METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY POLICY

SUBJECT:	DISTRIBUTION DATE: 03/26/2010
INFORMATION SECURITY MANAGEMENT POLICY	EFFECTIVE DATE: 03/26/2010
ISSUING AUTHORITY: Mayor of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this Information Security Management Policy ("Policy") is to provide consistent direction and support for Information Security at the Metropolitan Government of Nashville and Davidson County ("Metropolitan Government").

POLICY

1. **Minimum Standards**

   Maintaining the confidentiality, integrity, and availability of information, information technology, and critical operational processes in a manner meeting the Metropolitan Government's legal, regulatory and ethical responsibilities on behalf of its citizens is of paramount importance to the Metropolitan Government. The Director of Information Technology Services ("Director") shall develop, disseminate, review, and update an Information Security Management Program ("Program") consisting of policies, procedures, plans, standards, guidelines, and controls that are consistent with and meet those responsibilities.

   Metropolitan Government departments, agencies, and boards must meet the minimum security requirements recommended by the Director and adopted by the Metropolitan Government that set the floor for Information Security management. Each department, agency, and board must also:

   - Define their mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, and individuals,
   - Determine information protection needs arising from the defined mission/business processes and revise the processes as necessary, until achievable protection needs are obtained,
   - Communicate those protection needs to the appropriate providers, and
   - Adopt Information Security requirements that afford greater protections than the baselines if necessary.

   Metropolitan Government aspires to fully protect citizen information and services through the use of multiple information security controls, including technical, administrative and physical controls. However, information security is not an absolute and the Metropolitan Government cannot absolutely guarantee the security of the information that it handles. This Program is an

effort to strive to maintain a reasonable continuous process for implementing, reviewing and improving data security.

2. Security Policies and Procedures, Plan, and Priorities

2.1 Policies and Procedures

The Director shall develop, disseminate, review, and update:

- Policies that address the purpose, scope, roles, responsibilities, management commitment, compliance, and coordination among the Metropolitan Government departments, agencies, and boards for protecting the confidentiality, integrity and availability of the information used and services provided by the Metropolitan Government;
- Procedures to facilitate the implementation of those policies and associated controls.

2.2 Plan

The Director shall develop and disseminate an Information Security plan that:

- Provides an overview of the requirements for the Program and approved Policies and a description of the controls in place or planned for meeting those requirements;
- Provides sufficient information controls to enable an implementation that is compliant with the intent of this Policy and all applicable Policies and a determination of the risk to be incurred if the plan is implemented as intended;
- Includes roles, responsibilities, management commitment, coordination among Metropolitan Government entities, and compliance;
- Is reviewed annually;
- Is revised to address organizational changes and problems identified during plan implementation or security control assessments.

2.3 Priorities

The Metropolitan Government priorities for Information Security are:

- Complying with applicable federal and state information privacy and security laws, regulations and contractual requirements;
- Developing an Information Security awareness training program for Metropolitan Government employees and third party users as originally required by Executive Order No. 005 and affirmed by Executive Order No. 034;
- Utilizing information security standards, frameworks and controls to develop the Program.

3. Review

The Director of the Department of Information Technology Services is responsible for the development, review, and evaluation of this Policy and all Policies developed in support of the Program. The review shall include assessing opportunities for improvement of Policies and responding to changes to the Metropolitan Government's environment, business circumstances, legal conditions, or technical environment.

4. Oversight

An Information Security Steering Committee (the "Steering Committee"), as established in Executive Order No. 038 and affirmed by Executive Order No. 34 will review and recommend to the Director changes to the information security policies, standards, and practices for the

Metropolitan Government. The Steering Committee will also develop and report on performance measures to determine the effectiveness of the Program.

5. **Exception Request**
   Any individual, department, or group that wishes to diverge or be exempt from any established Policies must request an exception from the Director.

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.

REFERENCES

ISO 27002: sections 5.1.1, 6.1
NIST Special Publications 800-53 Rev4, *Recommended Security Controls for Federal Information Systems and Organizations*, PM-1, PM-9, PM-11

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	3/26/2010	First released version.
1.1	2/24/2016	References to new affirmed EO. 34 added. Added CONTACT and REFERENCES section to align with current policy format. Removed specific references to areas to be addressedin 5.1 due to Program transition to NIST Cybersecurity Framework and from ISO 27002. Added bulleted list to section 1 to align with NIST SP800-53