Information System Activity Review Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Scope:

This policy applies to <<Organization Name>> in its entirety, including all systems that process sensitive information.

Policy:

<<Organization Name>> will clearly identify all critical systems that process sensitive information. <<Organization Name>> will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible, of the following, as reasonable and appropriate:

* User IDs
* Dates and times of log-on and log-off
* Terminal identity, IP address and/or location, if possible
* Records of successful and rejected system access attempts

Safeguards must be deployed to protect against unauthorized changes and operational problems including:

* The logging facility being deactivated
* Alterations to the message types that are recorded
* Log files being edited or deleted
* Log file media becoming exhausted, and either failing to record events or overwriting itself

Responsibilities:

The Security Officer will clearly identify:

* The systems that must be reviewed
* The information on these systems that must be reviewed
* The types of access reports that are to be generated
* The security incident tracking reports that are to be generated to analyze security violations
* The individual(s) responsible for reviewing all logs and reports

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Compliance:

Failure to comply with this or any other security policy will result in disciplinary actions as per the HR XXXXX Policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s):

Procedure(s) related to Information System Activity Review include:

* Security Incident Procedures

Form(s): None

References:

* The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
* International Standards Organization (ISO 27002).

Contact:

John Doe, Security Officer

1234 Anystreet

Anywhere, WY XXXXX

E: John.doe@anywhere.com

P: 307.XXX.XXXX

F: 307.XXX.XXXX

Policy History: Initial effective date: July 1, 2015