METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 13
SUBJECT: CHANGE MANAGEMENT	DISTRIBUTION DATE: 5/1/2017
	EFFECTIVE DATE: 5/15/2017
ISSUING AUTHORITY: DIRECTOR OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to ensure Metropolitan Government of Nashville and Davidson County (Metropolitan Government) reduces risks to information security caused by changes to information assets and systems. Inadequate control of changes to information assets and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications.

POLICY

1.0 Generally

Changes to the organization, business processes, information assets and systems that affect information security shall be controlled by the use of formal change control procedures.

Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all applicable changes. When applicable changes are made, an audit log containing all relevant information should be retained.

As set forth below, Metropolitan Government's change management processes are supported through the use of the controls set forth in: (i) baseline configuration (Section 2.1 below); (ii) change control (see Section 2.2 below); (iii) security impact analysis (see Section 2.3 below); (iv) access restrictions for change (see Section 2.4 below); (v) configuration settings (see Section 2.5 below); (vi) least functionality (see Section 2.6 below); and (vii) configuration management plan (see Section 2.7 below).

2.0 Detailed

2.1 Baseline Configuration

Metropolitan Government shall develop, document and maintain under configuration control, a current secure baseline configuration of applicable information assets and systems. Metropolitan Government shall review and update the applicable baseline configuration on a periodic basis and when any changes are made.

2.2 Change Control

Metropolitan Government shall test, validate and document changes to the information processing facility and/or the information system before implementing the changes on its operational system. In addition, it shall employ, where applicable, automated mechanisms to implement changes to the current information system baseline. Metropolitan Government shall:

a. Determine the types of changes to the information assets that should be controlled through the change management process;

b. Approve controlled changes to the assets and/or system with explicit consideration for security impact;

c. Document approved controlled changes to the assets and/or system, documentation to include:

    a. documentation of the changes;

    b. planning and testing of changes;

    c. assessment of the potential impacts, including security impacts, of such changes;

    d. communication of change details to all relevant persons;

    e. fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;

    f. approval of changes;

d. Retain and review records of controlled changes to the assets and/or system;

e. Audit activities associated with controlled changes to the assets and/or system; and

f. Coordinate and provide oversight for configuration change control activities through a change management committee or change approval board, which convenes weekly.

2.3 Security Impact Analysis

Metropolitan Government shall include as part of change control a consideration for any potential security impacts prior to change implementation. Individuals conducting security impact analyses shall have the appropriate skills and technical expertise to analyze and identify the associated security ramifications.

2.4 Access Restrictions for Change

Metropolitan Government shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information assets. It also shall:

a. Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions, where applicable;

b. Conduct audits of information assets changes, and when indications so warrant, determine whether unauthorized changes have occurred;

c. Limit developer/integrator privileges to change hardware, software and firmware components and system information directly within a production environment; and

d. Review and reevaluate developer/integrator privileges annually.

2.5 Configuration Settings

Metropolitan Government shall:

a. Establish and document mandatory configuration settings for applicable information technology products using security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

b. Implement the configuration settings;

c. Identify, document and approve exceptions from the mandatory configuration settings for individual components based on explicit operational requirements; and

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

e. Employ, where possible, automated mechanisms to centrally manage, apply and verify configuration settings;

f. Employ, where possible, automated mechanisms to respond to unauthorized changes to defined configuration settings;

g. Incorporate detection of unauthorized security-relevant configuration changes into its incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes;

h. Demonstrate conformance to security configuration guidance (i.e., security checklists), prior to change being introduced into a production environment.

2.6 Least Functionality

Metropolitan Government shall configure information assets to provide only essential capabilities and specifically prohibit or restrict the use of designated and documented functions, ports, protocols, and/or services. It shall:

a. Review information assets to identify and eliminate unnecessary functions, ports, protocols, and/or services; and

b. Employ automated mechanisms, where possible, to prevent program execution.

2.7 Configuration Management Plan

Metropolitan Government shall develop, document and implement a configuration management plan for information assets that:

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

b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management;

c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items; and

d. Defines how business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300.

4/26/17

Keith Durbin
Director of Information Technology Services
Metropolitan Government of Nashville and Davidson County

Date

REFERENCES

- ISO 27002: sections *10.1.2(ISO 207002 A.12.1.2) (A.14.2.2)*
- NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST Special Publication 800-53 rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations:* Control numbers – CA-2, CA-7, RA-5, SC-34, SI-4, SI-7, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9
- Center for Internet Security Critical Security Benchmark #4

REVISION HISTORY

REVISION	DATE	CHANGES
0.1	02/17/2017	Draft
1.0	4/26/2017	Approved policy.