| METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY<br>**INFORMATION SECURITY POLICY** | POLICY NUMBER:<br>ISM 7 |
|---|---|
| SUBJECT:<br>INFORMATION CLASSIFICATION | DISTRIBUTION DATE:<br>5/3/2011 |
| | EFFECTIVE DATE:<br>11/1/2011 |
| ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County | EXPIRATION: UNTIL RESCINDED |

**PURPOSE**

The purpose of this policy is to ensure that the Information of the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) receives an appropriate level of protection.[1]

**POLICY**

1. Generally
   Metropolitan Government shall classify Information of the Metropolitan Government in terms of their value, legal requirements, sensitivity, and criticality to the business and operations of the government and those it serves or as specified by any superseding state or federal law or regulation. Such legal requirements shall include applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance. This policy and accompanying procedures shall be reviewed/updated at least annually.

2. Information Classifications
   The following classifications shall be used by Metropolitan Government to assign potential risk and to provide guidelines for Information of the Metropolitan Government:

| | |
|---|---|
| Public Information (no risk) | Public Information is Information of the Metropolitan Government that Metropolitan Government must provide for access to Tennessee residents. Public Information is shared publicly to facilitate Metropolitan Government operations. *Examples of public Information include Information provided on the Metropolitan Government Web site and reports meant for public distribution.* |
| Internal Information (lowest risk) | Internal Information is non-sensitive Information of the Metropolitan Government that is used in daily business operations. If internal Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, little or no loss would be incurred. *Examples of internal Information include staff phone numbers building address.* |

[1]In addition to this policy, care should be taken to ensure compliance with other applicable federal, state and local laws and authorities including but not limited to Title 2, Chapter 140 of the Metropolitan Code of Laws, Karl Dean Executive Order No. 35, and the Tennessee Public Records Act, T.C.A. § 10-7-503.

| | |
|---|---|
| Confidential Information (high risk) | Confidential Information is sensitive Information of the Metropolitan Government. If confidential Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, considerable loss could occur. *Examples of confidential Information include social security numbers and credit card Information.* |
| Restricted Information (highest risk) | Restricted Information is highly sensitive Information of the Metropolitan Government. If restricted Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, significant loss including loss of life could occur. *Examples of such Information are witness protection Information and Information related to critical infrastructure by the U.S. Department of Homeland Security.* |

All Information of the Metropolitan Government regardless of physical form or characteristics shall be assigned a classification by the Information Owners in accordance with the requirements set forth within this section in order to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification, or destruction.

Metropolitan Government shall comply with the Tennessee Public Records Act (the "TPRA") default presumption that all Metropolitan Government records are available for inspection and copying unless they are protected by a specific exception under the TRPA. Any Metropolitan Government department, agency or entity that disseminates Information in response to a TPRA request shall ensure that the appropriate classification is applied when that Information is released from their department.

When Information of the Metropolitan Government with multiple classifications is stored, transmitted, or destroyed together, Information handling requirements for the higher classification shall apply.

3. Labeling and Handling

Metropolitan Government Information Owners shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification of information.

Metropolitan Government's information labeling and handling is supported through the use of controls set forth in: Access, (Section 3.1 below), *Labeling* (Section 3.2 below) and *Security and Handling Descriptions* (Section 3.3 below).

3.1 Access

Metropolitan Government shall restrict access to all forms of media containing Information of the Metropolitan Government to only those authorized. Access shall be controlled using appropriate security measures (password protected, key lock, etc.) based on the characteristics of the information, including, but not limited to, the classification of the information.

The information shall be encrypted as part of the handling process if required by the classification of the information, as directed by the Information Owner or designee or as required by applicable statutes and regulations.

3.2 Labeling

Metropolitan Government shall label removable media (i.e. electronic, magnetic, optical, and paper) indicating:

- if it contains Sensitve Information;
- the distribution limitations of the information;
- any other applicable security and handling descriptions (see Section 3.3 below).

Removable media containing Sensitive Information may be exempted from labeling as long as the media remains in a defined Secure Area.

Classification of Information Assets, including workstations and servers, shall be based on the highest classification of the Information stored on the asset and secured appropriately.

3.3 Security and Handling Descriptions

3.3.1 Metropolitan Government shall support and use descriptions and other representations of information classification. These include tags in metadata, watermarks, footers, headers, etc. Descriptions and other representations should be clearly displayed where appropriate.

3.3.2 Established security shall be maintained when information is exchanged between and/or within information systems or additional parties, including hosting providers.

## 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

## SIGNATURE

_____

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

## REFERENCES

ISO 27002: sections 7.2, 7.2.1, 14.1.2, 7.2.2, 9
NIST Special Publication 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*: RA-2, CC-9, AC-16, MP-2, MP-3, SC-16
Tennessee Public Records Act, T.C.A. § 10-7-503

Tennessee Code Annotated 10-7-101 et seq.
Criminal Justice Information Services Security Policy version 6.0
Center for Internet Security Critical Security Controls v 6.0, 10.1, 13.1, 13.2, 13.3, 13.4, 14.2 14.5
NIST Cyber Security Framework version 2, ID.AM-4, PR.AC-4, PR.PT-2
NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

## REVISION HISTORY

| REVISION | APPROVAL DATE | CHANGES |
|---|---|---|
| 1.00 | 11/19/2010 | ISSC recommended |
| 1.01 | 3/8/2011 | Transferred to new template |
| 1.1 | 7/2/2015 | 2.Information Classifications<br>Example of "Internal Information (lowest risk) was changed from ". . . and upcoming vaction time" to "building address."<br><br>2.Information Classifications: Additional statement added to be called out specifically given the previous statement referencing the TRPA. Added statement:<br><br>"Any Metropolitan Government department, agency or entity that disseminates Information in response to a TPRA request shall ensure that the appropriate classification is applied when that Information is released from their department."<br><br>Changed policy number to meet new standard.<br><br>Some formatting adjustments. |
| 1.2 | | Addition of headings 3 to capture labeling and handling requirements.<br>Added review of applicable NIST CSF.<br>Added review of applicable CSCs.<br>Added review of applicable Criminal Justice Information Services Security Policy |
| 1.3 | 8/29/2025 | Change to reflect use of rev 5 of NIST 800-53 as a reference<br>Change to reflect use of rev 2 of NIST Cybersecurity Framework<br>Change to reflect use of version 6 of CJIS as a reference<br>Change to reflect use of NIST 800-171 r3 as a reference |