Audit Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Security controls and safeguards are part of ABC Company’s risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

# II. Purpose

Security audits help ensure that security controls are sufficient and effective at providing information confidentiality, availability, and integrity.

# III. Scope

This policy applies to all Department Heads with authorized access to any of ABC Company’s Information Resources.

# IV. Policy

Security audits help manage and reduce risks to ABC Company’s Information Resources. A security auditor, usually an independent third party, evaluates systems for security best practices and compliance with an established set of security requirements.

An independent security audit assists the Chief Security Officer (CSO) in ensuring that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The CSO shall:

* Resources – identify resources to perform the security audit.
* Scope – define the scope of the system being certified as well as its boundaries.
* Security Requirements – prepare a list of the security requirements that are relevant to the system.
* Description – Describe the system including mission description, system identification, criticality, etc. Document the environment including facilities, physical security, maintenance, etc. Identify the system architecture, interfaces, data flow, etc. Describe the system security requirements.

The CSO shall consider the following when determining the audit scope:

* Vulnerabilities – establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact.
* Evaluating – identify methods for evaluating vulnerabilities and assigning risk ratings based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit sensitive data.
* Automated tools – automated tools may be used to identify a variety of vulnerabilities including weak passwords, configuration issues, improper access controls, and patch management issues.
* Administrative safeguards – the auditor can review and evaluate policies, procedures, training plans and other administrative security controls.
* Penetration testing – penetration testing may be used to identify system vulnerabilities. Examples of penetration testing include evaluations of firewalls and other network entry points, analysis of software applications and websites, and social engineering tests of Staff security education and awareness training.
* Internal vulnerability assessment – layers of defense help protect ABC Company’s internal systems should the external network perimeter be breached. Internal vulnerability assessments identify weaknesses in the network.

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

Where possible, the CSO shall use Certified Information Systems Auditors to audit the security controls of ABC Company’s Information Systems. Security audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources.

The auditor’s report shall include their project scope, findings, and recommendations to enhance security. The CSO 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 Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The CSO shall document important findings in the Audit Log Form and The Risk Management Officer shall provide necessary reporting to ABC Company Executive Management.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Department Heads, CSO, Risk Management Officer, and those responsible for information system security.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.02, APO01.03, APO01.11, APO12.02, APO12.07, MEA03.01, MEA04.11

GDPR Article 32

HIPAA 164.308(a)(8)

ISO 27001 9.2, A.15.2.1

NIST SP 800-37 3.5

NIST SP 800-53 3.3, AC-5, AU-6, CA-2

NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2

PCI 2.2.a-d