METROPOLITAN GOVERNMENT # INFORMATION SECURITY POLICY	NUMBER: ISM 17
SUBJECT: # CRYPTOGRAPHIC CONTROLS	DATE EFFECTIVE: 08/1/2011
	EFFECTIVE DATE: 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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 Metropolitan Government of Nashville and Davidson County (Metropolitan Government) protects the confidentiality, authenticity or integrity of information by cryptographic means.

POLICY

1. Generally
   Metropolitan Government shall encrypt sensitive information by use of: (i) valid encryption processes for data at rest and (ii) valid encryption processes for data in motion, additionally, Metropolitan Government will support its use of cryptographic techniques by putting in place key management. Metropolitan Government shall review and update this policy and accompanying procedures at a defined interval. Metropolitan Government's cryptographic controls usage is supported through the use of the following controls: (i) cryptographic module authentication (see Section 2 below); (ii) transmission integrity (see Section 3 below); (iii) transmission confidentiality (see Section 4 below); (iv) use of cryptography (see Section 5 below); (v) cryptographic key establishment and management (see Section 6 below); and (vi) public key infrastructure certificates (see Section 7 below).

2. Cryptographic Module Authentication
   The Metropolitan Government information system shall use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use by Metropolitan Government will be compared to the list of NIST validated cryptographic modules annually to ensure compliance.

3. Transmission Integrity
   The Metropolitan Government information system shall protect the integrity of transmitted information traveling across both internal and external communications. This control applies to communications across internal and external networks.

4. Transmission Confidentiality

The Metropolitan Government information system shall protect the confidentiality of transmitted information. Metropolitan Government shall employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

5. Use of Cryptography
   The Metropolitan Government information system shall implement required cryptographic protections using cryptographic modules that comply with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance.

6. Cryptographic Key Establishment and Management
   Metropolitan Government shall establish and manage cryptographic keys for required cryptography employed within its information system. Cryptographic key management and establishment shall be performed using automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, cryptographic key management shall provide protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

7. Public Key Infrastructure Certificates
   Metropolitan Government shall issue public key certificates under an appropriate certificate policy or obtain public key certificates under an appropriate certificate policy from an approved service provider. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

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 to ciso@nashville.gov.

SIGNATURE

_____

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

REFERENCES

ISO 27002: sections 6.1.5, 6.2.1, 6.2.3, 8.1.1, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 12.5.5, 12.3.2
NIST Special Publications 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*: SC-9, CC-4, CC-14, CC-15, IA-7, SC-8, SC-12, SC-13, SC-17
NIST Special Publications 800-111, *Guide to Storage Encryption Technologies for End User Devices*
Federal Information Processing Standards (FIPS) 140-2
NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
NIST Special Publications 800-77, *Guide to IPsec VPNs*
NIST Special Publications 800-113, *Guide to SSL VPNs*
CIS Critical Security Controls 3, 10, 13, 15, 16, 18

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	8/1/2011	First released version
1.1	8/15/2018	Change review time from quarterly to annual. Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against. Adding review of Center for Internet Security Critical Security Controls. Modified number to reflect new numbering convention.