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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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

The Metropolitan Government of Nashville and Davidson County ("Metropolitan Government") implemented an Information Security Management program per Mayor Karl Dean Executive Order No. 038 andreaffirmed by subsequent mayoral Executive Orders. 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,".. 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 subsequent mayoral Executive Orders. 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

The roles and responsibilities of the following groups with regards to the information security management program are defined in the *Metropolitan Government Information Security Management* policy:

- Metropolitan Government Directors, Heads and Chairs
- Metropolitan Government's Information Technology Departments
- Metropolitan Government's Director of Information Technology Services
- Metropolitan Government's Information Security Steering Committee
- Metropolitan Government's Users

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

Freddie O'Connell Executive Order No. 37
Karl Dean Executive Order No. 38
Megan Barry Executive Order No. 34
NIST Special Publication 800-53 rev. 5. *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
1.2	5/10/2023	• Migrated roles and responsibilities to *Metropolitan Government Information Security Management* • Removal of Exception Request language to eliminate duplication of this section in the *Metro Information Security Management* policy. • Changes to reference "subsequent mayoral executive orders" so as to not have to continually revise the document.

		• Removal of mail address to contact the CISO.
1.3	8/29/2025	Changes to references to reflect new administration Change to reflect use of rev 5 of NIST 800-53 as a reference