METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 2
SUBJECT: HUMAN RESOURCES SECURITY POLICY	DISTRIBUTION DATE: 11/1/2013
	EFFECTIVE DATE: 11/1/2013
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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) and its employees, contractors and third party users:

- understand their responsibilities and are suitable for their Roles, in order to reduce the risk of theft, fraud or misuse of Information and Information Technology Assets;
- are aware of Information Security threats and concerns and liabilities and are equipped to support Information Security in the course of their normal work in order to reduce the Risk of human error; and
- understand their responsibilities so that employees, contractors, and third party users may exit the Metropolitan Government or change employment in an orderly manner.

POLICY

1. Generally

Metropolitan Government shall:

1.1. define and document security Roles and responsibilities of employees, contractors and third-party Users;
1.2. require employees, contractors, and third party Users to apply security in accordance with Metropolitan Government policies and procedures;
1.3. define and assign responsibilities for performing employment termination or change of assignment or duties to include removing access rights to Information and Information Technology Assets;
1.4. ensure individuals requiring access to Metropolitan Government information and information systems sign appropriate confidentiality and/or non-disclosure agreements prior to being granted access; and
1.5. review and update confidentiality and/or non-disclosure agreements annually.

Metropolitan Government shall require that employees, contractors and third-party Users:

1.6. agree and sign the terms and conditions of access and responsibilities regarding Information and Information Technology Assets during their employment or other applicable contract, which should state their and Metropolitan Government's responsibilities for Information Security;

1.7. apply security in accordance with Metropolitan Government's policies and procedures; and
1.8. return all Metropolitan Government Information and Information Technology Assets in their possession upon termination of their employment, contract, or agreement.

2. Prior to and During Employment

2.1. Roles and Responsibilities

Metropolitan Government shall review, update and disseminate this and other Information Security Policies and accompanying procedures as well as the Roles and responsibilities of its employees, contractors and third-party users in order to keep them relevant with other Information privacy and security laws, regulations and guidelines.

As Metropolitan Government defines Roles and responsibilities for employees, contractors and third party users, it shall:

- assign a Risk designation to all positions based on classification of the applicable Information;
- review and revise position Risk designations as needed;
- consider different sets of access rules based on User Roles and responsibilities;
- take into account Separation of Duties and Least Privilege; and
- define and document oversight and User Roles and responsibilities with regard to external Information System services.

For all Users, including third party users, Metropolitan Government shall:

- establish and make readily available to all Information System Users the rules that describe their responsibilities and expected behavior with regard to Information of the Metropolitan Government, Information Technology Assets and Information System usage;
- receive acknowledgment of access agreement from Users before authorizing access to Information and Information Technology Assets; and
- provide users accessing information systems a system use notification message or banner delineating required privacy and security notices.

Employees who commit a security breach or through actions cause a breach to occur can be subject to disciplinary action up to and including termination of employment.

2.2. Personnel Screening

Metropolitan Government shall screen or rescreen all individuals as required when any new role and responsibility is assigned and prior to authorizing access to Information and Information Technology Assets.

Screening and rescreening shall be consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The screening criteria shall

include explicit information security role appointment requirements (e.g., training, security clearance). Metropolitan Government shall define different rescreening conditions and frequencies for personnel accessing Information and Information Technology Assets based on the type of information processed, stored or transmitted.

2.3. Security Awareness and Training

Metropolitan Government shall provide basic security awareness training to all information system users (including department, agency and board directors, heads and chairs, and contractors) as part of initial training for new users, and as required by system changes. As all employees have responsibility for some degree of physical security, information security, and information technology security, all employees and third party contractors are required to complete this basic security awareness training upon initial employment and maintain that training periodically.

As part of its security awareness program, Metropolitan Government shall:

- include practical exercises in security awareness training that simulate actual cyber-attacks; and
- address awareness of the need for operations security as it relates to Metropolitan Government's information security program

Metropolitan Government shall provide Role-based security-related training:

- before authorizing access to the Information of the Metropolitan Government and/or Information Technology Assets;
- before performing assigned duties;
- whenever there are significant changes to the Information System or environment of operation (including identification of new threats and vulnerabilities;
- when any other conditions occur that may impact the security state; and
- as required by applicable regulations.

Metropolitan Government shall determine the appropriate content of security training based on assigned Roles and responsibilities based on the Information of the Metropolitan Government and Information Technology Assets to which personnel have authorized access.

Adequate security-related technical training shall be provided to Information System managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software to perform their assigned duties.

Metropolitan Government security training shall address management, operational and technical responsibilities covering physical, personnel and technical safeguards and countermeasures. It shall also provide the guidance necessary to carry out responsibilities related to operations security within the context of Metropolitan Government's Information Security program, including contingency planning and incident response.

2.4. Security Training Records

Metropolitan Government shall:

- document and monitor security training activities, including basic security awareness training and specific Information System security training;
- retain training records for employees as a part of their personnel record;
- retain training records for contracted vendors for the duration of the working relationship with Metro plus five years.

2.5. Incident Response Training

Metropolitan Government shall train personnel in incident response roles and responsibilities with respect to the Information of the Metropolitan Government and Information Technology.

3. Termination or Change of Employment

3.1. Personnel Termination

Metropolitan Government, upon termination of individual employment, contract or use of Information or Information Technology Assets by third parties, shall:

- terminate information system access;
- meet with employee, contractor, or third party User's manager to determine assets and information technology access to be addressed at termination;
- retrieve all security-related Metropolitan Government information system-related property; and
- retain access to its Information and Information Technology Assets formerly controlled by the terminated individual.

3.2. Personnel Transfer

Metropolitan Government shall review logical and physical access authorizations to Information, Information Technology Assets and facilities, including responsibilities contained within any confidentiality agreement, when personnel are reassigned or transferred to other Metropolitan Government positions or change in assignment of duties. This requirement shall apply when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted.

3.3. Access Rights

Metropolitan Government shall manage access rights when there is termination, change of employment, or change in assignment of duties including, as applicable.

4. External Information System Services

   Metropolitan Government shall, among other things, require that providers of external information system services comply with Metropolitan Government information security requirements and employ appropriate security controls, including required confidentiality and/or non-disclosure agreements for service providers, their employees and contractors, in accordance with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards and guidance.

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 6.1.5, 8.1, 8.2, 8.3
- NIST Special Publications 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*: XX-1 controls, AC-2, AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, IR-2, PL-4, PL-6, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-9

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	11/1/2011	First released version
1.1	11/1/2013	Merged Confidentiality Agreements Policy 6.1.5 with this policy. Rescinded Confidentiality Agreements Policy 6.1.5 and Human Resources Security Policy.