METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY POLICY

SUBJECT:	DISTRIBUTION DATE:
METROPOLITAN GOVERNMENT SCOPE, BACKGROUND, AND GOVERNANCE STATEMENTS FOR INFORMATION SECURITY POLICIES	5/3/2011
	EFFECTIVE DATE: IMMEDIATELY
ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED

PURPOSE

Metropolitan Government implemented an Information Security Management program per Mayor Karl Dean Executive Order No. 038 and was reaffirmed by Mayor Megan Barry Executive Order No. 034. A core component of this program is a set of information security policies based on international standards. This document provides the scope, background, and governance information common to all of Metropolitan Government's information security policies. For brevity and clarity, instead of restating this information in every policy, it is referenced; therefore, this information is considered a part of each and every Metropolitan Government information security policy unless specifically noted otherwise.

SCOPE

All Metropolitan Government developed information security policies shall apply to all Metropolitan Government departments, agencies and boards except: "the Nashville Electric Service, the Metropolitan Nashville Airport Authority, the Metropolitan Hospital Authority, and the Metropolitan Development and Housing Agency," as specified in *the Metropolitan Government Information Security Management Policy*. FAILURE TO ADHERE TO THIS POLICY MAY RESULT IN DISCIPLINARY ACTION, UP TO AND INCLUDING TERMINATION AND, WHERE APPLICABLE, CAN RESULT IN CIVIL DAMAGES AND CRIMINAL PENALTIES, INCLUDING FINES AND IMPRISONMENT, AS WELL AS METROPOLITAN GOVERNMENT'S ATTORNEYS' FEES AND COSTS. IN ADDITION, METROPOLITAN GOVERNMENT SHALL BE ENTITLED TO SEEK INJUNCTIVE RELIEF IN ORDER TO PREVENT BREACHES OR THREATENED BREACHES OF THIS POLICY. All developed policies and accompanying procedures shall be consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance. These policies supersede all previous Metropolitan Government IT related policies written or communicated, where applicable, and are not intended to be nor should be construed as an employment contract. These policies may be amended or revised at any time by Metropolitan Government. These policies shall not supersede departmental, agency or board policies that address areas defined in these policies as long as the requirements of the departmental, agency or board policies equals or exceeds the minimum requirements set forth.

All developed policies and accompanying procedures shall be reviewed as needed. Any set review periods shall be defined within the implementation plans of the policy.

BACKGROUND

Maintaining the confidentiality, integrity and availability of information (including Sensitive Information), information technology, information systems and critical operational processes in a manner consistent with and meeting the Metropolitan Government legal, regulatory and ethical responsibilities on behalf of its citizens is of paramount importance to Metropolitan Government. Each asset is classified in terms of its value, legal requirements, sensitivity, and criticality to Metropolitan Government. Standards are designed to minimize the potential exposure of Metropolitan Government to damage that may result from unauthorized access, use or disclosure of information (including Sensitive Information), information technology, information systems and critical operational processes.

These policies specify minimum security requirements for Metropolitan Government information (including Sensitive Information), information technology, information systems and critical operational processes. Metropolitan Government departments, agencies and boards must meet the minimum security requirements as defined herein through the adoption of system-wide information security policies, standards and practices as recommended to the Director of Information Technology Services by the Metropolitan Government Information Security Steering Committee (the "Steering Committee") as established in Mayor Karl Dean Executive Order No. 038 and reaffirmed by Mayor Megan Barry Executive Order No. 034. Since such policies, standards and practices are the minimum requirements to be adopted by Metropolitan Government for information security management they are a floor, not a ceiling. Each department, agency and board may adopt security requirements that afford greater protections than those contained in this Policy.

GOVERNANCE

1. Oversight

   These policies are adopted pursuant to the recommendation of the Steering Committee to the Director of Information Technology Services. The Steering Committee consists of seven (7) permanent voting members and four (4) revolving voting members. The seven (7) voting members of the Steering Committee are the following officials of the Metropolitan Government:

   - The Director of Information Technology Services
   - The Chief of Police
   - The Sheriff
   - The Director of Justice Integration Services
   - The Director of Law
   - The Director of Finance
   - The Director of Schools

   The four (4) revolving members of the Steering Committee are officials of Metropolitan Government selected by the Mayor for 2-year terms.

2. Roles and Responsibilities

2.1. Metropolitan Government Directors, Heads and Chairs

Metropolitan Government directors, heads 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, strored or processed by organization and ensures proper handling of information assets;
- Acting as official with ultimate statuatory, 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;
- Providing a security awareness program for all users for any issues applicable to their organization;
- 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.

2.2. 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;
- Manages (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 requirments;
- Ensuring compliance with information security requirements;
- Establishes access requirements;

- Addresses 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.

2.3. 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.

2.4. Metropolitan Government's Information Security Steering Committee

Metropolitan Government's Steering Committee 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 him or her 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.

2.5. 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.

EXCEPTION REQUESTS

As stated in *the Metropolitan Government Information Security Management Policy*, any individual, department, agency or board that wishes to diverge or be exempt from any of these policies must request an exception from the Director of Information Technology Services. 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.

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

Karl Dean Executive Order No. 38
Megan Barry Executive Order No. 34
NIST Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, section PM1 – 11, PS-7

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	5/3/2011	First released version
1.1	12/29/2016	Changes to references to reflect new administration Changs to address auditing responsibilities Changes to align business owner responsibilities with current standards