[Insert Company Name Or Logo]	
Title: Configuration Change	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: [Insert Company name] is responsible for ensuring the confidentiality, integrity, and availability of all sensitive and regulated data stored on its systems. [Insert Company name] has an obligation to provide appropriate protection against threats, which could adversely affect the security of the system or its data entrusted on the system. Implementation of this policy will limit the exposure and possible effects of common threats to the systems

Scope: The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by [Insert Company name]. All users are responsible for adhering to this policy.

Definitions:

1. Email: The electronic transmission of information through a mail protocol such as SMTP, POP, or IMAP.
2. User: any employee or other person authorized by the organization to read, edit or update information created or transmitted via the electronic mail system.

Procedure:

1. The Security Officer will be responsible for implementing this policy, and ensuring users comply with it.
2. Baseline Configuration
    a. Develop, document, and maintain a current baseline configuration of Information Systems.
    b. The baseline configuration must be reviewed and updated based on environment changes.
    c. At minimum, the baseline configuration shall include:
        i. Standard operating system/installed applications with current version numbers.
        ii. Standard software load for workstations, servers, network components, and mobile devices and laptops.
        iii. Up-to-date patch level information.
        iv. Network topology.
        v. Logical placement of the component within the system and enterprise architecture.
        vi. Technology platform.
    d. Maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.
    e. Monitor systems for security baselines and policy compliance.
3. Configuration Change Control
    a. Perform change control for key Information Systems. This shall include:
        i. Determining the type of changes to the information asset that are configuration controlled.
        ii. Approving configuration-controlled changes to the system with explicit consideration for security impact analysis.
        iii. Documenting approved configuration-controlled changes to the system.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

iv. Retaining and reviewing records of configuration-controlled changes to the system.
v. Auditing activities associated with configuration-controlled changes to the system.
    1. Auditing of changes must include changes in activity before and after a change is made to the information system and the auditing activities required to implement the change.
vi. Coordinating and providing oversight for configuration change control activities through Change Control Board (CCB) that convenes [Insert Timeframe (eg. Weekly, monthly)].
vii. Configuration change control for the information system shall involve the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications.
viii. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products, emergency changes, and changes to remediate flaws.

4. Security Impact Analysis
    a. Analyze changes to the Information Systems to determine potential security impacts prior to change implementation.
    b. Security impact analysis may include reviewing information system documentation, such as the security plan, to understand how specific security controls are implemented within the system and how the changes might affect the controls.
    c. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required.
    d. Security impact analysis is scaled in accordance with the security categorization of the information system.
5. Access Restrictions for Change
    a. Define, document, approve, and enforce physical and logical access restrictions with changes to the information asset.
    b. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.
    c. No local administrative rights will be granted without the submission of an exemption form or approval by the Security Officer or Information Systems Officer (ISO).
    d. Maintain records of access to ensure configuration change control is being implemented as intended, and for supporting alterations should the organization become aware of an unauthorized change to the information system.
    e. Create and maintain logical and physical access control lists that authorize qualified individuals to make changes to an information system or component.
    f. Access restrictions for change also include software libraries.
    g. Limit information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment.
    h. Review and reevaluate information system developer/integrator privileges [Insert timeframe (eg. Monthly, annually)].
6. Configuration Settings
    a. Establish, document, implement and monitor mandatory configuration settings for IT products employed within the information asset using a security configuration checklist that reflects the most restrictive mode consistent with operational requirements.
    b. Any exceptions to the mandatory configuration settings within the information asset must be identified, documented, and approved prior to ongoing use.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

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

7. Least Functionality
    a. Configure the information asset to provide only essential capabilities and specifically prohibit or restrict the use of the following functions, ports, protocols, and/or services.
    b. Any exceptions to baseline security configurations must be documented by security operations staff in writing and approved by the ISO.
    c. Security operations staff shall maintain records confirming the implementation of baseline security configurations for each IT system they manage.
    d. Security baseline implementation records will be audited [Insert timeframe (eg. Monthly, annually)] by the ISO, to verify the implementation of the appropriate baseline security configurations.
    e. Security operations staff shall perform network vulnerability scans of all server and desktop computers [Insert timeframe (eg. Monthly, annually)].
        i. The ISO shall review the results of the IT system vulnerability scans when completed.
        ii. Sensitive internal-facing web applications will be scanned for vulnerabilities [Insert timeframe (eg. Monthly, annually)]. Sensitive external-facing web applications must be scanned for vulnerabilities [Insert timeframe (eg. Monthly, annually)]. This scanning may be performed by security operations staff or system owners as is appropriate and convenient.
        iii. All identified operating system and application vulnerabilities will be remediated without undue delay according to the severity and risk.
    f. Where feasible, the organization will limit component functionality to a single function per device (e.g., email server or web server, not both).
8. Information System Component Inventory
    a. Develop, document, and maintain an inventory of the information asset components that exist within their area.
    b. Inventory detail must:
        i. Be maintained at a sufficient level for purposes of tracking and reporting.
        ii. Be consistent with the authorization boundary of the information system.
        iii. Be at the level of granularity deemed necessary for tracking and reporting.
        iv. Include organization-defined information deemed necessary to achieve effective property accountability, such as:
            1. Hardware inventory specifications (manufacturer, type, model, serial number, physical location).
            2. Software license information.
            3. Information system/component owner.
            4. For a networked component/device, the machine name and network address.
    c. Updated system and network diagrams must be maintained.
    d. The inventory must be made available for review and audit by designated organizational officials.
    e. The inventory must be updated as an integral part of component installations, removals, and information system updates.
    f. The inventory must include assessed component configurations and any approved deviations to current deployed configurations.
    g. The inventory must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:
        i. Manufacturer
        ii. Type
        iii. Model

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

iv. Serial number
v. Physical location
vi. Software license information
vii. Information system/component owner
viii. Associated component configuration standard
ix. Software/firmware version information
x. Networked component/device machine name or network address

9. Configuration Management Plan
    a. Develop, document, and implement a configuration management plan for the information asset that:
        i. Addresses roles, responsibilities, and configuration management processes and procedures.
        ii. Defines the configuration items for the information asset and that, when in the system development life cycle, the configuration items are placed under configuration management.
        iii. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
        iv. Assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.
        v. Defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level.
        vi. Describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated.
    b. The configuration management approval process must include:
        i. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system.
        ii. Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.
    c. In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process.

Violations:
Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment. Violations shall be noted in the [Insert Company name] issue tracking system and support teams shall be dispatched to remediate the issue.

Attachments: None

Related Policies:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.