METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY POLICY

SUBJECT: **INFORMATION SECURITY MANAGEMENT POLICY**	DISTRIBUTION DATE: 03/26/2010
	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ISSUING AUTHORITY: Mayor of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 ("CIO") shall develop, disseminate, review, and update an Information Security Management Program ("Program") consisting of policies, procedures, plans, standards, guidelines, and controls that shall aid departments, agencies, and boards in meeting this goal.

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

   - Fully understand their roles and responsibilities as defined in the *Metropolitan Government Scope, Background, and Governance Statement for Information Security Policies*,
   - 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, including the Department of Information Technology Services, 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 CIO 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 CIO shall develop and disseminate an Information Security plan for each Policy, where appropriate, 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 as needed on a periodic basis, but not more than every 3 years;
- 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. 038 and reaffirmed by subsequent mayoral Executive Orders ;
- Utilizing information security standards, frameworks and controls to develop the Program.

2.3 Policy Goals

Metropolitan Government Policies, Procedures and Plans shall be developed to address the following goals:

- Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.

- Inventory and Control of Software Assets
  Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- Data Protection
  Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

- Secure Configuration of Enterprise Assets and Software
  Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

- Account Management
  Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

- Access Control Management
  Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

- Continuous Vulnerability Management
  Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

- Audit Log Management
  Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

- Email and Web Browser Protections
  Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

- Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

- Data Recovery
  Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

- Network Infrastructure Management
  Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

- Network Monitoring and Defense
  Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

- Security Awareness and Skills Training
  Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

- Service Provider Management
  Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

- Application Software Security
  Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

- Incident Response Management
  Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

- Penetration Testing
  Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

3. Review

The CIO 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 originally established in Executive Order No. 038 and reaffirmed by subsequent mayoral Executive Orders will review and recommend to the CIO 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. Roles and Responsibilities

5.1 Metropolitan Government Directors, Heads, Elected Officials and Chairs

Metropolitan Government directors, heads, elected officials and chairs of its departments, agencies, and boards, as business owners, are responsible for information security within their organization, including ensuring the protection of the information and information systems used within their organization. They are responsible for the following activities:

- Acting as Information Owner for all information assets collected, stored or processed by organization and ensuring proper handling of information assets;
- Acting as official with ultimate statutory, management and operational authority over information assets;
- Adhering to the statements set forth in these Policies and ensuring adherence to these Policies within their organization;
- Defining their mission/business processes with consideration for information security;
- Determining information protection needs arising from the defined mission/business processes and revising processes as necessary, until achievable protection needs are obtained;
- Communicating those protection needs to the appropriate providers;
- Identifying and meeting security requirements and ensuring that they are incorporated in business processes;
- Implementing these Policies;
- Establishing additional policies and procedures concerning governance of information assets;
- Leading by example in protecting sensitive information;
- Providing requisite funding, training, and other resources for information security;
- Ensuring that all users, including privileged users, understand their roles and responsibilities and are trained appropriately to meet those responsibilities;
- Ensuring users participate in ecurity awareness program activities, and provide business specific security awareness for all users as applicable;
- Creating an appropriate organizational structure for information security within their organization; and
- Ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.

5.2 Metropolitan Government's Information Technology Departments

All Metropolitan Government's information technology departments are responsible for the following activities:

- Providing oversight and auditing of Metropolitan Government information technology used within the department;
- Developing and implementing operational procedures to ensure compliance with these Policies;
- Managing (i.e., documents, tracks, and reports) the security state of department information systems and the environments in which those systems operate;
- Monitoring compliance of third-party personnel (contractors, vendors, etc.) with applicable security requirements;
- Ensuring compliance with information security requirements;
- Establishing access requirements;
- Addressing operational interests of department’s end users;
- Auditing on a periodic basis, their department for compliance to all policies, procedures, standards, etc. and
- Approving new information technology for implementation and use, ensuring those technologies operate within the appropriately defined security standards.

5.3 Metropolitan Government's Director of Information Technology Services

Metropolitan Government's Director of Information Technology Services is responsible for the following activities:

- Developing, reviewing, and implementing these Policies;
- Developing a process for reviewing all exception requests to these Policies;
- Designating appropriate staff to manage Metropolitan Government’s Information Security Management Program, including a senior information security officer;
- Assessing opportunities for improvement of these Policies;
- Assisting with departmental auditing on a periodic basis for compliance to all policies, procedures, standards, etc. and
- Developing and maintaining a Metro-wide information security program.

5.4 Metropolitan Government's Information Security Steering Committee

The Metropolitan Government's Information Security Steering Committee (ISSC) is responsible for the following activities:

- Reviewing and advising the Director of Information Technology Services on system-wide information security policies, standards and practices for the Metropolitan Government;
- Recommending to the Director of Information Technology Services alterations or changes to the minimum-security requirements for Metropolitan Government departments, agencies and boards;
- Recommending to the Director of Information Technology Services performance measures to determine the effectiveness of Metropolitan Government policies, standards and practices designed to meet or exceed the objectives identified in the *Metropolitan Government Information Security Management* Policy; and
- Reviewing as requested by the Director of Information Technology Services and then recommending to the Director whether the *Metropolitan Government Information Security Management* Policy would be violated by or should be revised for an individual, department or group requesting an Exception.

5.5 Metropolitan Government's User

Metropolitan Government's Users are responsible for the following activities:

- Adhering to the statements set forth in these Policies;
- Understanding their roles and responsibilities in securing Metropolitan Government and meeting those responsibilities;
- Knowing the Classification of the Information of the Metropolitan Government to which they have access, and with which they are permitted to work;
- Understanding the appropriate security controls that should be applied to that Information; and
- Reporting any suspected violations of security policies and procedures or any other information security issue to their supervisor or other appropriate staff.

6 Exception Request

Any individual, department, or group that wishes to diverge or be exempt from any established Policies must request a security exception using the defined security exception request process. The Directors, Agency Heads and Elected Officials of all Metropolitan Government departments, agencies and commissions are responsible for understanding and accepting the risk associated with a security exception request, including the impact that such an exception may have on their department and on Metropolitan Government. All security exception requests shall be submitted for review by the requester to the applicable Director, Agency Head or Elected Official. In addition to exceptions to documented processes, certain service requests may pose a threat or open vulnerabilities in Metropolitan Government's computing environment. When a request of this nature is identified, it is handled in the same manner as an exception to documented processes.

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

SIGNATURE

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

REFERENCES

ISO 27002: sections 5.1.1, 6.1

NIST Special Publications 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*, PM-1, PM-9, PM-11

NIST 800-37 Rev2, *Risk Management Framework for Information Systems and Organizations*

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 addressed in 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
1.2	5/11/2023	• Changes to section 1. Minimum Standards to better reflect operational reality of Metro's information security management program. • Revised review period of all policies: "Is reviewed as needed on a periodic basis, but not more than every 3 years." • Addition of section 5. Roles and Responsibilities. This section was moved from the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies* document as this section is more application to the program as a whole and as recommended by recent assessments. • Modification to Exception Request language to further clarify roles and responsibilities within Metro's ISM program and to eliminate duplication of this section in *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*. • Use throughout of "reaffirmed by subsequent mayoral Executive Orders" so policy does not have to be continually updated with administrative changes. • Removal of mail address to contact the CISO.