UNIVERSITY OF OKLAHOMA
Information Technology
OU Health Sciences Center Security Policy

Information Resource Activity Review Policy

Purpose:

Processes must be in place for information system resources classified as sensitive per the Information System Resource Identification and Classification Standard to ensure all access and activity is recorded and reviewed by the Resource Owner or Resource Owner Representative.

Policy:

For all information system resources that contain or access data classified as sensitive per the Data Classification Standard, processes must be in place to ensure the access and activity is recorded and reviewed (audited).

The level and type of auditing mechanisms will be determined by the information system resource classification. At a minimum the following activity must be monitored by the Resource Owner or Resource Owner Representative:

- Use of a privileged account
- Information system resource start-up or stop
- Failed authentication attempts
- General login activity
- Password change activity
- Data modification where required for regulatory compliance

The appropriate hardware, software, or procedural auditing mechanisms must be implemented and at a minimum, these mechanisms must provide the following information:

- Date and time of activity
- Origin of activity
- Identification of user performing activity
- Description of attempted or completed activity

The recorded activity created by audit mechanisms for these information system resources must be reviewed regularly. The frequency of such review is determined by the information system resource classification. This review must be via a formal documented process which, at a minimum, will define:

- The person or persons responsible for reviewing activity records
- What constitutes “significant” activity
- Defining what steps are taken when exceptions or anomalies are identified
- Which activity records need to be archived and for what period of time
- What constitutes a security incident to be reported
- The procedures for preserving records of significant activity

Whenever possible, employees should not be assigned to monitor or review activity related to their own user accounts.

Scope/Applicability:

This policy is applicable to all OUHSC workforce members.

Regulatory Reference:

- 45 CFR 164.308(a)(1)(ii)(B) [HIPAA Security rule]
- 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘GLB Act’’)
- PCI DSS v3.0 (Payment Card Industry Data Security Standard)
- State of Oklahoma Information Security Policy, Procedures, Guidelines

Policy Authority/ Enforcement:	The University's Internal Auditing department is responsible for monitoring and enforcing this policy.

Policy:	Information Resource Activity Review Policy
Coverage:	University of Oklahoma HSC
Version:	2.1
Approved:	03/14/2007
Effective:	03/14/2007
Revised:	10/28/2014, added -- "Defining what steps are taken when exceptions or anomalies are identified" under the section "This review must be via a formal documented..."
Reviewed:	10/15/2014