[Insert Company Name Or Logo]	
Title: Information System Activity Review	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: [Insert Local Gov/K-12 Name] is committed to safeguarding the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, our organization shall review logs of access and activity to detect, report, and guard against:

1. Network vulnerabilities and intrusions.
2. Breaches in confidentiality and security of data.
3. Performance problems and flaws in applications.
4. Improper alteration or destruction of data (information integrity).

This policy has been developed to address the organization-wide approach to information system log review processes. Departments and business units shall work with the Security Officer and/or IT to develop specific procedures based on applications and systems for review processes.

Scope: This policy applies to organizational information applications, systems, networks, and any computing devices, regardless of department ownership [e.g., owned, leased, contracted, and/or stand-alone).

Definitions:

1. Log Review: The internal process of reviewing information system access and activity (e.g., logins, file accesses, and security incidents.) A review may be done as a periodic event, because of a complaint, or suspicion of employee wrongdoing. Review activities shall also take into consideration the organization's information system risk analysis results.
2. System Logs: Records of activity maintained by the system which provide:
    a. Date and time of activity
    b. Origin of activity
    c. Identification of user performing activity
    d. Description of attempted or completed activity
3. Review Trail: A means to monitor information operations to determine if a security violation occurred by providing a chronological series of logged computer events (review logs) that relate to an operating system, an application, or user activities. Review trails provide:

a. Individual accountability for activities such as an unauthorized access of sensitive and regulated data.
b. Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information.
c. Problem analysis such as an investigation into a slowdown in a system's performance.
d. Other data as needed based on [Insert Local Gov/K-12 Name] objectives.
e. A review trail identifies who (login) did what (create, read, modify, delete, add, etc.) to what (data) and when (date, time).

4. Trigger Event: Activities that may be indicative of a security breach that require further investigation.

Policy:

[Insert Local Gov/K-12 Name] Security Officer or designee will review logs of access and activity of applications, systems, and networks and address standards set forth by the NIST Cybersecurity Framework and other cybersecurity best-practice frameworks to safeguarding the privacy and security of sensitive and regulated data. This policy implements reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive or regulated data. Review activities may be limited by application, system, and/or network reviewing capabilities and resources. Our organization shall make reasonable efforts to maintain information privacy and security through a well-thought-out approach to reviewing activity logs, which is consistent with available resources.

Procedure:

Workforce Training, Education, Awareness and Responsibilities

1. Workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and sensitive and regulated data.
2. [Insert Company name] commitment to reviewing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. Workforce members are made aware of responsibilities regarding privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the reviewing process detect a workforce member's failure to comply with organizational policies.
3. Responsibility for reviewing information system access and activity is assigned to the Information Systems (IS) Department Leader, Information Security Officer, or designee. The responsible individual shall:
    a. Assign the task of generating reports for review activities to the individual responsible for the application, system, or network.

b. Assign the task of reviewing the logs to the individual responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task.
c. Organize and provide oversight to a team structure charged with review compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).

4. [Insert Local Gov/K-12 Name] reviewing processes shall address access and activity at the following levels listed below. Reviewing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
    a. User: User level review trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and files, patients, and resources accessed.
    b. Application: Application-level review trails generally monitor and log user activities, including data files opened and closed, data accessed, specific actions, and printing reports.
    c. System: System level review trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
    d. Network: Network level review trails generally monitor information on current operations, penetrations, and vulnerabilities.
5. [Insert Local Gov/K-12 Name] shall determine the systems or activities that will be tracked or reviewed by:
    a. Focusing efforts on areas of greatest risk and vulnerability as identified in the information systems risk analysis and ongoing risk management processes.
    b. Maintaining confidentiality, integrity, and availability of applications and systems.
    c. Assessing the appropriate scope of system reviews based on the size and needs of the organization by determining:
        i. Information/sensitive or regulated data at risk.
        ii. Systems, applications or processes which are vulnerable to unauthorized or inappropriate access.
        iii. Activities that should be monitored (create, read, update, delete = CRUD).
        iv. Information to be included in the review record.
        v. Assessing available organizational resources.
6. [Insert Local Gov/K-12 Name] shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. The "events" may be applied to the entire organization or may be specific to a department, unit, or application. At a minimum, [Insert Local Gov/K-12 Name] shall provide immediate reviewing in response to:
    a. Employee complaint.

b. Suspected breach of confidentiality.
c. High risk or problem-prone event.
d. External report, such as from credit bureau or law enforcement.

7. [Insert Local Gov/K-12 Name] shall determine review criteria with a risk-based approach. This may include, but is not limited to, reviewing security risk analysis findings, experience, current and projected future needs, and industry trends and events. [Insert Local Gov/K-12 Name] will determine its ability to generate, review, and respond to review reports using internal resources. [Insert Local Gov/K-12 Name] may determine that external resources are also appropriate.
8. [Insert Local Gov/K-12 Name] shall designate the employees or contractors who are authorized to use security testing and monitoring tools. Such tools may not be used by anyone not specifically authorized. These tools may include, but are not limited to:
    a. Scanning tools and devices.
    b. War driving software.
    c. Password cracking utilities.
    d. Network or wireless packet capture utilities.
    e. Passive and active intrusion detection systems.
9. Other devices as determined by the organization.
10. Review documentation/reporting tools shall address, at a minimum, the following data elements:
    a. Authorizing official or policy, Application, System, Network, Department, and/or User Reviewed
    b. Review Type
    c. Individual/Department Responsible for Review
    d. Date(s) of Review
    e. Reporting Responsibility/Structure for Review Results
    f. Conclusions
    g. Recommendations
    h. Actions
    i. Assignments
    j. Follow-up
    k. The process for review of logs, trails, and reports shall include:
        vi. Description of the activity as well as rationale for performing review.
        vii. Identification of which workforce members or department/unit will be responsible for review (workforce members should not review logs which pertain to their own system activity unless there is no alternative).
        viii. Frequency of the reviewing process.
        ix. Determination of significant events requiring further review and follow-up.
        x. Identification of appropriate reporting channels for review of results and required follow-up.

11. Vulnerability testing software may be used to probe the network. Any publicly known vulnerabilities should be corrected. Re-evaluate whether the system can withstand attacks aimed at circumventing security controls.
    a. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, vendors providing IT services should not be reviewing their own services.
    b. Testing shall be done on a routine basis (e.g., annually).

Specific Review Requests

1. A request may be made for specific review. The request may come from a Human Resources, Risk Management, the Privacy Officer, the Security Officer and/or a member of administration.
2. A request for a review must include the time frame and nature of the request. The request must be reviewed and approved by [Insert Local Gov/K-12 Name] Privacy or Security Officer.
3. A request for a review because of a confidentiality concern shall be initiated by the Privacy Officer and/or Security Officer. Detailed review may be shared with the complainant. If this is done, a careful explanation must be given concerning the need for many individuals to have access to data.
    a. Should the review disclose that a workforce member has accessed a sensitive or regulated data inappropriately, the information shall be shared with the workforce member's supervisor/and or Human Resources Department to determine appropriate sanction/corrective disciplinary action.
    b. [Insert Local Gov/K-12 Name] may, but is not obligated to, share details of the logs with the complainant. Prior to communicating with the complainant, consider the need to collaborate with risk management and/or legal counsel for incidents of a more sensitive nature.

Evaluation and Reporting of Review Findings

1. System logs that are routinely gathered must be reviewed in a timely manner.
2. Reports of review findings will be limited to a minimum necessary/need to know basis. Legal or administrative counsel may need to be consulted.
3. There is no legal requirement to disclose the name of an individual who breached sensitive or regulated data. There is also no obligation to share the name of every individual that was involved in processing data. [Insert Local Gov/K-12 Name] may choose to disclose this information. If the organization chooses to provide a complete list of everyone that accessed sensitive or regulated data, it must be done with a careful explanation. Most people do not know how many individuals are involved in processing their data. When someone asks if a specific individual has accessed records, only that name should be disclosed.
4. The reporting process shall allow for meaningful communication of the review findings to the appropriate departments/units.

a. Significant findings shall be reported immediately in a written format. [Insert Local Gov/K-12 Name] security incident response form may be utilized to report a single event.
b. Routine findings shall be reported to the sponsoring leadership structure in a written report format.

5. Security reviews constitute an internal, confidential monitoring practice that may be included in the organization's performance improvement activities and reporting. Care shall be taken when releasing the results of the reviews. Review information, which may further expose organizational risk, should be shared with extreme caution. Generic security review information may be included in organizational reports.
6. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible and sponsoring departments/units.
7. If criminal activity is discovered during a review, it should be reported to appropriate law enforcement.

Reviewing Business Associate and/or Vendor Access and Activity

1. Periodic monitoring of business associate and vendor information system activity should be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between [Insert Local Gov/K-12 Name] and the external agency.
2. If it is determined that the business associate or vendor has exceeded the scope of access privileges, [Insert Local Gov/K-12 Name] leadership must reassess the business relationship.
3. If it is determined that a business associate has violated the terms of the business associate agreement, [Insert Local Gov/K-12 Name] must take immediate action to rectify the situation. Continued violations may result in discontinuation of the business relationship.

Review Log Security Controls and Backup

1. Review logs shall be protected from unauthorized access or modification, so the information they contain will be available if needed to evaluate a security incident.
2. Whenever possible, audit trail information shall be stored on a separate system. A separate system would allow the organization to detect hacking security incidents.
3. Review logs maintained within an application shall be backed-up as part of the application's regular backup procedure.
4. [[Insert Local Gov/K-12 Name] shall review internal back-up, storage and data recovery processes to ensure that the information is readily available in the manner required.

External Reviews of Information Access and Activity

1. Information system review reports gathered from contracted external review firms, business associates and vendors shall be evaluated, and appropriate corrective action

steps taken as indicated. Prior to contracting with an external review firm [Insert Local Gov/K-12 Name] shall:

a. Outline the review responsibility, authority, and accountability.
b. Choose a review firm that is independent of other organizational operations.
c. Ensure technical competence of the review firm staff.
d. Require the review firm's adherence to applicable codes of professional ethics.
e. Obtain a signed HIPAA-compliant business associate agreement.
f. Assign organizational responsibility for supervision of the external review firm.

Retention of Review Information

1. Review logs and audit trail report information shall be maintained based on organizational needs. There is no standard or law addressing the retention of review log/trail information. Retention of this information shall be based on:
    a. Organizational history and experience.
    b. Available storage space.
    c. Reports summarizing review activities shall be retained for a period of six years.

Violations:

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Attachments:

None

Related Policies:

Security Incident Response Policy