METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 5
SUBJECT: INFORMATION SECURITY INCIDENT MANAGEMENT POLICY	DISTRIBUTION DATE: 4/1/2014
	EFFECTIVE DATE: 4/1/2014
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 security events, weaknesses, and incidents associated with Information Systems are managed in a consistent, effective, and timely manner, to include evaluation and improvement of information security procedures, processes, and controls based on lessons learned.

POLICY

Metropolitan Government shall promptly address Information Security Incidents with consistent and effective management. Such response shall include the Business Owner and the Information Owner and be coordinated by the Chief Information Officer/Director of Information Technology Services. Other personnel may be required based on the type and severity of the incident.

1. Reporting Information Security Events, Information Security Vulnerabilities, and Information Security Incidents

Metropolitan Government Users shall expeditiously report to the Information Technology Services Department (ITS) any observed or suspected Information Security Events , Information Security Vulnerabilities, and Information Security Incidents, including any loss and/or theft of Information Technology Assets.

Metropolitan Government shall report any observed or suspected Information Security Events and Incidents to law enforcement or other regulating agencies if laws are suspected to have been broken.

Information Security Events, Vulnerabilites and Incidents, including incident reponse plans shall be classified as Confidential. Metropolitan Government shall protect incident response plans from unauthorized disclosure and modification.

2. Management of Information Security Incidents

Metropolitan Government shall:

2.1. Develop an Information Security Incident Management response process that:
- 2.1.1. Maintains appropriate contacts with law enforcement or other regulating agencies;
- 2.1.2. Describes a roadmap for Information Security Incident response;

2.1.3. Defines the structure and organization of personnel involved in the Information Security Incident response to include both overall Metropolitan Government and specific departmental responses;
2.1.4. Outlines the high-level approach for how the Information Security Incident response relates to organizational needs and processes to include business continuity and disaster recovery processes;
2.1.5. Meets the unique requirements of Metropolitan Government, which relate to mission, size, structure, and functions;
2.1.6. Provides metrics for the Metropolitan Government Information Security Incident response effectiveness;
2.1.7. Describes evidence retention procedures;

2.1.8. Defines the resources and management support needed to effectively develop and maintain an Information Security Incident response capability; and
2.1.9. Is reviewed and approved as set forth in this Policy.

2.2. Distribute copies of its Information Security Incident Management Plan to all Metropolitan Government departments, agencies and boards; and
2.3. Review its Information Security Incident Management Plan annually and communicate changes to all Metropolitan Government departments, agencies and boards.

3. Prioritization or Severity Ratings of Incidents

Metropolitan Government shall establish thresholds for determining when an incident is triggered.

Metropolitan Government shall prioritize incidents based on two factors:
3.1. Current and potential impact of the incident; and
3.2. Criticality of affected or potentially affected resources.

4. Information Security Incident Handling

4.1. Metropolitan Government shall quantify and monitor Information Security Incidents based on:
4.1.1. Classification of the Information Security Incident within defined categories;
4.1.2. The impact of the Information Security Incident; and
4.1.3. The cost of the Information Security Incident.

4.2. Metropolitan Government shall:
4.2.1. Coordinate Information Security Incident handling activities with contingency planning activities;
4.2.2. Include roles and responsibilities in response plans;
4.2.3. Categorize incidents consistent with response plans;
4.2.4. Focus on containment and mitigation of incident;
4.2.5. Incorporate lessons learned from ongoing Information Security Incident handling activities into Information Security Incident response procedures and training; and
4.2.6. Implement the resulting changes accordingly.

5. Incident Response Training

Metropolitan Government shall provide training to personnel in their Information Security Incident response roles and responsibilities as needed.

6. Loss or Theft

Metropolitan Government Users shall be required to immediately report the loss or theft of Information Technology Assets.

7. Breach Notification

Metropolitan Government shall comply with all applicable federal and state security breach notification laws and regulations, including all requirements to provide notification of an Information Security Breach.

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: section13, 6.1.6
- NIST Special Publication 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*: AU-6, AU-9, IR-1-8, PL-4, SI-2, SI-4, SI-5, CP-2
- NIST Special Publication 800-61 Rev2, *Computer Incident Handling Guide*
- NIST Cybersecurity Framework: PR.IP-9, DE.AE-5, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2
- Criminal Justice Information Security Policy v5.6, Policy Area 3
- Center for Internet Security Critical Security Control 19

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	5/1/2012	First released version
2.0	3/31/2014	Updated to include additional ISO 6.1.6 control
2.1	6/27/2016	Section 1. Change "Weaknesses" to "Vulnerabilities" to better align with standard terminology. Addition of the following to clarify the classification of all incident response documents to meet NIST 800-53 IR-8. *Information Security Events, Vulnerabilities and Incidents, including incident response plans shall be classified as Confidential. Metropolitan Government shall protects incident response plans from unauthorized disclosure and modification.* Section 2. Remove "and Information Security Improvements" from heading as this policy only addresses incident handling. Under Section 3., add the following to meet NIST Cyber Security Framework DE.AE-5 *Metropolitan Government shall establish thresholds for determining when an incident is triggered* Under Section 4., add the following to meet NIST Cyber Security Framework RS.AN-4, RS.MI-1 and RS.MI-2 *4.2.2. Categorize incidents consistent with response plans;* *4.2.3 Focus on containment and mitigation of incident* Under "References" add the applicable NIST Cyber Security Framework sections and the newest revision of NIST SP 800-53
2.2	10/26/2018	• Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against. •Added 2.1.7 and 4.2.2 to address Information Security Incident Management gap assessment findings •Added review of applicable CSCs. •Added review of applicable Criminal Justice Information Services Security Policy