METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 15
SUBJECT: AUDIT, MONITORING AND LOGGING	DISTRIBUTION DATE: 3/2/2018
	EFFECTIVE DATE: 3/15/2018
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OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED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 the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) provide accurate and comprehensive audit logs in order to detect and react to inappropriate and unauthorized activities. This document addresses the creation, protection, and retention of Information System audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity within the Information and how the actions of individual Information System users can be uniquely traced to those users so they can be held accountable for their actions. The level of logging, auditing and monitoring shall be commiserate to the security required for the Information System.

POLICY

1.0 Generally

Metropolitan Government shall, where applicable:

1.1. Assess the Information System and determine the appropriate level of logging, auditing and monitoring that shall be in place, as commiserate to the classification of the data collected, stored or processed, to the criticality of the service provided by the Information System and to meet any regulatory or legal requirements;

1.2. Produce audit logs recording user activities, exceptions and information security events and keep them for an agreed period to assist in future investigations and access control monitoring;

1.3. Establish procedures for monitoring use of information processing facilities and regularly review results of the monitoring activities;

1.4. Protect logging solutions and log information against tampering and unauthorized access;

1.5. Log system administrator and system operator activities;

1.6. Log, analyze and take appropriate action regarding faults; and

1.7. Synchronize the clocks of all relevant systems within Metropolitan Government with an agreed upon accurate time source.

As set forth below, Metropolitan Government shall detect unauthorized information processing activities through the use of the controls set forth in: (i) security auditable events (see Section 2.0 below); (ii) content of audit records (see Section 3.0 below); (iii) audit generation (see Section 4.0 below); (iv) audit storage capacity (see Section 5.0 below); (v) response to audit failures (see Section 6.0 below); (vi) audit review, analysis and reporting (see Section 7.0 below); (vii) audit reduction and

report generation (see Section 8.0 below); (viii) time stamps (see Section 9.0 below); (ix) audit record retention (see Section 10.0 below); (x) protection of audit information (see Section 11.0 below); (xi) non-repudiation (see Section 12.0); (xii) monitor for information disclosure (see Section 13.0 below); (xiii) session audit (see Section 14.0 below); (xiv) Information System monitoring (see Section 15.0 below); and (xv) flaw remediation (see Section 16.0 below).

2.0 Security Auditable Events

Metropolitan Government shall:

2.1. Determine, based on a risk assessment and mission/business needs, that the Information System must be capable of auditing the appropriate events as deemed necessary;

2.2. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

2.3. Determine, based on current threat information and ongoing assessment of risk, that the appropriate events are to be audited within the Information System;

2.4. Review and update the list of auditable events on a periodic basis or as required by changes to the Information System; and

2.5. Include execution of privileged functions in the list of events to be audited by its Information System.

3.0 Content of Audit Records

The Information System shall produce audit records and logs that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred (normally the destination system), the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. In addition, Metropolitan Government shall, where possible, store and manage the content of audit records and logs generated by the applicable Information System in a centralized location, in order to improve log analysis, integrity and retention.

4.0 Audit Generation

The Metropolitan Government shall assess Information Systems capability of producing necessary audit logs based on business need.

5.0 Audit Storage Capacity

Metropolitan Government shall allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded. It also shall consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

6.0 Response to Audit Processing Failures

The Information System shall, is possible:

6.1. Alert designated Metropolitan Government staff in the event of an audit processing failure; and

6.2. Take the appropriate, applicable additional action, including, but not limited to: shut down Information System, overwrite oldest audit records, and stop generating audit records.

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

7.0 Audit Review, Analysis and Reporting

Metropolitan Government shall:

7.1. Review and analyze Information System audit records for indications of inappropriate or unusual activity, and report findings to designated Metropolitan Government officials; and

7.2. Adjust the level of audit review, analysis, and reporting within the Information System when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Metropolitan Government shall, if possible, integrate/correlate:

a. Audit review, analysis and reporting processes to support organizational processes for investigation and response to suspicious activities; and

b. Analyze audit records of vulnerability scanning information, performance data and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

8.0 Time Stamps

The Information System shall use internal system clocks to generate time stamps for audit records. Those clocks shall be configured to use a Metropolitan Government approved time source.

9.0 Audit Record Retention

Metropolitan Government shall retain audit records for an appropriately defined time to provide support for after-the-fact investigations of security incidents and to meet regulatory and Metropolitan Government information retention requirements. It shall retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes.

10.0 Protection of Audit Information

The Metropolitan Government shall take necessary steps to protect audit logs, including limiting access to appropriate personnel, backing up logs and alerting to log deletion/clearing.

11.0 Non-repudiation

Metropolitan Government Information System shall:

11.1. Protect against an individual falsely denying having performed a particular action; and

11.2. Associate the identity of the information producer with the information.

12.0 Monitoring for Information Disclosure

Metropolitan Government shall identify and monitor intelligence sources, including open source information, for evidence of unauthorized exfiltration or disclosure of organizational information.

13.0 Session Audit

The Information Systems shall provide the capability to capture/record and log content related to a user initiated session at system start-up.

14.0 Information System Monitoring

Metropolitan Government shall, where applicable:

14.1. Monitor events on the Information System in accordance with documented standards and detect attacks against the Information System;

14.2. Deploy monitoring devices: (i) strategically within the Information System to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

14.3. Heighten the level of Information System monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

14.4. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification and deletion;

14.5. Analyze outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies;

14.6. Employ controls to detect unauthorized network devices, such as rogue wireless devices, and to detect attack attempts and potential compromises/breaches to the Information System; and

14.7. Assess and configure Information Systems to leverage monitoring and alerting capability where capable.

15.0 Flaw Remediation

Metropolitan Government shall, among other things, expeditiously address flaws discovered during security assessments, continuous monitoring, incident response activities, or Information System error handling.

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.

3/2/2018

_____ _____

Keith Durbin
Director of Information Technology Services
Metropolitan Government of Nashville and Davidson County

Date

REFERENCES

- ISO 27002: sections 10.10.1-6, 10.3.1, 15.1.3
- NIST Special Publication 800-92, *Guide to Computer Security Log Management*
- NIST Special Publication 800-53 rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations:* Control numbers – SI-1,AU-1, AU-4, AU-5, PE-6, PE-8, SC-7, AU-9, SI-2, AU-2(4), AU-3(1, 2), AU-12(2), AU-6(1), AU-6(5), AU-7, AU-8, SI-4(1), SI-4(8), SI-4(11), SI-4(14), SI-4(4), SI-4(5)

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	11/17/2017	Original Version