|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Audit and Compliance Assessment Policy | | | | | |
| Policy # | CPL-03-04 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

**Table of Contents**

[Purpose 1](#_Toc457887101)

[Scope 1](#_Toc457887102)

[Policy 1](#_Toc457887103)

[Audit Planning 1](#_Toc457887104)

[Audit Program Contents 2](#_Toc457887105)

[Key Controls 2](#_Toc457887106)

[Independence 2](#_Toc457887107)

[Audit Reports 2](#_Toc457887108)

[Technical Compliance Checking 2](#_Toc457887109)

[Review and Response 3](#_Toc457887110)

[Independent Review of Information Security 3](#_Toc457887111)

[Violations 3](#_Toc457887112)

[Definitions 3](#_Toc457887113)

[References 4](#_Toc457887114)

[Related Documents 4](#_Toc457887115)

[Approval and Ownership 4](#_Toc457887116)

[Revision History 4](#_Toc457887117)

Purpose

This policy defines the requirements for the audit and compliance assessment for all Company X computer and communications information system assets.

Scope

This policy applies to all Company X computer systems and facilities, with a target audience of Company X Executive Management, Information Technology employees and partners.

Policy

### ****Audit Planning****

**Plan Development – Company X must develop an information systems audit plan that defines the requirements and scope of audit activities.**

**Appropriate Scope - Auditors must perform audits and maintain reports that are commensurate with the size, activities performed by, and risk profile of the organization.**

**Audit Tool Protection - Information systems audit tools must be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.**

### ****Audit Program Contents****

**Audit Program Requirements - The Company X information system audit program requires management approval of all audit requirements.**

**Scope Approval – Company X management must approve the scope of all audit checks defined within the A Company X information system audit program.**

**Audit Check Access - The Company X information system audit program must limit all audit checks of software and data to read-only access.**

**Extended Access - The Company X information system audit program must only support extended access (greater than read only) for isolated copies of system files, which must be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.**

**Audit Resources - The Company X information system audit program must explicitly identify and make available the resources required.**

**Monitoring and Logging - The Company X information system audit program must require all access is monitored and logged to produce a reference trail.**

**Documentation - The Company X information system audit program must document all procedures, requirements, and responsibilities.**

**Independence – The Company X information system audit program must requires that the person(s) carrying out the audit be independent of the activities audited.**

### ****Key Controls****

**Identification of Key Controls - Key controls, systems, and procedures of the Company X information security program must be identified and documented.**

**Testing of Key Controls - Key controls, systems, and procedures of the Company X information security program must be regularly tested by independent third parties or qualified independent staff in accordance with the risk assessment.**

**Testing Frequency - The nature and frequency of testing of key controls, systems, and procedures of the Company X information security program must be consistent with the risk assessment and must consider the rapidly evolving nature of threats to computer security.**

### ****Independence****

**Testing Staff - Testing of the Company X information security program must be conducted by internal staff or consultants that are independent of those that develop operate or maintain the information security program.**

### ****Audit Reports****

**Report Findings - Audit findings and issues must include that any actions be reported by the auditors or management to the board of directors or audit committee.**

**Detailed Steps - Audit report work papers must disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the reports.**

### ****Technical Compliance Checking****

**Manual Compliance Checks - Manual technical compliance checking must be performed by an experienced system engineer.**

**Avoiding System Compromise - Management must develop and implement controls to ensure that penetration tests or vulnerability assessments do not lead to a compromise of the security of any Company X computer or communications system.**

**Planning and Documentation - All penetration tests or vulnerability assessments must be planned, documented and repeatable.**

**Expertise - Any technical compliance check performed on Company X computer and communications systems must only be executed by competent, authorized persons, or under the supervision of such persons.**

### ****Review and Response****

**Review Timing -Company X management must review the results of information security program tests within 30 days.**

**Corrective Actions - Company X management must take appropriate steps to address and correct the root cause of adverse results of information security program tests**

**Response Timing - A response to all control deficiencies from audits must be documented within 120 days of the audit findings.**

### Independent Review of Information Security

**Information System Control Reviews — Independent** - An independent and externally-provided review of information systems security must be periodically obtained to determine both the adequacy of and compliance with controls.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Information Shield reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Information Shield does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Information Shield reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

**Confidential Information (Sensitive Information)** – Any Information Shield information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Information Shield from a third party under a non-disclosure agreement.

**Information Asset –** Any Information Shield data in any form, and the equipment used to manage, process, or store Information Shield data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Partner –** Any non-employee of Information Shield who is contractually bound to provide some form of service to Information Shield.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**User -** Any Information Shield employee or partner who has been authorized to access any Information Shield electronic information resource.

References

CPL: 3.3 Audits and Compliance Assessment

ISO/IEC 27002: 18.2 Information security reviews

PCI-DSS: 12.8.4 Monitoring PCI DSS Status

HIPAA: Security Management Process - Information System Activity Review (R)

HIPAA: Compliance Evaluation 164.308(a)(8) (R)

NIST: Security Assessment and Authorization (CA)

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |