METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 10
SUBJECT: INVENTORY AND OWNERSHIP OF ASSETS	DISTRIBUTION DATE: 9/1/2011
	EFFECTIVE DATE: 3/1/2012
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 that the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) achieves and maintains appropriate protection of its assets as they relate to the collection, processing and storage of information.

POLICY

1. Generally

   Metropolitan Government shall clearly identify all of its assets and shall develop and maintain an inventory of all important assets that, in the event of loss, disclosure or unauthorized access, could pose a risk to the Metropolitan Government. Such assets shall include hardware, software, information, services, people, and intangibles. As applicable, ownership for hardware, software, and information as well as parties responsible for services, personnel, and intangibles shall be designated and documented for each asset and shall be reviewed/updated at least annually.

   Metropolitan Government's compilation of its inventory and ownership of assets is supported through the use of the controls set forth in the sections below.

   All assets shall include classification, based on the classification of the data that they store or process, and criticality, based on the criticality of the services they support.

2. Configuration Management Plan

   Metropolitan Government shall develop, document and implement a configuration management plan for its inventory of assets, otherwise referred to as configuration items, that:

   2.1. Addresses roles, responsibilities and configuration management processes and procedures;
   2.2. Defines the configuration items and at what point in the system development life cycle the configuration items are placed under configuration management; and
   2.3. Establishes the means for identifying configuration items throughout the system development life cycle and a process for identifying and managing the relationships of the configuration items.

3. Inventory of Configuration Items

Metropolitan Government shall develop and maintain an inventory of its assets. Such inventory shall:

3.1. Be the responsibility of the director of the department to which the asset is assigned;
3.2. Be current and accurate;
3.3. Identify the owner of and/or individual responsible for the asset;
3.4. Be at a level of granularity deemed necessary for tracking and reporting;
3.5. Include information deemed necessary to achieve effective property accountability;
3.6. Be available for review and audit by designated Metropolitan Government officials;
3.7. Include information designated and/or required to ensure business continuity.

4. Hardware

Metropolitan Government shall develop and maintain an inventory of its hardware connected to the network and the network devices themselves including information identifying by name, position or role, as appropriate, owners and/or individuals responsible for the hardware.

5. Software

Metropolitan Government shall develop and maintain an inventory of its software and applications. The inventory shall include information identifying by name, position or role, as appropriate, owners and/or individuals responsible for the software, the location of the software, related license keys, and any pertinent installation information. The inventory shall also include baseline software configurations, approved deviations and any mission critical applications. The inventory of software and applications shall be updated as an integral part of installations, removals and information system updates.

Metropolitan Government shall develop a process to alert on the installation of any unapproved software.

All software and applications must be fully licensed and supported. Any software or applications that have reached end of life/end of support must be tracked as security exceptions.

6. Information

Metropolitan Government shall develop an inventory of its information. Electronic information shall be mapped to the hardware (including servers, workstations and laptops) on which such information resides. The physical location of non-electronic information, including paper records, shall be identified as part of the inventory. A Metropolitan Government department, agency or board and an owner of such information (Information Owner) shall be identified, recorded and tracked. Such information shall be classified as set forth in the Metropolitan Government *Information Classification Policy.*

7. Services

Metropolitan Government shall develop and maintain an inventory of its essential services. The inventory for both internally and externally provided and/or required services shall include, but is not limited to, computing, communications services, general utilities (e.g., heating, lighting, power,

and air-conditioning), and other general services (e.g., security, shredding services, janitorial, etc.). Those roles responsible for the provisioning of such services shall be identified.

8. People

   Metropolitan Government shall develop and maintain an inventory of its personnel, contractors and other essential individuals. The inventory for personnel shall include their qualifications, skills, experience and supervisor.

9. Intangibles

   Metropolitan Government shall develop and maintain an inventory of its intangibles. The inventory for intangibles shall include Metropolitan Government's reputation and image.

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

SIGNATURE

Keith Durbin,
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: sections 7.1.1, 7.1.2
- Center for Internet Security Critical Security Controls 1, 2, 3, 11
- NIST Cyber Security Framework ver 2.0 ID.AM-1, ID.AM-2, ID.AM-5, PR.DS-3
- NIST Special Publications 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*: CM-8, CM-9, PM-5
- Metropolitan Government Information Security Policy *Information Classification Policy*
- NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	9/1/2011	First released version
1.1	5/24/2016	• Change number of policy from 7.1 to 10 to reflect new naming standard. • Addition of Hardware and Software subheadings under the General heading and all the content is those subheadings to better align with NIST CyberSecurity Framework ID.AM-1 and ID.AM-2. • Addition of "Secure Configurations" heading to align with Center For Internet Security Controls 1.1, 1.3, 1.4, 2.3, 3.x • Additional references (NIST Cyber Security Framework ID.AM-1, ID.AM-2 and Center For Internet Security Controls 1.1, 1.3, 1.4, 2.3, 3.x
1.2	8/15/2018	• Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against. • Added "All assets shall include classification, based on the classification of the data that they store or process, and criticality, based on the criticality of the services they support." based on CSF ID.AM-5 • Added review of applicable CSCs.
1.3	8/29/2025	• Change to reflect use of rev 2 of NIST Cybersecurity Framework • Change to reflect use of NIST 800-171 r3 as a reference