METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 7.2.2
SUBJECT: INFORMATION LABELING AND HANDLING POLICY	DISTRIBUTION DATE: 3/1/2012
	EFFECTIVE DATE: 9/1/2012
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 help ensure that the Information of the Metropolitan Government receives an appropriate level of protection.

POLICY

1. Generally

   Metropolitan Government shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification of information as defined in the Metropolitan Government *7.2.1 Information Classification Policy*.

   As set forth below, Metropolitan Government's information labeling and handling is supported through the use of controls set forth in: (i) Media (Section 2 below) and (ii) Security and Handling Descriptions (Section 3 below).

2. Media

   2.1. Media 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 labeling and handling process if required by the classification of the information as defined by the Metropolitan Government *7.2.1 Information Classification Policy* or as directed by the Information Owner or designee.

2.2. Media Labeling

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

- if it contains Confidential and/or Restricted Information;
- the distribution limitations of the information;
- handling caveats; and
- any other applicable security and handling descriptions (see Section 3 below).

Removable media containing Confidential and/or Restricted Information may be exempted from labeling as long as the media remains in a defined Secure Area as described in the Metropolitan Government *9.1 Secure Areas Policy*.

3. Security and Handling Descriptions

3.1. Metropolitan Government shall support and use descriptions and other representations of information security risk potential. The description shall include the classification of the information as defined by the Metropolitan Government *7.2.1 Information Classification Policy*.

3.2. Established security shall be maintained when information is exchanged between and / or within information systems.

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 7.2.1, 7.2.2, 9
- NIST Special Publication 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*: AC-16, MP-2, MP-3, SC-16
- Metropolitan Government Information Security Policies *7.2.1 Information Classification* and *9.1 Secure Areas*

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	3/1/2012	First released version