Policy #:	Title:	Effective Date:
x.xx	System and Services Acquisition Policy	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