*Audit*

*and*

*Compliance Assessment Policy*

**Table of Contents**

[Purpose 1](#_Toc4059226)

[Scope 1](#_Toc4059227)

[Policy 1](#_Toc4059228)

[Audit Planning 1](#_Toc4059229)

[Audit Program Contents 2](#_Toc4059230)

[Key Controls 2](#_Toc4059231)

[Independence 2](#_Toc4059232)

[Audit Reports 2](#_Toc4059233)

[Technical Compliance Checking 3](#_Toc4059234)

[Review and Response 3](#_Toc4059235)

[Independent Review of Information Security 3](#_Toc4059236)

[Security Program Compliance 3](#_Toc4059237)

[Program Attestation 3](#_Toc4059238)

[Violations 4](#_Toc4059239)

[Definitions 4](#_Toc4059240)

[References 4](#_Toc4059241)

[Related Documents 5](#_Toc4059242)

[Approval and Ownership 5](#_Toc4059243)

[Revision History 5](#_Toc4059244)

Purpose

This policy defines the requirements for the audit and compliance assessment for all CompanyX (the “Company”) information system assets.

Scope

This policy applies to all CompanyX Information systems and facilities, with a target audience of CompanyX Executive Management, Information Technology employees and Third-Party.

Policy

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

**Plan Development – CompanyX 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****

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

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

**Extended Access - The CompanyX 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 CompanyX information system audit program must explicitly identify and make available the resources required.**

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

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

**Independence – The CompanyX 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 CompanyX information security program must be identified and documented.**

**Testing of Key Controls - Key controls, systems, and procedures of the CompanyX 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 CompanyX 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 CompanyX 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****

**Technical System Assessments** – All production information systems that store or process sensitive data must be evaluated for compliance with internal policies and baseline standards.

**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 CompanyX Information system.**

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

**Expertise - Any technical compliance check performed on CompanyX Information systems must only be executed by competent, authorized persons, or under the supervision of such persons.**

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

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

**Corrective Actions - CompanyX 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.

### Security Program Compliance

**Program Evaluation** – CompanyX management must monitor the status of compliance with the information security program. A report on the overall compliance must be produced at least once annually.

**Information System Control Reviews** – A review of information systems security must be periodically obtained to determine both the adequacy of and compliance with controls.

**Compliance Records** – As part of ongoing program compliance, CompanyX management must keep a record of compliance evidence and artifacts for a period of at least 5 year.

### Program Attestation

(Note: This requirements is becoming common and is part of NYS DFS: 500.02 (d) Management Attestation)

**Management Attestation** – As part of the review of the information security program, the Chief Information Officer will prepare a formal attestation of compliance with the controls of the information security program. This formal attestation must be classified for external distribution to third parties and regulatory agencies.

Violations

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

Any employee or Third-Party 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 CompanyX 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 CompanyX from a Third-Party under a non-disclosure agreement.

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

**Third-Party –** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002: 18.2 Information security reviews

PCI-DSS: 12.8.4 Monitoring PCI DSS Status

NIST: Security Assessment and Authorization (CA)

US-CSF: DE.CM: Security Continuous Monitoring

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 | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |