Audit and Accountability (AU)

Purpose:

The following standards are established to support the policy statement 10.5 that "CSCU will: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems."

Scope:

1. Institutional Units of the Connecticut State College and University System including the Connecticut Board of Regents System Office.
2. All Connecticut State College and University institutional units' information systems.

Standard:

1. Auditable Events [NIST 800-53 AU2]

1.1 All Information Systems must produce audit records for the following events:

a.) System startup and shutdown

b.) User logon and logoff

c.) Modifications of privileges and access controls

d.) Account creation, modification, or deletion

e.) Password changes

1.2 Moderate and High Risk Information Systems must additionally produce audit records for the following events:

a.) System alerts and error messages

b.) System administration activities including configuration changes

c.) Starting and stopping of processes and services

d.) Installation, modification, and removal of software

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.500	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

e.) Access to and modification of high risk (DCL2, DCL3) information and data.

1.3 Information systems that primarily provide information security control functions and capabilities must additionally produce the audit records associated with those functions (e.g. firewall policy logs, intrusion detection logs, access control logs, anti-virus logs, etc.)

1.4 The Information Security Program Office (ISPO) must review and update the selected audited events biannually, or as required. [NIST 800-53 AU-2(3)]

2. Content of Audit Records [NIST 800-53 AU3]

2.1 Audit log records must include at least the following elements:

a.) Identifier of the system that generated the event

b.) Date and time when the event occurred

c.) The action or type of event and any relevant data

d.) Success or failure of the action

e.) Subject identity (e.g., user, device, process context)

f.) Remote address, if the event occurs over a network connection

3. Audit Storage Capacity [NIST 800-53 AU-4]

3.1 The audit storage capacity must be configured to allow for sufficient space to record all necessary auditable actions identified in section 1, Auditable Events, and section 9, Audit Record Retention, to prevent the capacity from being exceeded.

4. Response to Audit Processing Failures [NIST 800-53 AU-5]

4.1 All Information Systems must be configured to:

a.) Alert designated officials in the event of an audit failure or when audit storage capacity is 80%, and again at 90% utilization automatically. [NIST 800-53 AU-5(1)]

b.) Distribute alerts by a mechanism that allows system administrators to receive it at any time including after normal working hours (e.g., email, text message).

c.) Once the maximum storage capacity for audit logs is reached, the information system must overwrite the oldest audit records.

4.2 Moderate and High Risk Information Systems must additionally:

a.) When devices cannot generate logs or the maximum storage capacity has been reached, the information system must be configured to send an alert to system administrators within two minutes. Procedures must reflect escalation of priority resolution actions after twenty-four hours. [NIST 800-53 AU-5(2)]

5. Audit Review, Analysis, and Reporting [NIST 800-53 AU-6]

5.1 For all information systems the Information System Owner must:

a.) Review and analyze audit logs and records weekly for indications of inappropriate or unusual activity; and report findings in accordance with CSCU Incident Handling Procedures.

5.2 Moderate and High Risk Information Systems must additionally:

a.) Review and analyze audit logs and records daily for indications of inappropriate or unusual activity; and reports findings in accordance with CSCU Incident Handling Procedures.

b.) Employ automated tools that can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation, analysis, reporting, and alerting to support organizational processes for investigation and response to suspicious activities. [NIST 800-53 AU-6(1)]

c.) Analyze and correlate audit records across different repositories to gain CSCU-wide situational awareness. [NIST 800-53 AU-6(3)]

5.3 The level of audit review, analysis, and reporting may be adjusted if there is a change in risk to CSCU operations, assets, or personnel. Adjustments must be based upon advisories, warnings, legal, or regulatory notification such as, but not restricted to: [NIST 800-53 AU-6(10)]

a.) United States Computer Emergency Readiness Team (US-CERT) alerts

b.) CSCU Information Security Program Office (ISPO) advisories

c.) Law Enforcement Requests

d.) Freedom of Information Requests

e.) eDiscovery \ Legal Requirements

f.) Security Investigations

5.4 All staff involved with audit log review and analysis responsibilities must:

a.) Be trained on how to review and analyze audit logs

b.) Report incidents in according with the CSCU Incident Handling Procedures.

6. Audit Reduction and Report Generation [NIST 800-53 AU-7]

6.1 Moderate and High Risk Information Systems must:

a.) Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and does not alter original audit records.

b.) Provide the capability to process audit records for events of interest based on the following audit fields within audit records: [NIST 800-53 AU-7(1)]

- Individual identities
- Event types
- Event locations
- Event times and time frames
- Event dates
- System resources involved, IP addresses involved
- Information object accessed

7. Time Stamps [NIST 800-53 AU-8]

7.1 The information system must be configured to use the internal system clock to generate time stamps for audit records; audit record timestamps must include:

a.) Date and time to millisecond precision; and

b.) Time zone in use by the device.

7.2 The information system must synchronize system clocks daily with a CSCU defined authoritative time source when the time difference is greater than thirty seconds. [NIST 800-53 AU-8(1)]

8. Protection of Audit Information [NIST 800-53 AU-9]

8.1 All Information Systems must:

a.) Protect audit information and audit tools from unauthorized access, modification, and deletion. Audit information includes all information (e.g. Audit records, audit settings, and audit reports) needed to successfully audit information system activity

b.) Audit logs that contain high risk (DCL2, DCL3) records must be encrypted using a FIPS-140-2 compliant cryptography. [NIST 800-53 AU-9(3)]

8.2 Moderate and High Risk Information Systems must also:

a.) Authorize access and modification to management of audit functionality to only a defined subset of privileged users. [NIST 800-53 AU-9(4)]

8.3 High Risk Information Systems must additionally:

a.) Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

b.) Back up audit records onto a physically different system or system components than the system or component being audited. [NIST 800-53 AU-9(2)]

c.) Use file integrity monitoring or change detection software on audit logs to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts.

9. Audit Record Retention [NIST 800-53 AU-11]

9.1 All information systems must:

a.) Retain audit logs for at least one (1) year with a minimum of ninety (90) days immediately available for analysis to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

b.) Comply with the Connecticut General Records Retention Schedule for State Agencies, Specifically, S6-100: Information Systems Usage Records, and implement whichever retention period is most rigorous, binding or exacting.

c.) Audit Log records that are relevant to litigation hold notifications or active investigations must be preserved until notice that these logs may be destroyed.

10. Audit Generation [NIST 800-53 AU-12]

10.1 All information systems must:

a.) Provide audit generation capabilities for security related events defined in section 1.1, Audit Records.

b.) Generate audit records for the events, defined in section 1.1, Audit Events, with the content defined in Section 2, Content of Audit Records.

10.2 Moderate and High Risk Information Systems must additionally:

a.) Provide audit generation capabilities for security related events defined in section 1.2, Audit Records.

b.) Generate audit records for the events, defined in section 1.2, Audit Events, with the content defined in Section 2, Content of Audit Records.

11. Session Audit [NIST 800-53 AU-14]

11.1 Moderate and High Risk Information Systems must:

a.) Provide capabilities to record application layer details and packet data for all network sessions across boundaries.

Roles & Responsibilities

Refer to the Roles and Responsibilities located on the website.

Definitions

Refer to the Glossary of Terms located on the website.

References

ITS-04 CSCU Information Security Policy

NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016.

General Records Retention Schedules for State Agencies, S6: Information Systems Records, Connecticut State Library, Office of the Public Records Administrator, Item S6-100, December 2010.