Purpose

ASU's Information Security Policy and ACD125 require security controls to manage protection measures and minimize risks to the confidentiality, availability and integrity of ASU's data and information system resources. One primary method is to monitor access to computing resources through appropriate system logging.

Applicability

This standard applies to all users of ASU's computing, internet, and communications resources that have a high or medium criticality rating[1]; including all, faculty, staff (including student employees), contractors, vendors, consultants, temporary and other workers for ASU and its component units users.

Standard

Computing, internet and communication systems in the ASU technology network that support access to ASU services, and that handle sensitive and/or highly sensitive information (as defined in the ASU Data Handling Standard), accept network connections, or make access control (authentication and authorization) decisions must record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What was the activity performed on (object)?
- When was the activity performed?
- With what tool(s) was the activity performed?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Logs must be retained as needed per applicable data retention policy. Where log retention requirements are not provided by applicable law or regulation, logs should be retained for a period sufficient for review and investigation of current and past incidents, a minimum of six months.[2]

A periodic review by the unit's technology staff of security event logs, critical system component logs and logs from systems that perform security functions should occur as necessary to identify potential issues including anomalous activity. Alerts and any anomalous activity requiring further analysis should be routed to appropriate individuals and teams for action in accordance with the ASU Information Security Incident Response Standard. The following events are to be reviewed frequently and at least twice weekly.[3]

- All security related events (as described in the Server Security standard)
- Logs of all system components that store, process, or transmit sensitive and/or highly sensitive data
- Logs of all critical system components

---

[1] System tier rating may be affected by factors such as network placement or level of access to certain systems.

[2] https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense . CSC 6.1 does not supply log retention criteria however NIST 800-53 low AU-11 states that "Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes."

[3] https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense, CSC 6.4

- Logs of all servers and system components that perform security functions including firewalls, intrusion-detection systems/intrusion-prevention systems, file-integrity monitoring systems, authentication servers, and e-commerce redirection servers

Activities to be Logged

Within the abilities of the system, logs should be created for the following types of activities:

- Create, read, update or delete actions;
- Accept a network connection;
- User authentication and authorization for activities such as user login and logout, failed privileged account (including system admin or DBA) attempted logins or privileged account password/authentication reset requests;
- Grant, modify or revoke access rights, including adding a new User or group, changing User privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and User password changes;
- System, network, or services configuration changes, including installation of a software patches and updates or other installed software changes;
- Application process startup, shutdown or restart;
- Application process abort, failure or abnormal end especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources) and/or the failure of network services such as DHCP or DNS, or hardware fault; and
- Detection of suspicious/malicious activity such as from an intrusion detection or prevention system (IDS/IPS), anti-malware system or anti-spyware system.

Elements of the Log[4]

Within the abilities of the system, logs should identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete and accept network connection;
- Subsystem performing the action – examples include process or transaction name, process or transaction identifier;
- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, mac address. All identifiers should be standardized to facilitate log correlation;
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address. All identifiers must be standardized to facilitate log correlation;
- Before and after values when action involves updating a data element;
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;
- Whether the action was allowed or denied by access-control mechanisms; and
- Description and/or reason-codes why the action was denied by the access-control mechanism, if applicable.

Formatting and Storage[5]

The system shall support the formatting and storage of audit logging in such a way as to ensure the integrity of the logs, protect logs from modification or deletion and support enterprise-level analysis and reporting.

[4] https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring

[5] https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense

An enterprise-level log management mechanism capable of supporting the centralized retention, protection, and analysis of audit log data exists. It is recommended that enterprise-level systems log to the enterprise-level log management mechanism. The enterprise-level log management mechanism serves as ASU's audit retention system of record.

Mechanisms known to support these goals include, but are not limited to, the following:

- Microsoft Windows Event Logs collected by a centralized log management system;
- Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system;
- PeopleSoft logs collected;
- Logs stored in an DBMS database that itself generates audit logs in compliance with the requirements of this document; and
- Other open logging mechanisms supporting the above requirements include those based on CheckPoint OpSec, ArcSight CEF, Splunk, and IDMEF.

Security Related Event Review

Security-related events should trigger an alert and need to be reviewed frequently.

Violations and Enforcement

Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU's computing, Internet and communication resources until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

In a circumstance where compliance may not be immediately possible, the ASU academic or business units must confer with the Information Security Office to develop a plan for moving into compliance within a reasonable amount of time.

Resources

ACD 125
Arizona State Library, Archives, & Public Records
Data Handling Standard
Information Security Incident Response Standard
Server Security Standard
Add Data to Splunk (ServiceNow request)
CIS CSC 20 Control 6

Standard Revision

This Standard is subject to review and revision at the direction of, and only after approval by, Chief Information Security Officer. To offer suggestions and/or recommendations, contact the ASU Information Security Office at infosec@asu.edu.