UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Event Logging Standard

Revision History

Date:	By:	Contact Information:	Description:
05/02/18	Robert Smith	robert.smith@ucop.edu	Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC.
10/19/18	Robert Smith	robert.smith@ucop.edu	Updated standard title in 4.6.
07/31/19	Robert Smith	robert.smith@ucop.edu	Made minor changes to improve clarity. No requirements were added or removed. Added “When there is a requirement set for a specific protection level” to the Scope statement.
08/21/19	Robert Smith	robert.smith@ucop.edu	Updated to conform to standard format.
10/03/19	Robert Smith	robert.smith@ucop.edu	Approved by ITLC.
11/04/20	Robert Smith	robert.smith@ucop.edu	Updated to address comments, questions, to make minor corrections and to make minor improvements. Updated Appendix 1. Approved by ITLC.

Contents

1 Background and Purpose

Logging and log monitoring are essential information security controls used to identify, prevent and respond to operational problems, security incidents, policy violations and fraudulent activity. Logging facilitates the optimization of system and application performance and assists in business recovery activities. In many cases, logging and the associated monitoring are required in order to comply with federal, state and local laws and regulations.

Logging also provides system administrators, supervisors and compliance officers with information useful for diagnostics and auditing.

This Standard details the requirements for event logging to support information security and also addresses some operational needs to support availability.

The IT Policy Glossary can be helpful when applying this Standard. The term "IT Resources" is defined with examples in the glossary. IT Resource processing, storing, managing or transmitting Institutional Information are import sources of events.

2 Scope

This Standard applies to all Locations.

This Standard applies to all IT Resources used by anyone conducting business by, for or on behalf of the University of California for administrative and academic purposes when:

- The IT Resource is processing, storing, managing or transmitting Institutional Information classified at Protection Level 3 or above, not including single user devices.
- The IT Resource is classified at Availability Level 3 or above.
- Complying with contracts or grants that set forth security and/or operational concerns addressed by logging.
- Complying with regulatory requirements.
- Complying with event logging requirements set by specific Protection Levels, Availability Levels or risk assessments.
- The UISL, CISO or CIO identifies a specific need to collect logs for security or operational concerns.

2.1 Scope exclusions

Unless included above, the following devices are beyond the scope of this Standard:

- Personal or non-UC devices not managed by UC.
- Research computing; academic experiments; or student projects not involving Institutional Information classified at Protection Level 3 or higher.
- IT Resources excluded by the CISO and CIO.
- Single user devices.

3 Definitions and Key Terms

There are no specially defined terms required for using this Standard.

For more information about definitions, consult the IT Policy Glossary.

4 Requirements

The CISO and CIO identify security and operational concerns to establish event logging requirements. (See Scope above.)

Unit Information Security Leads (UISLs) and IT Workforce Members must ensure the implementation of the requirements detailed in this section.

4.1 Plan and inventory

UISLs must establish a logging plan. The plan must include:

- A method to inventory systems that are required to log events for information security purposes.
- Steps to manage cyber risk by assessing risk levels and resources for logging.
- Security and operational log monitoring to identify security and operational events requiring action.
- The level of security logging detail to identify events requiring action.
- The level of operational logging detail to identify events requiring action.
- Log storage (local and/or centralized).
- Log access controls.
- Centralized logging from IT Resources, including Service Providers and Suppliers.
- Log forwarding to applicable Service Providers and Suppliers.
- Time synchronization.
- A testing plan and interval.
- Gaps and mitigations.
- Log retention and schedule.
- Log management: log erasing, purging and trimming.

Units processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher must submit and review their plan with the CISO at least annually.

4.2 Log details

When managing cyber risk within their areas of responsibility, Centralized IT Units, Service Providers, Units and IT Resource Proprietors or other designated individuals have some flexibility in determining the type and amount of detail contained in the logs of IT Resources and systems in order to achieve the desired outcome. The following requirements, however, do apply:

- For privacy, confidentiality and integrity concerns, the amount and type of information logged should be commensurate with the Protection Level of the Institutional Information and/or IT Resource (e.g., systems that process Institutional Information classified at Protection Level 3 or 4 will appropriately capture more log detail than those that process less sensitive data).
- For availability concerns, the amount and type of information logged should be commensurate with the Availability Level of the Institutional Information and IT Resource (e.g., event logs for IT Resources classified at Availability Level 3 or 4 will appropriately capture more log detail than those of IT Resources processing less sensitive information).

Note: See Appendix A for examples.

4.3 Event sources

IT Workforce Members must include event sources that are needed to manage cyber security risk in the Unit's logging implementation. Event sources include, but are not limited to:

- Access control systems/physical security.
- Application appliances.
- Cloud services (e.g., IaaS, SaaS, and PaaS).
- Computer controlled instruments.
- Databases.
- End points.
- Industrial control systems.
- Internet of Things devices (IoT).
- Medical devices.
- Network devices.
- Printers, scanners and multifunction devices.
- Security and other network-attached appliances.
- Security devices or systems.
- Server/OS.
- Systems (Applications).

Note: For HIPAA and requirements like those found in the PCI DSS (credit cards), Gramm–Leach–Bliley Act (GLBA) (impacts student loans and other financial transactions) and the NIST 800-171 standard (supporting financial aid and some research contracts), application logs will also need to identify who accesses and who changes records.

4.4 Segregated log storage and tamper protection

A copy of log data must be stored on a separate logical device that is protected from unauthorized modification with at least the same control set as the source IT Resource. This is required for all:

- IT Resources handling Institutional Information classified at Protection Level 3 or higher.
- IT Resources handling Institutional Information classified at Availability Level 3 or higher.
- Critical IT Infrastructure.

Logging facilities and log information must be protected against tampering, modification, destruction and unauthorized access.

4.5 Time synchronization

Each Location must establish methods for time synchronization of logging and monitoring activities using Network Time Protocol (NTP), Precision Time Protocol (PTP) or following the Location-approved time synchronization method.

The clocks of IT Resources within a Unit or security domain must be synchronized to a standard reference time source.

Note: Refer to Section 5 References for details on time synchronization.

4.6 Timestamp format

Timestamps must not be truncated or abbreviated in any way and must:

- Follow the Location-approved time recording method or use a time zone offset that corresponds to local time.
- Be formatted in accordance with ISO 8601:2004 and RFC 3339.

4.7 Log management framework

For Institutional Information classified at Protection Level 3 or higher, event logging must use CISO-approved logging tools and framework(s).

Note: Example frameworks and tools include, but are not limited to:

- Arcsight.
- CLF/ELF for web servers.
- Elastic.
- IBM QRadar.
- log4j and log4net (applications).
- SNMP (Network).
- Splunk.
- syslog/syslog-ng/rsyslog.
- Windows event log.

4.8 Handling sensitive information in logs

Log management procedures require appropriate handling of sensitive information. IT Workforce Members must apply these controls to:

- Logs containing Institutional Information classified at Protection Level 3 or higher must require the same security controls, including encryption, as the Institutional Information they contain.
- Logs must be available only on a need-to-know basis and they must follow Location access procedures.[1]
- All transmissions of logs must use secure protocols and reliable mechanisms.

Workforce Members must obtain approval for erasing, purging or trimming event logs through the change management process.

IT Workforce Members must not log the following information:

- Social Security Numbers (SSN).
- Unencrypted personal information (e.g., personal account numbers, financial account numbers, credit card numbers, etc.).
- Clear text authentication credentials (e.g., passphrases, passwords, secret questions).

[1] See also the Electronic Communications Policy, http://policy.ucop.edu/doc/7000470/ElectronicCommunications, for important information needed to plan the administration, technical and operational implementation of logging and access to log information.

4.9 Requiring the use of a SIEM

As required and scoped by the CISO, Units must configure IT Resources processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher to send log data to a Security Incident and Event Management system (SIEM).

4.10 Logging privileged user actions

For Institutional Information classified at Protection Level 3 or higher and IT Resources classified at Availability Level 3 or higher, actions performed by privileged user accounts in performance of their duties must be logged and reviewed by a peer (e.g., other admin, InfoSec professional, etc.) based on risk in order to determine the appropriateness of the actions performed.

4.11 Limiting administrator access to logs

When possible, IT Workforce Members acting as system administrators on IT Resources classified at Protection Level 3 or higher and Availability Level 3 or higher must not have permission to erase, deactivate or modify logs of their own activities.

4.12 Log retention

IT Workforce Members must retain logs based on:

- UC Records Retention Schedule requirements set by the Institutional Information Proprietor.
- Contractual obligations.
- Litigation holds, preservation orders.
- Applicable regulatory requirements.
- Other retention requirements prescribed.

5 References

UC Policy

IS-3, III Section 12.4 - Logging and monitoring

Electronic Communications Policy:
http://policy.ucop.edu/doc/7000470/ElectronicCommunications

IS-3 Policy and Standards Implementation FAQs:
https://security.ucop.edu/policies/frequently-asked-questions.html

UC Standards

UC Institutional Information and IT Resource Classification Standard

External Resources

ISO 27002 Section 12.4 “Logging and monitoring”

ISO 27002 Section 13.1.1.d “Logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security”

Appendix A Glossary - Guide to Computer Security Log Management, NIST SP 800-92:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Comparison of NTP and PTP: http://www.en4tel.com/pdfs/NTPandPTP-A-Brief-Comparison.pdf

Guide to Computer Security Log Management, NIST SP 800-92: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

IEEE 1588-2019 - Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control: https://standards.ieee.org/standard/1588-2019.html

OWASP Logging Cheat Sheet: https://www.owasp.org/index.php/Logging_Cheat_Sheet

RFC 5424 The Syslog Protocol: https://tools.ietf.org/html/rfc5424

Deprecated: The BSD syslog Protocol: https://tools.ietf.org/html/rfc3164

6 Appendix A – Logged Events Examples

IT Resource logging configurations (e.g., which entries and data fields are sent to the centralized log servers and what log format should be used) must be established to manage operational and security risks.

A Workforce Member's ability to configure each log source is dependent on the features offered by that particular type of log source. For example, some log sources offer very granular configuration options, while some offer no granularity at all—logging is simply enabled or disabled, with no control over what is logged.

When planning which details to log, UISLs, CIOs and CISOs should consider:

- The classification of Institutional Information and/or the IT Resource(s).
- The Location's past experiences of IT Resource vulnerability, exploitation and/or misuse.
- The extent of system interconnectedness.
- The primary purpose of logging for the IT Resource (e.g., operational, security, or both).
- The effects on system performance.
- The costs of logging and reviewing log data vs. security and operational risks.

Logged events might include, but are not limited to:

- Access and access attempts to root administrator or other privileged credentials.
- Access to audit logs.
- Active Directory object name changes.
- Account activity which can include, but is not limited to, success and/or failure of:
    - Creation/deletion.
    - Activation/enablement.
    - De-activation/disablement.
    - Authentication (Log-on/log-off success/failed).
    - Lockouts.
    - Unlocks.
    - Password changes.
    - Privilege assignments.
- Account login with explicit credentials.
    - Activation and deactivation of protection systems (e.g., anti-virus, intrusion detection, encryption and file integrity systems).
    - Alarms raised by IT Resources (e.g., console alerts or messages, system log exceptions, network management alarms, alarms raised by access control systems).
- Application/service error, hang, stop, start, and restart.
- Boot events.
- Changes to IT Resource(s) or system configuration.
- Cron events.
- Event log change or purge.
- Firewall and security tool rule changes (add, delete, modify, suspend, etc.).

- Group changes (create, property change, delete, and membership change), including privileged group modifications.
- Group or other system policy failed to load.
- Kerberos events, which can include, but are not limited to:
  - Kerberos authentication ticket (ticket granting ticket - TGT) was requested.
  - Kerberos authentication ticket request failures.
  - Kerberos authentication ticket requests.
  - Kerberos events.
  - Kerberos failure codes.
  - Kerberos pre-authentication failures.
  - Kerberos service ticket requests.
- Password change (by privileged user).
- Password change (by user).
- Privileged account events.
- Proxy events.
- Remote desktop sessions (connect, reconnect, and disconnect).
- Screensaver events.
- Security tool detection events.
- Sensitive search terms[2] (like medical record number, uncommon or flagged names, etc.).
- Session timeouts.
- System or application audit or logging policy change.
- Termination of database related processes.
- Workstation lock/unlock events.

For each logged security event, including the ones above, the following must be recorded, as appropriate:

- Application, program or utility used.
- Data accessed, including identity or name of affected data, information system or network resource.
- Date and time, and when applicable time zone or offset.
- Origination of event (e.g., user ID, system account, network address, etc.).
- Protocol.
- Success or failure indication.
- Target of event (e.g., network address, host name, application, service, port, etc.).
- Type of event, event ID.

Open source workstation logging baseline projects (review required before use):

- Microsoft Windows security baselines:

[2] Most common in UC Health.

    - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
    - https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines
- SwiftOnSecurity/sysmon-config:
    - https://github.com/SwiftOnSecurity/sysmon-config
- ion-storm/sysmon-config, based on SwiftOnSecurity:
    - https://github.com/ion-storm/sysmon-config

Note: The list above provides examples and is not exhaustive. Operating systems, applications, run-time environments (or run-time containers), ICS/SCADA, IoT devices, medical devices, software-as-a-service, security tools and devices vary in their logging capabilities and event detail. IT Workforce Members should use best practice guides and tools from SIEM vendors and other sources to tune what is logged locally and what is forwarded to centralized tools. This is important for detection, response and recovery from adverse incidents. This approach is necessary for both security and operational events.
