# Information Systems Audit Policy

## Overview

Audit controls and effective security safeguards are part of normal operational management processes to mitigate, control, and minimize risks that can negatively impact business operations and expose sensitive data.

2. Purpose

Regular operational, process, and security audits help to ensure that proper controls are sufficient and effective at providing information confidentiality, protecting Personally Identifiable Information (PII), ensuring system availability, and fostering a higher degree of data integrity. This policy sets forth [LEP]’s practice regarding [LEP] information system related audits.

## Scope

This policy applies to all [LEP] management and staff involved in the creation, deployment, operations, or support of application and system software used throughout the [LEP].

## Policy

### GENERAL

A regular and proactive audit policy helps to manage and reduce risks to [LEP]’s information systems, the data it manages, and the users it services. A security auditor is usually an external/independent third party (or at a minimum someone who is not operationally responsible for the area being audited), who evaluates systems for best practices and ensures compliance within an established set of requirements and controls.

The [Insert Appropriate Role] or their designee uses independent security audits to assist in ensuring security controls and safeguards are appropriate, sufficient, and effective at treating operational and security risks. Within this framework, the [Insert Appropriate Role] works with [LEP] management to define:

* **Resources** – Identify resources to perform the audit
* **Audit Scope** – Define the scope of the systems being certified and their boundaries
* **Requirements** – Prepare a list of security and/or privacy requirements that are relevant to the system
* **Description** – Technically and functionally describe the system including functional systems description, system operational environment, criticality, system architecture, interfaces, data flow, and any data privacy / system security requirements

### AUDIT SCOPE

The [Insert Appropriate Role] considers the following when determining organizational audit scope:

* **Security Vulnerabilities** – Identifies security vulnerabilities using reputable outside sources, and assign risk rankings (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.
* **Risk Evaluation** – Identifies methods for evaluating vulnerabilities and assigning risk ratings to systems. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. Vulnerabilities are considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or result in a potential security compromise or breach if not addressed. Examples of critical educational systems include premise security, pupil accounting, learning management, general financial, and personnel systems. It also includes any public-facing system, database, or transmission mechanism around sensitive information or PII.
* **Automated Tools** – Evaluates and recommends automated assessment tools and external resources that are suitable in identifying vulnerabilities including weak passwords, configuration issues, improper access controls, network penetration testing, and patch management issues.
* **Administrative Safeguards** – Defines protocols, policies, procedures, training plans and other administrative security controls (e.g. – these policies are a good example of a procedural control) useful to an auditor in comparing against a standard of operation.
* **Penetration Testing** – Evaluates whether penetration testing may be used to identify system vulnerabilities. Examples of penetration testing include evaluations of firewalls and other external network entry points, analysis of software applications and websites, review of logging and account procedures, social engineering tests of staff.

### AUDIT PROCEDURES

Access to audit tools shall be controlled and restricted to prevent possible misuse or compromise resources and log data. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to normal business operations.

Where possible, the [Insert Appropriate Role] shall use Certified Information Systems Auditors to audit the security controls of [LEP] systems. Audits shall be performed on a regular basis as defined by law, statute, or executive management protocol.

The auditor’s report shall include their project scope, findings, and recommendations to enhance security. The [Insert Appropriate Role] shall:

* Review the security auditor’s report to confirm the findings and verify the security recommendations are sufficient and effective.
* Convey the findings to the [Insert Appropriate Role] and appropriate [LEP] heads so that findings and resolutions can be reviewed, understood, and remedied.

The [Insert Appropriate Role] shall provide necessary reporting to executive management and the Board of Education.

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of day to day operations. Examples of controls and practices include:

* Departmental audit procedural documentation
* Software Tools and logs of usage related to penetration testing
* Procedures around audit processes and response
* Documented audit results, finding, action plans, and results
* Annual audit calendar schedules as appropriate

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/20/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |