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:** 11/23/2021 **Issued By:** NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

Security logs record data so that systems can be appropriately monitored. This monitoring allows authorized staff to support operations, maintain awareness of security events, and verify compliance.

This standard defines requirements for security log generation, management, storage, disposal, access, and use. Security logs are generated by many sources, including but not limited to security software and firewalls; intrusion detection and prevention systems; operating systems (OS) on servers, workstations, networking equipment, and databases; and applications.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive Order No. 117[1], established January 2002, provides the State Chief Information Officer with 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

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

(IT) Policy, Standards and Guidelines.

3.0 Scope

This standard applies to all "State Entities" (SE), defined as "State Government" entities as defined in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law, and NYS political subdivisions, and includes, but is not limited to, their employees, consultants, vendors, and contractors, that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. Where a conflict exists between this standard and a SE's standard, the more restrictive standard will take precedence.

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, collectively referred to as "security logs."

4.0 Information Statement

Security logs must be generated in information technology (IT) systems and networks. Due to the nature of the data contained in security logs (e.g., passwords, e-mail content), they are considered Personal, Private, or Sensitive Information (PPSI) with a minimum of moderate confidentiality and moderate integrity and must be protected as such per the NYS-S14-002 Information Classification Standard.

4.1 Initial Log Generation

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

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

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, except for individual workstations, must be transferred to a consolidated log infrastructure. Systems running workstation OSs that are used for shared services, such as shared file storage or web services, must also satisfy these requirements.

b. When required, workstations must have the ability to transfer logs to a consolidated log infrastructure.

c. Security log data must be transferred in real-time from individual hosts to a consolidated log infrastructure. Where real-time transfer is not possible, the security log data must be transferred from the individual hosts to a consolidated log infrastructure as quickly as the technology allows.

d. 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, security logs must be maintained and readily available for a minimum of 92 days. Based on SE requirements, including audit or legal requirements, security logs may need to be retained for a longer period of time.

b. Security log data must be securely disposed of (at both the system and the infrastructure level) in compliance with the NYS-S13-003 Sanitization/Secure Disposal Standard.

c. Systems that collect security logs, whether local or consolidated, must maintain sufficient storage space to meet the minimum requirements for both readily available and retained security 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 incidents.

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

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

4.5 Log Access and Use

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

b. Security log data must be initially analyzed as close to real time as possible.

c. Procedures must exist for managing unusual events identified through security log analysis. Any corresponding response must be commensurate with system criticality, data sensitivity, and regulatory requirements.

5.0 Compliance

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

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs must request an exception through the Chief 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.

7.0 Contact Information

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

Chief Information Security Office
Reference: NYS-S14-005
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@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

Date	Description of Change	Reviewer
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
09/13/2018	Scheduled review – minor wording changes and minor update to Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer
11/23/2021	Scheduled review	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:

1. Successful and unsuccessful authentication events including 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 the event;
   - the date and time of the event; and
   - identification of the source of the event such as location, IP addresses terminal ID, or other means of identification.
2. 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.

3. Successful and unsuccessful access to security log files to including but not limited to:

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

3. Unsuccessful 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 the event;
   - the resource; and
   - identification of the source of the event such as location, IP addresses terminal ID, or other means of identification.

4. 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 the event;
    - the resource; and
    - identification of the source of the event such as location, IP addresses terminal ID, or other means of identification.

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 the 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.