NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S14-005
IT Standard: **Security Logging**	**Updated:** 02/21/2017
	Issued By: NYS Office of Information Technology Services **Owner:** Enterprise Information Security Office

1.0 Purpose and Benefits

Logs record data so that systems and networks can be appropriately monitored to maintain use for authorized purposes and an awareness of the operating environment, including detecting indications of security problems.

This standard defines requirements for security log generation, management, storage, disposal, access and use. Security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; databases and applications.

2.0 Authority

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

3.0 Scope

This standard is promulgated pursuant to New York State Information Technology Policy NYS-P03-002, Information Security, and applies to ITS, all State Entities (SE) that receive services from ITS, and affiliates of same (e.g., contractors, vendors,

solution providers), which have access to or manage SE information. It also serves as recommended practice for the State University of New York, the City University of New York, non-Executive branch agencies, authorities, NYS local governments and third parties acting on behalf of same.

This standard applies to all information technology equipment owned and/or operated by, or on behalf of, New York State. This standard addresses only those logs that typically contain computer security-related information, such as audit logs that track user authentication attempts and user actions, and security device logs that record possible attacks.

4.0 Information Statement

Logs must be generated in information technology (IT) systems and networks. Because of the nature of the data contained in security logs (e.g., passwords, e-mail content), they are considered Personal, Private or Sensitive Information (PPSI) and must be protected with the controls for a confidentiality and integrity of high (see Information Security Controls Standard).

4.1 Initial Log Generation

a. All hosts and networking equipment must perform security log generation for all of its components (e.g., OS, service, application).

b. All security events (Appendix A) must be logged and must be set to capture significant levels of detail to indicate activity.

4.2 Log Administration

a. All hosts and networking equipment must issue alerts on security log processing failures, such as software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. All alerts must be as close to real time as possible.

b. When non-revolving log storage reaches 90% capacity, a warning must be issued.

4.3 Log Consolidation

a. Security-related information from all systems, with the exception of individual workstations, must be transferred to a consolidated log infrastructure. Systems running workstation operating systems which are used for shared services, such as shared file storage or web services must also satisfy these requirements.

b. All workstations must have the ability to transfer logs to a consolidated log infrastructure, if needed.

c. Log data must be transferred real-time from individual hosts to a consolidated log infrastructure. Where real-time transfer is not possible, data must be

transferred from the individual hosts to a consolidated log infrastructure as quickly as the technology allows.

d. State entities (SEs) must establish processes for the establishment, operation and, as appropriate, integration of log management systems.

4.4 Log Storage and Disposal

a. Within the consolidated log infrastructure, logs must be maintained and readily available for a minimum of 92 days. Based on SE requirements, including audit or legal needs, logs may need to be retained for a longer period of time.

b. Log data must be securely disposed of (at both the system and the infrastructure level) in compliance with the Sanitization/Secure Disposal Standard.

c. Systems that collect logs, whether local or consolidated, must maintain sufficient storage space to meet the minimum requirements for both readily available and retained logs. Storage planning must account for log bursts or increases in storage requirements that could reasonably be expected to result from system issues, including security.

d. A process must be put in place to provide for log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records (e.g., how the impacted logs must be marked, stored, and protected).

e. Log integrity for consolidated log infrastructure needs to be preserved, such as storing logs on write-once media or generating message digests for each log file.

4.5 Log Access and Use

a. Log data must be initially analyzed as close to real time as possible.

b. Access to log management systems must be recorded and must be limited to individuals with a specific need for access to the records. Access to log data must be limited to the specific sets of data appropriate for the business need.

c. Procedures must exist for managing unusual events. Response must be commensurate with system criticality, data sensitivity and regulatory requirements.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Enterprise Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	Definition
Consolidated Log Infrastructure	The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Enterprise Information Security Office
Reference: NYS-S14-005
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
02/21/2014	Original Standard Release; *replaces ITS S11-001 Security Monitor and Logging and CSCIC/OCS S10-005 Monitoring System Access and Use*	Thomas D. Smith, Chief Information Security Officer
02/20/2015	Standard Review; no changes	Deborah A. Snyder, Deputy Chief Information Security Officer
02/21/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer

9.0 Related Documents

NIST Special Publication 800-92, Guide to Computer Security Log Management

Appendix A: Security Events to Log

Security events that must be logged for all systems include but are not limited to:

Successful and unsuccessful authentication events to include but not limited to:

- system logon/logoff;
- account or user-ID;
- change of password;
- the type of event;
- an indication of success or failure of event;
- the date and time of event; and
- Identification of the source of event such as location, IP addresses terminal ID or other means of identification.

Unsuccessful resource access events will be logged to include at minimum:

- account or user-ID;
- the type of event;
- an indication of the event;
- the date and time of event;
- the resource; and
- identification of the source of event such as location, IP addresses terminal ID or other means of identification.

Successful and unsuccessful privileged operations including but not limited to:

- use of system privileged accounts;
- system starts and stops;
- hardware attachments and detachments;
- system and network management alerts and errors messages; and
- security events - account/group management and policy changes.

Successful and unsuccessful access to log files to include but not limited to:

- account or user-ID;
- the type of event;
- an indication of success or failure of event;
- the date and time of event; and
- identification of the source of event such as location, IP address, terminal ID or other means of identification.

Appendix A: Security Events to Log

Most web servers offer the option to store log files in either the common log format or an extended log format. The extended log format records more information than the common log file format. When technically feasible web servers must use extended log format. The extended log format adds valuable logging information to your log file so you can determine where messages are coming from, who is sending the message and adds information to the log file that would be necessary to trace an attack.

For systems identified as critical based on an SE risk assessment or systems that have not yet been classified, in addition to the above, successful resource access events will be logged to include at a minimum:

- account or user-ID;
- the type of event;
- an indication of the event;
- the date and time of event;
- the resource; and
- identification of the source of event such as location, IP addresses terminal ID or other means of identification.