# COMMONWEALTH OF PENNSYLVANIA

# HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY POLICY

|  |  |
| --- | --- |
| Name of Policy:  **Configuration Management Policy** | **Number:**  **POL-SEC014** |
|  |  |
| Domain: | Category: |
| **Security** | **Configuration Management** |
| Date Issued: | Issued by Direction Of: |
| **02/10/2021** |  |
| Date Revised: |  |
| **02/10/2021** | **Sandra K. Patterson, CIO**  **Health & Human Services Delivery Center** |

**Abstract:**

The purpose of this policy is to establish a Configuration Management program and to provide responsibilities, requirements and principles for Change Management processes to support Information Technology Management across the Department of Human Services (DHS).

**General:**

Information systems are always in a constant state of change due to steady releases of new hardware, software, firmware or modifications to the environment where these systems reside. Industry standards such as National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the Internal Revenue Service (IRS) Publication 1075 have all identified the need for control around configuration management. Configuration Management is a key control for ensuring changes to network devices are continuously tracked and authorized.

**Policy:**

**Scope**

All DHS employees, contractors and business partners are responsible for understanding and complying with this policy. This policy is based on Federal and Pennsylvania state laws, regulations, leading information security practices (e.g., National Institute of Standards and Technology [NIST] Special Publication 800-53 Revision 4 and the Internal Revenue Service [IRS] Publication 1075). Guidance provided from other various laws and standards for this policy are listed in the Appendix.

**Compliance**

Violations of this policy may lead to revocation of system privileges and/or disciplinary action.

# Roles and Responsibilities

Required roles and responsibilities may be fulfilled by one or more individuals.

**Change Advisory Board (CAB)** is responsible for:

* Provide enterprise risk management, communication management and process compliance management to the change process environment; Review/Approve changes and ensure changes to DHS infrastructure or contracted DHS systems are reviewed and processed in accordance with established Change Management processes and procedures,
* Establishing a configuration management framework ensuring definition and maintenance of configuration baselines and the identification, management and tracking of associated hardware, software and documentation configuration items for each DHS system,
* Ensuring all changes to configuration items adhere to DHS policy and are documented, tested, and approved. This includes ensuring changes are evaluated to determine the impact to system security before implementation; and

**Change Coordinator** is responsible for:

* Coordinating and facilitating CAB meetings,
* Documenting and distributing CAB meeting minutes, decisions and actions,
* Reviewing proposed Requests for Changes,
* Preparing and distributing implementation schedules for all approved changes,
* Providing immediate disposition of directed or emergency changes, without going through the mechanism of change control,
* Assisting with Change Post Implementation Reviews,
* Collecting, collating and reporting change management metrics and
* Executing tasks delegated by the CAB Chairperson.

**CAB Chairperson** is responsible for:

* Managing, maintaining & ensuring compliance to the Change Control process,
* Tabling Requests for Changes for CAB meetings,
* Determining CAB meeting participants based on the nature of the Requests for Changes Chairing the CAB,
* Convening meetings to consider emergency Requests for Changes and
* Acting as a main point of contact for change management issues.

**Configuration Manager** is responsible for:

* Overall responsibility and authority for the Configuration Management process,
* Handling all Configuration Management issues involving management and oversight of requirements; version control; hardware/software development; and, adherence to established standards and guidance,
* Ensuring that proposed changes are executed within a disciplined process & considering the technical, programmatic, security, and schedule impacts of the proposed changes,
* Conducting audit reviews and
* Assigning attributes to configuration items.

**Change Implementers** are responsible for:

* Testing, Implementing and Reversing changes,
* Entering configuration status accounting information and
* Responding to inquiries regarding changes.

**Change Requestor** is responsible for creating a Request for Change.

**Chief Technology Officer (CTO)** is responsible for:

* Providing procedures, standards, and guidance to senior level managers in support of the Agency’s Configuration Management Policy,
* Instituting change management processes and
* Providing a change approval system for DHS (i.e., CDMB, a change approval and tracking application and database).

**Configuration Management Policy**

| **DHS Policy** |
| --- |
| 1. DHS must meet or exceed all Federal regulatory policies and procedures which affect Configuration and Change Management processes to be implemented on DHS information technology assets. This includes procedures such as: 2. Documenting and maintaining the configuration baseline(s) applicable to the deployed system; 3. Managing and tracking all system configuration and associated document changes, as well as the integrity, availability and maintainability of the system; 4. Planning to ensure the ability to reverse a deployment or implementation; and 5. Tracking all system changes made, including installation of patches, to hardware, software, firmware, and documentation, through development, approval, testing, and controlled implementation of changes delivered into production environments. 6. Agencies should utilize a Configuration Management Database (CMDB) that contains and tracks relevant information about configuration items, their attributes, baselines, documentation, changes, and relationships. 7. Changes to any portion of DHS’s IT environment that might impact network security, performance, or operations must be recorded in a central tracking application and database. These include changes to portions of DHS’s IT environments, including network, LAN, WAN, telecommunications, mainframe, hosting, and servers. |

# Appendix

1. National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4)
2. IRS Publication 1075

CMS Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E) Version 2.0

# Exemptions from this Policy:

Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period.

**Refresh Schedule:**

This policy is required to be revised at least every three years. Procedures stemming from this policy are required to be reviewed & revised on an annual basis.

**Policy Revision Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Change Date** | **Version** | **Change Description** | **Author and Organization** |
| 02/10/2021 | 1.0 | Policy created | John Miknich |