automated mechanisms weekly to determine the state of system components with regard to flaw remediation.

SI-3: Malicious Code Protection

ACCS:

a. Implements signature based and non-signature based malicious code protection mechanisms at endpoint and system entry/exit points to detect and eradicate malicious code;
b. Automatically updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
    1.

f. Obtain legal opinion regarding system monitoring activities; and
g. Provide pertinent system monitoring information to system administrators, security operations center personnel, system owners, information owners and other personnel or roles as needed.

ACCS employs automated tools and mechanisms to support near real-time analysis of events.

ACCS monitors inbound and outbound communications traffic daily during business hours for unusual or unauthorized activities or conditions.

ACCS systems alert the Security Operations Center, system administrators, and other roles and personnel as needed when system-generated indications of compromise or potential compromise occur.

ACCS systems notify the Security Operations Center, CISO, system administrators, and other applicable personnel of detected suspicious events and take necessary actions to address suspicious events.

With respect to ACCS systems that receive, process, store, transmit, or dispose of Federal Tax Inf0.588 rg1q(f0.588 rg1q(f0.588 rg

ACCS centrally manages spam protection mechanisms.

ACCS automatically updates spam protection mechanisms.

SI-10: Information Input Validation

ACCS systems check the validity of all information inputs.

SI-11: Error Handling

ACCS:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
b. Reveal error messages only to development personnel, system administrators, system owners, and other agency personnel as necessary.

SI-12: Information Handling and Retention

ACCS handles and retains information within the information system and information output from the system in accordance with appl