METROPOLITAN GOVERNMENT INFORMATION SECURITY MANAGEMENT POLICY

1.0 Definitions of Common Terms

- **Director** – The Director of Information Technology Services.
- **Information Security** – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
  - Confidentiality - Preserving authorized restrictions on access and disclosure including means for protecting personal privacy and proprietary information;
  - Integrity - Guarding against improper information modification or destruction and protecting information nonrepudiation and authenticity; and
  - Availability - Ensuring timely and reliable access to and use of information.
- **Procedures** – The steps that need to be performed to meet standards and comply with this Policy. There are typically many procedures in place to maintain compliance.
- **Standards** – The Metropolitan Government of Nashville and Davidson County's ("Metropolitan Government") minimum requirements for users to assure compliance with this Policy.
- **Systems -** Metropolitan Government information systems.

2.0 Purpose

The purpose of this Information Security Management Policy ("Policy") is to provide consistent direction and support for Information Security.

3.0 Scope

This Policy shall apply to all Metropolitan Government employees and third party users except: employees and users of the Nashville Electric Service, the Metropolitan Nashville Airport Authority, the Metropolitan Hospital Authority, and the Metropolitan Development and Housing Agency. However, these agencies are requested to consider adopting these or similar policies.

4.0 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, therefore, 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.

The 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 may adopt Information Security requirements that afford greater protections.

5.0 Security Policies and Procedures, Plan, and Priorities

5.1 Policies and Procedures

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

a. Policies that address the purpose, scope, roles, responsibilities, management commitment, compliance, and coordination among the Metropolitan Government departments, agencies, and boards for:

i. **Access Control** - limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) acting on behalf of authorized users, and to the types of transactions and functions that authorized users are permitted to exercise.

ii. **Awareness and Training** - (a) teaches managers and users of Systems awareness of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of the Systems; and (b) assures that Metropolitan Government personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

iii. **Audit and Accountability** - (a) creates, protects and retains information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (b) traces the actions of individual information system users so they can be held accountable for their actions.

iv. **Certification, Accreditation, and Security Assessments** - (a) periodically assesses the security controls in Systems to determine if the controls are effective in their application; (b) develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in Systems; (c) authorizes the operation of Systems and any associated information system connections; and (d) monitors information system security controls on an ongoing basis for continued effectiveness of the controls.

v. **Configuration Management -** (a) establishes and maintains baseline configurations and inventories of Systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (b) establishes and enforces necessary security configuration settings for information technology products employed in information systems.

vi. **Contingency Planning -** establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for information systems and creates the availability of critical information resources and continuity of operations in emergency situations.

vii. **Identification and Authentication -** developing prerequisites to allowing access to Systems by information system users, processes acting on behalf of users, or devices acting on behalf of users, and authentication (or verification) of the identities of those users, processes, or devices.

viii. **Incident Response** - (a) establishes incident handling capability for Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (b) that tracks, documents, and reports incidents to Metropolitan Government officials and/or authorities.

ix. **Maintenance** - (a) performs periodic and timely maintenance on Systems; and (b) provides effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

x. **Media Protection** - (a) protects information system media, both paper and digital; (b) limits access to information on information system media to authorized users; and (c) sanitizes or destroys information system media before disposal or release for reuse.

xi. **Physical and Environmental Protection -** (a) limits physical access to information systems, equipment, and the respective operating environments to authorized individuals; (b) protects the physical plant and support infrastructure for information systems; (c) provides supporting utilities for information systems; (d) protects information systems against environmental hazards; and (e) provides environmental controls in facilities containing information systems.

xii. **Planning** - develops, documents, periodically updates, and implements security plans for Systems that describe the security controls in place or plans for the information systems and the rules of behavior for individuals accessing the information systems.

xiii. **Personnel Security -** (a) requires that individuals occupying positions of responsibility within the Metropolitan Government (and third-party service providers) meet established security criteria for those positions; (b) maintains Metropolitan Government information and information systems protections during and after personnel actions such as terminations and transfers; and (c) employs sanctions for personnel failing to comply with Metropolitan Government security policies and procedures.

xiv. **Risk Assessment** - periodic assessments of risk to Metropolitan Government operations (including mission, functions, image, or reputation), its assets, and individuals, resulting from the operation of its information systems and the associated processing, storage, or transmission of its information.

xv. **System and Services Acquisition -** (a) allocates sufficient resources to adequately protect Systems; (b) employs system development life cycle processes that incorporate information security considerations; (c) employs software usage and installation restrictions; and (d) requires that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from Metropolitan Government.

xvi. **System and Communications Protection -** (a) monitors, controls, and protects Metropolitan Government communications (i.e., information transmitted or received by Systems) at the external boundaries and key internal boundaries of the information systems; and (b) employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within its information systems.

xvii. **System and Information Integrity -** (a) identifies, reports, and corrects information and information system flaws in a timely manner; (b) provides protection from malicious code at select locations within its information systems; and (c) monitors information system security alerts and advisories and takes actions in response.

b. Procedures to facilitate the implementation of those policies and associated controls.

c. The Director shall also develop, disseminate, review, and update the foregoing policies and procedures consistent with the ISO/IEC 27002 Code of Practice for Information Security Management objectives and controls relating to:

(1) security policy;
(2) organizing information security,
(3) asset management;
(4) human resources security;
(5) physical and environmental security;
(6) communications and operations management;
(7) access control;
(8) information systems acquisition, development and maintenance;
(9) information security incident management;
(10) business continuity management; and
(11) compliance.

5.2 Plan

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

- Provides an overview of the requirements for the Program and a description of the Program management controls and common controls in place or planned for meeting those requirements;

- Provides sufficient information about management controls and common controls to enable an implementation that is unambiguously compliant with the intent of this Policy 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;

In addition, the Director shall review the plan, at least annually, and shall revise the plan to address organizational changes and problems identified during plan implementation or security control assessments.

5.3 Priorities

The Metropolitan Government priorities for Information Security are:

- Complying with applicable federal and state information privacy and security laws, regulations and contractual requirements such as the Health Insurance Portability and Accountability Act, the Red Flags Rule under the Fair and Accurate Credit Transactions Act, the Payment Card Industry Data Security Standard, and the Tennessee Identity Theft Deterrence Act of 1999;

- Developing an Information Security awareness training program for Metropolitan Government employees and third party users as required by Executive Order No. 005;

- Training Metropolitan Government employees and third party users to understand the consequences of security violations and that security violations are subject to discipline, up to and including termination of employment and/or termination of contract, as applicable;

- Utilizing standards, frameworks and controls such as the ISO/IEC 27000 Information Security series, the National Institute of Standards and Technology ("NIST") Federal Information Processing Standards, and NIST Guidelines and the Payment Card Industry Data Security Standard.

6.0 Review

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

7.0 Oversight

An Information Security Steering Committee (the "Steering Committee"), as established in Executive Order No. 038 will review and recommend to the Director changes to the system-wide information security policies, standards, and practices for the Metropolitan Government. The Steering Committee will also develop performance measures to determine the effectiveness of the Program.

8.0 Exception Request

Any individual, department, or group that wishes to diverge or be exempt from this Policy must request an exception from the Director.

9.0 Revision History