CJIS Sample Policy Table of Contents

Policy #:	Title:	Effective Date:
x.xxx	Access Control Policy (Sample)	MM/DD/YY

PURPOSE

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;
NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of [entity] resources and assets.

1. ACCOUNT MANAGEMENT
   IT Department shall:

   a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

   b. Assign account managers for information system accounts.

   c. Establish conditions for group and role membership.

   d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

   e. Require approvals by system owners for requests to create information system accounts.

   f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

   g. Monitor the use of information system accounts.

h. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

i. Authorize access to the information system based on a valid access authorization or intended system usage.

j. Review accounts for compliance with account management requirements [entity defined frequency].

k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

l. Employ automated mechanisms to support the management of information system accounts.

m. Ensure that the information system automatically disables temporary and emergency accounts after usage.

n. Ensure that the information system automatically disables inactive accounts after [entity defined frequency]

o. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

2. ACCESS ENFORCEMENT
IT Department shall:

a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3. INFORMATION FLOW ENFORCEMENT
IT Department shall:

a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

4. SEPARATION OF DUTIES
IT Department shall:
a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

b. Document the separation of duties of individuals.

c. Define information system access authorizations to support separation of duties.

5. LEAST PRIVILEGE
   IT Department shall:

   a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

   b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

   c. Require that users of information system accounts, or roles, with access to [entity defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing non-security functions.

   d. Restrict privileged accounts on the information system to [entity defined personnel or roles].

   e. Ensure that the information system audits the execution of privileged functions.

   f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

6. UNSUCCESSFUL LOGON ATTEMPTS
   IT Department shall ensure that the information system:

   a. Enforces a limit of consecutive invalid logon attempts by a user during a [entity defined frequency].

   b. Locks the account/node automatically for [entity defined frequency] or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

7. SYSTEM USE NOTIFICATION
   IT Department shall ensure that the information system:

   a. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

i. Users are accessing a [entity] information system.

ii. Information system usage may be monitored, recorded, and subject to audit.

iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

iv. Use of the information system indicates consent to monitoring and recording.

v. There are not rights to privacy.

b. Retains 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 information system.

c. For publicly accessible systems, the IT Department shall ensure that the information system:

i. Displays system use information [entity defined conditions], before granting further access.

ii. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

iii. Includes a description of the authorized uses of the system.

8. SESSION LOCK
IT Department shall ensure that the information system:

a. Prevent further access to the system by initiating a session lock after [entity defined frequency] of inactivity or upon receiving a request from a user.

b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

9. SESSION TERMINATION
IT Department shall:

a. Ensure that the information system automatically terminates a user session after [entity defined frequency].

10. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
IT Department shall:

a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

11. REMOTE ACCESS
IT Department shall:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

b. Authorize remote access to the information system prior to allowing such connections.

c. Ensure that the information system monitors and controls remote access methods.

d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

e. Ensure that the information system routes all remote accesses through [entity defined number] managed network access control points to reduce the risk for external attacks.

f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for [entity defined needs].

g. Document the rationale for such access in the security plan for the information system.

12. WIRELESS ACCESS
IT Department shall:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

b. Authorize wireless access to the information system prior to allowing such connections.

c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

13. ACCESS CONTROL FOR MOBILE DEVICES
IT Department shall:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

b. Authorize the connection of mobile devices to organizational information systems.

c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

14. USE OF EXTERNAL INFORMATION SYSTEMS
IT Department shall:

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

    i. Access the information system from external information systems.

    ii. Process, store, or transmit organization-controlled information using external information systems.

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

    i. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan.

    ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

15. INFORMATION SHARING
IT Department shall:

a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [entity defined information sharing circumstances where user discretion is required].

b. Employ [entity defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

16. PUBLICLY ACCESSIBLE CONTENT
IT Department shall:

a. Designate individuals authorized to post information onto a publicly accessible information system.

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

d. Review the content on the publicly accessible information system for nonpublic information [entity defined frequency] and removes such information, if discovered.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	Auditing and Accountability Policy Sample	MM/DD/YYYY

PURPOSE

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Auditing and Accountability (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. AUDIT EVENTS
   The information systems owners, in cooperation with audits and IT, shall:

a. Determine that the information system is capable of auditing the following events: [entity defined auditable events]

b. Coordinate the security audit function with other organizational entities requiring audit.

c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

d. Determine that the following events are to be audited within the information system:

   i. [entity defined auditable events].

2. REVIEWS AND UPDATES

   a. The organization shall review and update the audited events [entity defined frequency].

3. CONTENT OF AUDIT RECORDS

a. The information system shall 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 individuals or subjects associated with the event.

4. ADDITIONAL AUDIT INFORMATION

   a. The information system shall generate audit records containing the following additional information: [entity defined additional, more detailed information].

5. AUDIT STORAGE CAPACITY

   a. The information owner shall ensure audit record storage capacity is allocated in accordance with [entity defined audit record storage requirements].

6. TRANSFER TO ALTERNATE STORAGE

   a. The information system shall off-load audit records [entity defined frequency] onto a different system or media than the system being audited.

7. RESPONSE TO AUDIT PROCESSING FAILURES
   The information system shall:

   a. Alert [entity defined personnel or roles] in the event of an audit.

   b. Take the following additional actions: [entity defined actions to be taken processing failure; and (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

8. AUDIT STORAGE CAPACITY

   a. The information system shall provide a warning to [entity defined personnel, roles, and/or locations] within [entity defined time period] when allocated audit record storage volume reaches [entity defined percentage] of repository maximum audit record storage capacity.

9. REAL-TIME ALERTS

   a. The information system shall provide an alert in [entity defined real-time period] to [entity defined personnel, roles, and/or locations] when the following audit failure events occur:

      i. [entity defined audit failure events requiring real-time alerts].

10. CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

a. The information system shall enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and rejects or delays network traffic above those thresholds.

11. SHUTDOWN ON FAILURE

a. The information system shall invoke a [full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available] in the event of [entity defined audit failures], unless an alternate audit capability exists.

12. AUDIT REVIEW, ANALYSIS, AND REPORTING
The information system owner shall:

a. Review and analyze information system audit records [entity defined frequency] for indications of [entity defined inappropriate or unusual activity].

b. Report findings to [entity defined personnel or roles].

13. PROCESS INTEGRATION

a. The information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

14. AUDIT REPOSITORIES

a. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness.

15. AUDIT REDUCTION AND REPORT GENERATION

a. The information system shall provide an audit reduction and report generation capability that:

i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.

ii. Does not alter the original content or time ordering of audit records.

16. AUTOMATIC PROCESSING

a. The information system shall provide the capability to process audit records for events of interest based on [entity defined audit fields within audit records].

17. TIME STAMPS
The information system shall:

a. Use internal system clocks to generate time stamps for audit records.

b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [entity defined granularity of time measurement].

18. SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
The information system shall:

a. Compare the internal information system clocks [entity defined frequency] with [entity defined authoritative time source].

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [entity defined time period].

19. PROTECTION OF AUDIT INFORMATION

a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

20. ACCESS BY SUBSET OF PRIVILEGED USERS

a. The organization shall authorize access to management of audit functionality to only [entity defined subset of privileged users].

21. AUDIT RECORD RETENTION

a. The information system owners shall retain audit records for [entity defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

22. LONG-TERM RETRIEVAL CAPABILITY

a. The information system owners shall employ [entity defined measures] to ensure that long-term audit records generated by the information system can be retrieved.

23. AUDIT GENERATION
The information system shall:

a. Provide audit record generation capability for the auditable events as defined at [entity defined information system components].

b. Allow [entity defined personnel or roles] to select which auditable events are to be audited by specific components of the information system.

c. Generate audit records for the events with the content as defined. [entity defined information system components].

24. TIME-CORRELATED AUDIT TRAIL

a. The information system shall comply with audit records from [entity defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [entity defined level of tolerance for relationship between time stamps of individual records in the audit trail].

25. STANDARDIZED FORMATS

a. The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

26. CHANGES BY AUTHORIZED INDIVIDUALS

a. The information system shall provide the capability for [entity defined individuals or roles] to change the auditing to be performed on [entity defined information system components] based on [entity defined selectable event criteria] within [entity defined time thresholds].

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xxx	Security Awareness and Training Policy Sample	MM/DD/YY

PURPOSE

To ensure that the appropriate level of information security awareness training is provided to all Information Technology (IT) users.

REFERENCES

National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Electronic Code of Federal Regulations (CFR): 5 CFR 930.301

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. SECURITY AWARENESS TRAINING
   The [entity] shall:

   a. Schedule security awareness training as part of initial training for new users.

   b. Schedule security awareness training when required by information system changes and then [entity specified frequency] thereafter.

   c. IT shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

      i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

      ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

2. SECURITY AWARENESS | INSIDER THREAT
   IT Department shall:

a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. ROLE-BASED SECURITY TRAINING
IT Department shall:

a. Provide role-based security training to personnel with assigned security roles and responsibilities:

i. Before authorizing access to the information system or performing assigned duties.

ii. When required by information system changes and [entity specified frequency] thereafter.

b. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

4. PHYSICAL SECURITY CONTROLS
IT Department shall:

a. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

5. PRACTICAL EXERCISES
IT Department shall:

a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

6. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

IT Department shall:

a. Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

7. SECURITY TRAINING RECORDS
The [entity] shall:

a. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

b. Retain individual training records for a [entity specified amount of time].

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xxx	Configuration Management Policy Sample	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) resources are inventoried and configured in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Configuration Management (CM)

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. BASELINE CONFIGURATION
   IT Department shall:

   a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

   b. Review and update the baseline configuration of the information system [entity defined frequency]

   c. Review and update the baseline configuration of the information system when required as a result of [entity defined circumstance] and as an integral part of information system component installations and upgrades.

   d. Retain one previous version of baseline configurations of information systems to support rollback.

2. CONFIGURATION CHANGE CONTROL
   IT Department shall:

   a. Determine the types of changes to the information system that are configuration-controlled.

   b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

   c. Document configuration change decisions associated with the information system.

d. Implement approved configuration-controlled changes to the information system.

e. Retain records of configuration-controlled changes to the information system for [entity defined time period].

f. Audit and review activities associated with configuration-controlled changes to the information system.

g. Coordinate and provide oversight for configuration change control activities through [entity defined configuration change control element (e.g., committee, board)] that convenes [entity defined frequency]; [entity defined configuration change conditions].

h. Test, validate, and document changes to the information system before implementing the changes on the operational system.

3. SECURITY IMPACT ANALYSIS
IT Department shall:

a. Analyze changes to the information system to determine potential security impacts prior to change implementation.

4. ACCESS RESTRICTIONS FOR CHANGE
IT Department shall:

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5. CONFIGURATION SETTINGS
IT Department shall:

a. Establish and document configuration settings for information technology products employed within the information system using [entity defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements.

b. Implement the configuration settings.

c. Identify, document, and approve any deviations from established configuration settings for [entity defined information system components] based on [entity defined operational requirements].

d. Monitor and control changes to the configuration settings in accordance with policies and procedures.

6. LEAST FUNCTIONALITY
   IT Department shall:

   a. Configure the information system to provide only essential capabilities.

   b. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.

   c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

   d. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

   e. Identify software programs not authorized to execute on information systems.

   f. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

   g. Review and update the list of unauthorized software programs annually.

7. INFORMATION SYSTEM COMPONENT INVENTORY
   IT Department shall:

   a. Develop and document an inventory of information system components that:

      i. Reflects the current information system accurately.

      ii. Includes all components within the authorization boundary of the information system.

      iii. Is at the level of granularity deemed necessary for tracking and reporting.

      iv. Includes information deemed necessary to achieve effective information system component accountability.

   b. Review and update the information system component inventory [entity defined frequency].

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

d. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.

e. Take the following actions when unauthorized components are detected:

    i. Disable network access by such components, or

    ii. Isolate the components and notifies the Chief Information Officer and system owner.

f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

8. CONFIGURATION MANAGEMENT PLAN
IT shall develop, document, and implement a configuration management plan for the information system that:

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

    b. Establishes a process for identifying configuration items throughout the system development life cycle 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.

    d. Protects the configuration management plan from unauthorized disclosure and modification.

9. SOFTWARE USAGE RESTRICTIONS
IT Department shall:

    a. Use software and associated documentation in accordance with contract agreements and copyright laws.

    b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

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

10. USER-INSTALLED SOFTWARE
IT Department shall:

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

c. Monitor policy compliance at [entity defined frequency].

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xxx	Identification and Authentication Policy (Sample)	MM/DD/YY

PURPOSE

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116; Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. IDENTIFICATION AND AUTHENTICATION
   IT Department shall:

   a. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of [entity] users.

   b. Ensure that information systems implement multifactor authentication for network access to privileged accounts.

   c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.

   d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.

   e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.

   f. Ensure that information systems implement 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 and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

g. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.

2. DEVICE IDENTIFICATION AND AUTHENTICATION
IT Department shall:

a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

3. IDENTIFIER MANAGEMENT
IT Department, through department information systems owners, shall:

a. Ensure that the [entity] manages information system identifiers by receiving authorization from [entity defined personnel or roles] to assign an individual, group, role, or device identifier.

b. Select an identifier that identifies an individual, group, role, or device.

c. Assign the identifier to the intended individual, group, role, or device.

d. Prevent reuse of identifiers for 90 days.

e. Disable the identifier after 30 days of inactivity.

4. AUTHENTICATOR MANAGEMENT
IT Department shall:

a. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

b. Establish initial authenticator content for authenticators defined by the organization.

c. Ensure that authenticators have sufficient strength of mechanism for their intended use.

d. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

e. Change default content of authenticators prior to information system installation.

f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.

g. Change/refresh authenticators every 90 days.

h. Protect authenticator content from unauthorized disclosure and modification.

i. Require individuals and devices to implement specific security safeguards to protect authenticators.

j. Change authenticators for group/role accounts when membership to those account changes.

k. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.

l. Ensure passwords must contain characters from three of the following five categories:

   i. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);

   ii. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);

   iii. Base 10 digits (0 through 9);

   iv. Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and

   v. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

m. Require passwords to have a minimum length of 8 characters.

n. Enforce at least one changed character when new passwords are created.

o. Store and transmit only cryptographically-protected passwords.

p. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.

q. Prohibit password reuse for 12 generations.

r. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

s. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

t. Enforce authorized access to the corresponding private key.

u. Map the authenticated identity to the account of the individual or group.

v. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

w. Require that the registration process to receive [entity defined types of and/or specific authenticators] be conducted in person or by a trusted third party before [entity defined registration authority] with authorization by [entity defined personnel or roles].

x. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [entity defined token quality requirements].

5. AUTHENTICATOR FEEDBACK
IT Department shall:

a. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

6. CRYPTOGRAPHIC MODULE AUTHENTICATION
IT Department shall:

a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

7. IDENTIFICATION AND AUTHENTICATION
IT Department shall:

a. Ensure that information systems uniquely identify and authenticate non-entity users or processes acting on behalf of non-entity users.

b. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

c. Ensure that information systems accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.

d. Ensure that the organization employs only FICAM-approved information system components in [entity defined information systems] to accept third-party credentials.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xxx	Incident Response Policy Sample	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to computer security incidents.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. INCIDENT RESPONSE TRAINING
   The [entity] shall:

   a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

      i. Within [entity defined time period] of assuming an incident response role or responsibility.

      ii. When required by information system changes, and [entity defined frequency] thereafter.

   b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

   c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

2. INCIDENT RESPONSE TESTING
   The [entity] shall:

   a. Test the incident response capability for the information system [entity defined frequency] using [Assignment: entity defined tests] to determine the incident response effectiveness and documents the results.

   b. Coordinate incident response testing with entity contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster

Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

3. INCIDENT HANDLING
   The [Entity] shall:

   a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

   b. Coordinate incident handling activities with contingency planning activities.

   c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

4. INCIDENT MONITORING
   The [Entity] shall:

   a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

5. INCIDENT REPORTING
   The [Entity] shall:

   a. Require personnel to report suspected security incidents to the incident response capability within [entity defined time period].

   b. Report security incident information to [entity defined authorities].

6. INCIDENT RESPONSE ASSISTANCE
   The [entity] shall:

   a. Provide an incident response support resource, integral to the incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

7. INCIDENT RESPONSE PLAN
   The [entity] shall:

   a. Develop an incident response plan that:

      i. Provides the entity with a roadmap for implementing its incident response capability.

      ii. Describes the structure of the incident response capability.

iii. Provides a high-level approach for how the incident response capability fits into the overall entity.

iv. Meets the unique requirements of the entity, which relate to mission, size, structure, and functions.

v. Defines reportable incidents.

vi. Provides metrics for measuring the incident response capability within the entity.

vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

viii. Is reviewed and approved by [entity defined personnel or roles].

b. Distribute copies of the incident response plan to [entity defined incident response personnel (identified by name and/or by role)].

c. Review the incident response plan [entity defined frequency].

d. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.

e. Communicate incident response plan changes to [entity defined incident response personnel (identified by name and/or by role)].

f. Protect the incident response plan from unauthorized disclosure and modification.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	Maintenance Policy Sample	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) resources are maintained in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – System Maintenance (MA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-88, NIST SP 800-100; Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. CONTROLLED MAINTENANCE
   IT Department shall:

   a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or requirements conducted by local IT and/or outsourced IT entities.

   b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

   c. Require that system owners explicitly approve the removal of the information system or system components from facilities for off-site maintenance or repairs.

   d. Sanitize equipment to remove all information from associated media prior to removal from [entity] facilities for off-site maintenance or repairs.

   e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

   f. Include IT and system owner’s defined maintenance-related information in maintenance records.

g. For those components not directly associated with information processing such as scanners, copiers, and printers, maintenance records must include date and time of maintenance, entity performing the maintenance, maintenance performed, components replaced or removed including identification/serial numbers as applicable.

2. MAINTENANCE TOOLS
IT Department shall:

a. Ensure that system owners and IT approve, control, and monitor information system maintenance tools.

b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

c. Check media containing diagnostic and test programs for malicious code before the media are used in the information system.

3. NONLOCAL MAINTENANCE
IT Department shall:

a. Approve and monitor non-local maintenance and diagnostic activities.

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with policy and documented in the security plan for the information system.

c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.

d. Maintain records for nonlocal maintenance and diagnostic activities.

e. Terminate session and network connections when nonlocal maintenance is completed.

f. Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

4. MAINTENANCE PERSONNEL
IT Department shall:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.

c. Designate personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

5. TIMELY MAINTENANCE
IT Department shall:

   a. Obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	Media Protection Policy Sample	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) controls access to and disposes of media resources in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Media Protection (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111;
NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. MEDIA ACCESS:
   IT through direction from departments shall:

   a. Restrict access to [entity defined types of digital and/or non-digital media] to [entity identified staff].

   b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

2. MEDIA STORAGE
   IT Department shall:

   a. Specify staff to physically control and securely store media within defined controlled areas.

   b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3. MEDIA TRANSPORT
   IT Department Shall:

   a. Protect and control media during transport outside of controlled areas.

   b. Maintain accountability for information system media during transport outside of controlled areas.

c. Document activities associated with the transport of information system media.

d. Restrict the activities associated with the transport of information system media to authorized personnel.

4. MEDIA SANITIZATION
IT Department shall:

a. Sanitize prior to disposal, release out of organizational control, or release for reuse using [entity specified standard] in accordance with applicable federal and organizational standards and policies.

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

5. MEDIA USE
IT Department shall:

Prohibit the use of [entity defined types of information system media] on entity owned equipment using unapproved security safeguards.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xxx	Personnel Security Policy Sample	MM/DD/YY

PURPOSE

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Personnel Security (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800 -100; Electronic Code of Federal Regulations (CFR): 5 CFR 731.106; Federal Information Processing Standards (FIPS) 199 and 201; Intelligence Community Directive (ICD) 704 Personnel Security Standards

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. POSITION RISK DESIGNATION
   Information Technology (IT) shall:

   a. Assign a risk designation to all positions.

   b. Establish screening criteria for individuals filling those positions.

   c. Review and update position risk designations [entity defined frequency].

2. PERSONNEL SCREENING
   IT and department system and application owners shall:

   a. Screen individuals prior to authorizing access to the information systems.

   b. Rescreen individuals according to [entity defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

   c. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

3. PERSONNEL TERMINATION
   Departments shall, upon termination of individual employment:

   a. Disable information system access within [entity defined time period].

b. Terminate/revoke any authenticators/credentials associated with the individual.

c. Conduct exit interviews that include a discussion of [entity defined information security topics].

d. Retrieve all security-related information system-related property.

e. Retain access to information and information systems formerly controlled by terminated individual.

f. Notify [entity defined personnel or roles] within [entity defined time period].

   Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

The entity shall:

g. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.

h. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).

i. Employ automated mechanisms to notify [entity defined personnel or roles] upon termination of an individual.

4. PERSONNEL TRANSFER

Departments shall:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.

b. Initiate [entity defined transfer or reassignment actions] within [entity defined time period following the formal transfer action].

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

d. Notify [entity defined personnel] within [entity defined time period] of transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

5. ACCESS AGREEMENTS
Departments shall:

a. Develop and document access agreements for information systems.

b. Review and update the access agreements [entity defined frequency].

c. Ensure that individuals requiring access to information and information systems:

i. Sign appropriate access agreements prior to being granted access.

ii. Re-sign access agreements to maintain access to information systems when access agreements have been updated or [entity defined frequency].

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

6. THIRD-PARTY PERSONNEL SECURITY
IT Department shall:

a. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.

b. Require third-party providers to comply with personnel security policies and procedures established by the entity.

c. Require third-party providers to notify [entity defined personnel] of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within [entity defined time period].

d. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

1. PERSONNEL SANCTIONS
   IT and HR shall:

   a. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures

   b. Notify [entity defined personnel] within [entity defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

   Sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	Physical and Environmental Protection Policy Sample	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Physical and Environmental Protection (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116; Intelligence Community Directive (ICD): 704 705; Department of Defense (DoD): Instruction 5200.39 Critical Program Information (CPI) Protection; Federal Identity, Credential, and Access Management (FICAM) publication: Personal Identity Verification (PIV) in Enterprise Access Control System (E-PACS) (2012)

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. PHYSICAL ACCESS AUTHORIZATIONS
   IT Department shall:

   a. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.

   b. Issue authorization credentials for facility access.

   c. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.

2. PHYSICAL ACCESS CONTROL
   IT Department shall:

   a. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.

   b. Control ingress/egress to the facility using [entity defined physical access control systems/devices and/or guards].

   c. Maintain physical access audit logs for [entity defined entry/exit points].

d. Provide [entity defined security safeguards] to control access to areas within the facility officially designated as publicly accessible.

e. Escort visitors and monitors visitor activity in [entity specified areas].

f. Secure keys, combinations, and other physical access devices.

g. Inventory [entity defined physical access devices] every [entity defined frequency].

h. Change combinations and keys [entity defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

3. FACILITY PENETRATION TESTING
IT Department shall:

a. Employ a penetration testing process that includes [entity defined frequency], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

4. ACCESS CONTROL FOR TRANSMISSION MEDIUM
IT Department shall:

a. Control physical access to [entity defined information system distribution and transmission lines] within entity facilities using [entity defined security safeguards].

5. ACCESS CONTROL FOR OUTPUT DEVICES
IT Department shall:

a. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

6. MONITORING PHYSICAL ACCESS
IT Department shall:

a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.

b. Review physical access logs [entity defined frequency] and upon occurrence of [entity defined events or potential indications of events]; and coordinate results of reviews and investigations with the organizational incident response capability.

7. VISITOR ACCESS RECORDS
IT Department shall:

a. Maintain visitor access records to the facility where the information system resides for [entity defined time period]; and reviews visitor access records [entity defined frequency].

8. POWER EQUIPMENT AND CABLING
IT Department shall:

a. Protect power equipment and power cabling for the information system from damage and destruction.

b. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational 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.

9. EMERGENCY SHUTOFF
IT Department shall:

a. Provide the capability of shutting off power to the information system or individual system components in emergency situations.

b. Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.

10. EMERGENCY POWER
IT Department shall:

a. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.

b. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

11. EMERGENCY LIGHTING
IT Department shall:

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

b. Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

12. FIRE PROTECTION
IT Department shall:

a. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

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

13. TEMPERATURE AND HUMIDITY CONTROLS
IT Department shall:

a. Maintain temperature and humidity levels within the facility where the information system resides at [entity defined acceptable levels].

b. Monitor temperature and humidity levels [entity defined frequency] to include alarms or notifications of changes potentially harmful to personnel or equipment.

14. WATER DAMAGE PROTECTION
IT Department shall:

a. Protect 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.

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

15. DELIVERY AND REMOVAL
IT Department shall:

a. Authorize, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

16. ALTERNATE WORK SITE
IT Department shall:

a. Employ [entity defined security controls] at alternate work sites.

b. Assess as feasible, the effectiveness of security controls at alternate work sites.

c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	Planning Policy Sample	MM/DD/YYYY

PURPOSE

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Security Planning (PL), NIST SP 800-12, SP NIST 800-18,
NIST SP 800-100

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. SYSTEM SECURITY PLAN
   IT Department shall:

   a. Develop a security plan for each information system that:

      i. Is consistent with the [entity's] enterprise architecture.

      ii. Defines explicitly the authorization boundary for the system.

      iii. Describes the operational context of the information system in terms of missions and business processes.

      iv. Provides the security categorization of the information system including supporting rationale.

      v. Describes the operational environment for the information system and relationships with or connections to other information systems.

      vi. Provides an overview of the security requirements for the system.

      vii. Identifies any relevant overlays, if applicable.

      viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.

ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.

c. Review the security plan for the information system at least annually.

d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

e. Protect the security plan from unauthorized disclosure and modification.

2. RULES OF BEHAVIOR
IT Department shall:

a. Establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

b. Receive a signed 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. Review and update the rules of behavior.

d. Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised and updated.

3. INFORMATION SECURITY ARCHITECTURE
IT Department shall:

a. Develop information security architecture for the information system that will:

i. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

ii. Describe how the information security architecture is integrated into and supports the enterprise architecture.

iii. Describe any information security assumptions and dependencies on external services.

b. Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.

c. Ensure that planned information security architecture changes are reflected in the security plan, the security operations and procurements/acquisitions.

4. DEFENSE-IN-DEPTH APPROACH
IT Department shall:

a. Design security architecture using a defense-in-depth approach that:

i. Allocates security safeguards to [entity] defined locations and architectural layers.

ii. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xxx	Risk Assessment Policy Sample	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) performs risk assessments in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Risk Assessment (RA), NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NIST SP 800-60, NIST SP 800-70, NIST SP 800-100, NIST SP 800-115; NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. SECURITY CATEGORIZATION
   IT Department shall:

   a. Apply proper security controls to data categorized as confidential by system owners, including protected health information (PHI) and personally identifiable information (PII), in accordance with applicable federal and state laws, directives, policies, regulations, standards, and guidance.

   b. Document the security controls (including supporting rationale) in the security plan for the information system.

2. RISK ASSESSMENT
   IT Department shall:

   a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

   b. Document risk assessment results in annual IT Risk Assessment.

   c. Review risk assessment results quarterly.

   d. Disseminate risk assessment results to stakeholders.

   e. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

3. VULNERABILITY SCANNING
   IT Department shall:

   a. Scan for vulnerabilities in the information system and hosted applications quarterly and/or randomly in accordance with [entity defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported.

   b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

      i. Enumerating platforms, software flaws, and improper configurations.

      ii. Formatting checklists and test procedures.

      iii. Measuring vulnerability impact.

   c. Analyze vulnerability scan reports and results from security control assessments.

   d. Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.

   e. Share information obtained from the vulnerability scanning process and security control assessments with the Chief Information Officer to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

   f. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

   g. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.

   h. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	System and Communications Protection Policy Sample	MM/DD/YYYY

PURPOSE

To establish guidelines for system and communications protection for Information Technology (IT) resources and information systems.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-53a - System and Communications Protection (SC), NIST SP 800-12, NIST SP 800-28, NIST SP 800-41, NIST SP 800-52, NIST SP 800-56, NIST SP 800-57, NIST SP 800-58, NIST SP 800-77, NIST SP 800-81, NIST SP 800-95, NIST SP 800-100, NIST SP 800-111, NIST SP 800-113; NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 199

POLICY

This policy is applicable to all departments and users of resources and assets.

1. APPLICATION PARTITIONING
   IT Department shall:

   a. Separate user functionality from information system management functionality either logically or physically.

      Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

2. INFORMATION IN SHARED RESOURCES
   IT Department shall:

   a. Prevent unauthorized and unintended information transfer via shared system resources.

      This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. DENIAL OF SERVICE PROTECTION
   IT Department shall:

a. Ensure that the information system protects against or limit the effects of the following types of denial of service attacks: [entity defined types of denial of service attacks] by employing [entity defined security safeguards].

b. The information system restricts the ability of individuals to launch [entity defined denial of service attacks] against other information systems.

4. BOUNDARY PROTECTION
IT Department shall:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

b. Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

5. TRANSMISSION CONFIDENTIALITY AND INTEGRITY
IT Department shall:

a. Deploy information systems that protect the [confidentiality; integrity] of transmitted information.

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

6. NETWORK DISCONNECT
IT Department shall:

a. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after [entity defined time period] of inactivity; this control applies to both internal and external networks.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

7. CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
IT Department shall:

   a. Establish and manage cryptographic keys for required cryptography employed within the information system in accordance with [entity defined requirements for key generation, distribution, storage, access, and destruction].

8. CRYPTOGRAPHIC PROTECTION
IT Department shall:

   a. Implement [entity defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal and state laws, directives, policies, regulations, and standards.

   Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

9. COLLABORATIVE COMPUTING DEVICES
IT Department shall:

   a. Prohibit remote activation of collaborative computing devices with the following exceptions: [entity defined exceptions where remote activation is to be allowed].

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

   Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

10. PUBLIC KEY INFRASTRUCTURE CERTIFICATES
IT Department shall:

   a. Issue public key certificates under a [defined certificate policy] or obtain public key certificates from an approved service provider.

b. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

11. MOBILE CODE
IT Department shall:

a. Define acceptable and unacceptable mobile code and mobile code technologies.

b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

c. Authorize, monitor, and control the use of mobile code within the information system.

Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.

12. VOICE OVER INTERNET PROTOCOL
IT Department shall:

a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

b. Authorize, monitor, and control the use of VoIP within the information system.

13. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
IT Department shall:

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

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

This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

14. SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
IT Department shall:

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

   Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

15. ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
IT Department shall:

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

b. Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy.

   Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

16. SESSION AUTHENTICITY
IT Department shall:

a. Ensure the information system protects the authenticity of communications sessions.

   This control addresses communications protection at the session versus 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.

17. PROTECTION OF INFORMATION AT REST
IT Department shall:

a. Ensure the information system protects the [confidentiality; integrity] of [entity defined information at rest].

   This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

18. PROCESS ISOLATION
    IT Department shall:

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

       Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	System and Information Integrity Policy Sample	MM/DD/YYYY

PURPOSE

To ensure that Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Information Integrity (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. FLAW REMEDIATION
   IT Department shall:

   a. Identify, report, and correct information system 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 within [entity defined time period] of the release of the updates.

   d. Incorporate flaw remediation into the configuration management process.

   e. Employ automated mechanisms [entity defined frequency] to determine the state of information system components with regard to flaw remediation.

2. MALICIOUS CODE PROTECTION
   IT Department shall:

   a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

b. Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.

c. Configure malicious code protection mechanisms to:

   i. Perform periodic scans of the information system [entity defined frequency] and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy.

   ii. Block malicious code; quarantine malicious code; send alert to administrator; [entity defined action] in response to malicious code detection.

   iii. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

1. INFORMATION SYSTEM MONITORING
IT Department shall:

a. Monitor the information system to detect:

   i. Attacks and indicators of potential attacks.

   ii. Unauthorized local, network, and remote connections.

b. Identify unauthorized use of the information system through defined techniques and methods.

c. Deploy monitoring devices strategically within the information system to collect [entity determined essential information] and at ad hoc locations within the system to track specific types of transactions of interest to the entity.

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.

g. Provide information system monitoring information to authorized personnel or business units as needed.

2. SYSTEM-GENERATED ALERTS
IT Department shall ensure that:

a. The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).

b. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. Personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

3. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
IT Department shall:

a. Receive information system security alerts, advisories, and directives from [entity defined 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: [entity defined personnel or roles]; [entity defined elements within the organization]; [entity defined external organizations].

d. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

4. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
IT Department shall:

a. Employ integrity verification tools to detect unauthorized changes to [entity defined software, firmware, and information];

b. Ensure the information system performs an integrity check of [entity defined software, firmware, and information] at startup, and/or at [entity defined transitional states or security-relevant events], [entity defined frequency].

c. Incorporate the detection of unauthorized [entity defined security-relevant changes to the information system] into the incident response capability.

5. SPAM PROTECTION
IT Department shall:

a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.

b. Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.

c. Manage spam protection mechanisms centrally.

d. Ensure information systems automatically update spam protection mechanisms.

6. INFORMATION INPUT VALIDATION
IT Department shall:

a. Ensure the information system:

i. Checks the validity of [entity defined information inputs].

ii. Provides a manual override capability for input validation of [entity defined inputs].

iii. Restricts the use of the manual override capability to only [entity defined authorized individuals].

iv. Audits the use of the manual override capability.

v. Reviews and resolve within input validation errors.

vi. Behaves in a predictable and documented manner that reflects system objectives when invalid inputs are received.

7. ERROR HANDLING
IT Department shall:

a. Ensure the information system:

i. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

ii. Reveals error messages only to [entity defined personnel or roles].

8. INFORMATION HANDLING AND RETENTION
   IT Department shall:

   a. Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

9. MEMORY PROTECTION
   IT Department shall:

   a. Ensure the information system implements [entity defined security safeguards] to protect its memory from unauthorized code execution.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
x.xx	System and Services Acquisition Policy Sample	MM/DD/YYYY

PURPOSE

To ensure that Information Technology (IT) resources and information systems are acquired with security requirements to meet the information systems mission and business objectives.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Services Acquisition (SA), NIST SP 800-12, NIST SP 800-23, NIST SP 800-35, NIST SP 800-36, NIST SP 800-37, NIST SP 800-64, NIST SP 800-65, NIST SP 800-70, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137; Homeland Security Presidential Directive (HSPD) 12; International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) Standard 15408; NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 201

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. ALLOCATION OF RESOURCES
   IT Department, in direct guidance and association with the information system owner shall:

   a. Determine information security requirements for the information system or information system service in mission/business process planning.

   b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.

   c. Establish a discrete line item for information security in organizational programming and budgeting documentation.

2. SYSTEM DEVELOPMENT LIFE CYCLE
   IT Department, in direct guidance and association with the information system owner shall develop a contingency plan for the information system that:

   a. Manages the information system using the system development life cycle to ensure incorporation information security considerations.

   b. Defines and documents information security roles and responsibilities throughout the system development life cycle.

c. Identifies individuals having information security roles and responsibilities.

d. Integrates the information security risk management process into system development life cycle activities.

3. ACQUISITION PROCESS
IT shall ensure the acquisition process includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal, state, and local laws, Executive Orders, directives, policies, regulations, standards, guidelines, and mission and 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 information system development environment and environment in which the system is intended to operate.

   g. Acceptance criteria.

4. SECURITY CONTROLS
Information Technology (IT) shall require the information system, system component, or information system service:

   a. Describe the functional properties of the security controls to be employed; security-relevant external system interfaces; high-level design, low-level design, source code or hardware schematics that meet the business requirements.

   b. Identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

   c. Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within information systems.

5. INFORMATION SYSTEM DOCUMENTATION
IT Department shall:

a. Obtain administrator documentation for the information system, system component, or information system service that describes:

    i. Secure configuration, installation, and operation of the system, component, or service.

    ii. Effective use and maintenance of security functions/mechanisms.

    iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

b. Obtain user documentation for the information system, system component, or information system service that describes:

    i. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.

    ii. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.

    iii. User responsibilities in maintaining the security of the system, component, or service.

c. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [entity defined actions] in response.

d. Protect documentation as required, in accordance with the risk management strategy.

e. Distribute documentation to only authorized persons or entities.

6. SECURITY ENGINEERING PRINCIPLES
IT Department shall:

a. Apply industry standard information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

7. EXTERNAL INFORMATION SYSTEM SERVICES
IT Department shall:

a. Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

b. Define and document government oversight and user roles and responsibilities with regard to external information system services.

c. Employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

d. Require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

8. DEVELOPER CONFIGURATION MANAGEMENT
IT Department shall ensure developers of the information system, system component, or information system service:

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

b. Document, manage, and control the integrity of changes to configuration items under configuration management.

c. Implement only organization-approved changes to the system, component, or service.

d. Document approved changes to the system, component, or service and the potential security impacts of such changes.

e. Track security flaws and flaw resolution within the system, component, or service and report findings to authorized personnel and/or business units.

9. DEVELOPER CONFIGURATION MANAGEMENT
IT Department shall:

a. Require the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

b. Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

c. Require the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

d. Require the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

e. Require the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

f. Require the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

10. DEVELOPER SECURITY TESTING AND EVALUATION
IT Department shall require the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan.

b. Perform unit; integration; system; regression 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.

e. Correct flaws identified during security testing/evaluation.

f. Employ static code analysis tools to identify common flaws and document the results of the analysis.

g. Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

11. INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE
IT Department shall:

a. Require an independent agent satisfying to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation.

b. Ensure that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.

c. Perform a manual code review of defined processes, procedures, and/or techniques.

d. Perform penetration testing.

e. Verify that the scope of security testing/evaluation provides complete coverage of required security controls.

f. Employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY