HSCEP OP: 56.50 – Audit & Accountability (AU)

Policy Statement:

TTUHSC El Paso shall create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity by ensuring that the actions of individual users and systems can be uniquely traced.

Reason for Policy:

The purpose of the Audit & Accountability (AU) policy is to ensure that TTUHSC El Paso creates and maintains appropriate scope and totality of audit records.

Entities Affected by this Policy are any and all users of Information Resources at TTUHSC El Paso.

What is covered in this Policy?

The overall policy addresses the Institutional stance as it applies to Audit & Accountability Policy and Procedures, Auditable Events, Auditable Events Reviews and Updates, Content of Audit Records, Audit Storage Capacity, Response to Audit Processing Failures, Audit Review, Analysis & Reporting, Audit Reduction & Report Generation, Time Stamps, Protection of Audit Information, Non-Repudiation, Audit Record Retention, Audit Generation, Monitoring For Information Disclosure, Session Audit, Alternate Audit Capability, and Cross-organizational Auditing.

It is the stance of TTUHSC El Paso to ensure that there are safeguards in place aligned with NIST 800-53 and TAC 202 to ensure the protection, integrity, and confidentiality of information resources at TTUHSC El Paso.

Who Should Read this Policy?

All individuals accessing, storing, viewing any TTUHSC El Paso information resources.

What happens if I violate this policy?

Any person(s) violating TTUHSC El Paso Information Technology policies are subject to penalty under Federal, state, and local legislation. Disciplinary actions are further outlined in HSCEP OP 56.50, Sanctions Policy.

AU-01: Audit & Accountability Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

TTUHSC El Paso is required to document organization-wide media protection controls that, at a minimum, include:

a. A formal, documented audit and accountability policy; and
b. Processes to facilitate the implementation of the audit and accountability policy, procedures and associated controls;

c. Name a person or role as the responsible party for the overall audit process and its results;
d. Determine the appropriate scope of audit controls that are necessary to protect organizational resources and ensure compliance requirements are met;
e. Determine what data will need to be captured by the audit controls and logs; and
f. Implement hardware, software, and procedural controls that record and examine activity.

AU-02: Auditable Events

TTUHSC El Paso:

- Determines, based on a risk assessment and mission/business needs that the system must be capable of auditing events;
- Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
- Provides a rationale for why the list of auditable events is deemed to be adequate to support after the fact investigations of security incidents

Auditable Events Include:

- All individual access to sensitive data (e.g., cardholder data and SSNs);
- All actions taken by any individual with root or administrative privileges;
- Invalid logical access attempts;
- Use of identification and authentication mechanisms; and
- Creation and deletion of system-level objects.

Auditable Events Include:

Reviews & Updates

These are required daily processes for linking access to systems and resources, including administrative privileged accounts (e.g., root or administrator).

AU-03: Content Of Audit Records

TTUHSC El Paso Systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Asset custodians are required to ensure the content of audit records generated by systems includes, at least, the following data fields for each event:

a. User identification;
b. Type of event;
c. Date and time;
d. Success or failure indication;
e. Origination of event; and
f. Identity or name of affected data, system component, or resource.

Audit Records Includes:

Content Of Audit Records

Asset owners and custodians are required to protect, and where required encrypt according to CIS level 1 baselines, log files that may contain sensitive data:

a. Passwords in the clear;
b. Social Security Numbers (SSN) or country-specific identification numbers;
c. Payment card numbers (e.g. credit or debit card); or

d. FINANCIAL ACCOUNT NUMBERS.

AU-04: Audit Storage Capacity

TTUHSC El Paso allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Asset custodians are required to allocate sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

Audit Storage Includes:

Transferring To Alternate Storage
Transfer refers to system off-loading of audit records based on an organization-defined frequency onto a different system or media than the system being audited. Asset custodians for critical systems are required to forward security-related event logs to a centralized log collection server.

AU-05: Response To Audit Processing Failures

TTUHSC El Paso Systems:

- Alert designated organizational officials in the event of an audit processing failure; and
- Take actions to remedy the audit processing failure.

Asset custodians are required to ensure critical systems are configured to:

a. Alert designated personnel in the event of an audit processing failure; and
b. Take actions to remedy the audit processing failure.

Audit Response Failures Includes:

Real Time Alerts
TTUHSC El Paso Systems provide a real-time alert to select personnel when the audit failure event requires real-time alerts. TTUHSC El Paso's IT staff is responsible for managing a 24x7x356 alerting process for critical system.

AU-06: Audit Review, Analysis & Reporting

TTUHSC El Paso:

- Reviews and analyzes system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
- Adjusts the level of audit review, analysis, and reporting within the system when there is a change in risk to organizational operations, organizational assets, individuals, or other organizations based on law enforcement information, intelligence information, or other credible sources of information.

Asset custodians are required to:

a. Review and analyze system audit records for indications of inappropriate or unusual activity, and report the findings in accordance with incident handling procedures;
b. Adjust the level of audit review, analysis, and reporting within the system when there is a change in risk to operations, assets, individuals, or other organizations based on credible sources of information;
c. Develop processes for the timely detection and reporting of failures of critical security control

systems, including but not limited to failure of:

i. Firewalls;
ii. IDS/IPS;
iii. FIM;
iv. Anti-malware;
v. Physical access controls;
vi. Logical access controls;
vii. Audit logging mechanisms; and
viii. Segmentation controls (if used); and

d. Responding to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:
    1. Restoring security functions;
    2. Identifying and documenting the duration (date and time start to end) of the security failure;
    3. Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause;
    4. Identifying and addressing any security issues that arose during the failure;
    5. Performing a risk assessment to determine whether further actions are required as a result of the security failure;
    6. Implementing controls to prevent cause of failure from reoccurring; and
    7. Resuming monitoring of security controls.

Audit Review Includes:

Process Integration
Where technically feasible, TTUHSC El Paso employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Correlate Audit Repositories
Where technically feasible, TTUHSC El Paso analyzes and correlates audit records across different repositories to gain enterprise-wide situational awareness.

Full-Text Analysis Of Privileged Commands
Where technically feasible, full-text analysis of privileged commands is required to be implemented to properly audit privileged actions performed on critical systems.

AU-07: Audit Reduction & Report Generation

TTUHSC El Paso Systems provide an audit reduction and report generation capability.

Asset custodians and data\process owners are required to provide the resources to automatically process audit records for events of interest, based on selectable event criteria and generate reports that allow asset custodians and data\process owners to review potentially significant issues and\or incidents on the system generating the event.

Audit Reduction Includes:

Automatic Processing
Where technically feasible, Information systems must provide the capability to process audit records for events of interest based on TTUHSC El Paso-defined audit fields within audit records.

AU-08: Time Stamps

Systems use internal system clocks to generate time stamps for audit records.

Asset custodians are required to configure systems and applications to use authoritative Network Time Protocol (NTP_ sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time:

a. Critical systems have the correct and consistent time;
b. Time data is protected; and
c. Time settings are received from industry-accepted time sources.

Time Stamp Includes:

Synchronization With Authoritative Time Source
The official NIST or USNO Internet Time Service (ITS) required to be used for system time synchronization include, but are not limited to:

- nist.gov 192.43.244.18 [primary]; and
- time-nw.nist.gov 131.107.13.100 [alternate]

AU-09: Protection Of Audit Information

TTUHSC El Paso Systems:

- Protect audit information and audit tools from unauthorized access, modification, and deletion:
- Authorize access to management of audit functionality to only a limited subset of privileged users; and
- Protect the audit records of non-local access to privileged accounts and the execution of privileged functions.

Asset custodians are required to:

a. Secure audit trails so they cannot be altered;
b. Limit viewing of audit trails to those with a job-related need;
c. Protect audit trail files from unauthorized modifications;
d. Promptly backup audit trail files to a centralized log server or media that is difficult to alter;
e. Write logs for external-facing technologies onto a log server on the internal LAN;
f. Use file-integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts, although new data being added should not cause an alert;
g. Identify all approved users with the ability to alter or destroy data; and
h. Ensure approved users are properly trained to handle sensitive data.

Audit Information Protection Includes:

Audit Backup On Separate Physical Systems\Components
Where technically feasible, TTUHSC El Paso shall back up audit records onto a physically different system or system component than the system or component being audited.

Access By Subset Of Privileged Users
TTUHSC El Paso restricts access to the management of audit functionality to users who have:

a. A valid business justification;
b. Received security awareness training commensurate with the level of risk from having privileged access; and
c. Demonstrated technical competence specific to the environment where privileged access is being granted.

AU-10: Non-Repudiation

TTUHSC El Paso Systems protects against an individual falsely denying having performed a particular action.

Asset custodians and data/process owners are required to implement electronic mechanisms to corroborate that sensitive data has not been altered in an unauthorized manner.

AU-11: Audit Record Retention

TTUHSC El Paso Systems retains audit records for an organization-defined time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Asset custodians and data/process owners are required to retain audit records as necessary by legal or contractual requirements to provide support for investigations of incidents and to meet data retention requirements. In general, logs must be retained according to TTUHSC El Paso's record retention schedule:

a. For critical or sensitive systems:
   i. Log entries must be immediately available for a minimum of 90 days (online);
   ii. Log entries must be available for 365 days (online or offline storage).
b. All logs must be exportable or transferable in an automated fashion;
c. Once logs are offloaded to a TTUHSC El Paso-approved log collector, the local logs may be removed from the reporting system or application.

AU-12: Audit Generation

TTUHSC El Paso Systems

- Provide audit record generation capability;
- Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
- Generate audit records.

Asset custodians and data/process owners are required to:

a. Ensure that systems produce a system-wide audit trail composed of audit records in a standardized format; and
b. Implement mechanisms to corroborate that sensitive data has not been altered or destroyed in an unauthorized manner.

All other IT Policies can be found at https://ttuhscep.edu/it/policies/

1. TAC §202.74, TAC §202.75
2. HIPAA 164.312(b) | PCI DSS 10.1 & 10.8 | NIST CSF PR.PT-1
3. MA201CMR17 17.04(4) | OR646A.622(2)(d)(B)(iii) | NIST CSF PR.PT-1
4. PCI DSS 10.3 & 10.3.1-10.3.6 | NIST CSF PR.PT-1
5. NIST CSF PR.DS-4 & PR.PT-1
6. NIST CSF PR.PT-1
7. NIST CSF PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.AN-1 & RS.CO-2
8. PCI DSS 10.8
9. PCI DSS 10.8.1
10. NIST CSF PR.PT-1 & RS.AN-3
11. PCI DSS 10.4 & 10.4.1-10.4.5 | NIST CSF PR.PT-1
12. http://tycho.usno.navy.mil/ntp.html

13. HIPAA 164.312(c)(a) | PCI DSS 10.5 & 10.5.1-10.5.5 | NIST CSF PR.PT-1
14. HIPAA 164.312(c)(b) | NIST CSF PR.PT-1
15. PCI DSS 10.7 | NIST CSF PR.PT-1
16. NIST CSF PR.PT-1, DE.CM-1, DE.CM-3 & DE.CM-7

Revised May 2018