This document is downloaded by ministryofsecurity.co

Policy #:	Title:	Effective Date:
x.xxx	Configuration Management Policy	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