|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Information Security Organization | | | | | |
| Policy # | CPL-03-02 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

**Table of Content**

[Purpose 1](#_Toc457915162)

[Scope 1](#_Toc457915163)

[Policy 1](#_Toc457915164)

[Management Commitment to Information Security 1](#_Toc457915165)

[Information Security Planning 2](#_Toc457915166)

[Information Security Responsibility Assignment 2](#_Toc457915167)

[Department Responsibilities 2](#_Toc457915168)

[Contact with Authorities 3](#_Toc457915169)

[Contact with Special Interest Groups 3](#_Toc457915170)

[Employee Information Security Roles 3](#_Toc457915171)

[Role Delegation 4](#_Toc457915172)

[Violations 4](#_Toc457915173)

[Definitions 5](#_Toc457915174)

[References 5](#_Toc457915175)

[Approval and Ownership 5](#_Toc457915176)

[Revision History 5](#_Toc457915177)

Purpose

This policy defines the specific information security roles and responsibilities for implementing the Company X information security program.

Scope

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

Policy

### Management Commitment to Information Security

**Explicit Management Support** - Company X management must provide clear direction and visible management support for security initiatives.

**Information Security Management Committee** – Company X must create an information security management committee composed of senior managers or their delegates from each major Company X functional area.

**Program Review** – The Security Management Committee must meet [quarterly] to review the current status of information security at Company X, approve and later review information security projects, approve new or modified information security policies, and perform other necessary high-level information security management activities.

**Annual Information Security Strategy Report To Board** - The Information Security Department must prepare an annual strategy report for the Board of Directors describing the ways that internal information security efforts support strategic business directions, current business objectives, and major organizational projects.

**Policy-Driven Information Systems Security Architecture** - To assure that business goals and objectives are properly translated into information systems as well as the controls employed in these same information systems, Company X must employ a policy-driven information systems security architecture approach that is coordinated and managed by the Information Security Department, and integrated into the information security risk management process.

### Information Security Planning

**Information Security Resources** - Management must allocate sufficient resources and staff attention to adequately address information systems security.

**Centralized Information Security** - Guidance, direction, and authority for all information security activities are centralized for the entire organization in the Information Security Team.

**Information Security Liaisons** - Every department manager must designate an information security liaison and give this liaison sufficient training, supporting materials, and other resources to properly perform their job.

### Information Security Responsibility Assignment

**Defining Specific Security Roles** – Company X must define specific job roles required for the effective implementation of the Company X information security program. Each role must include a specific description of the information security-related duties performed by each team member performing those job functions.

**Defining Department Responsibilities** – To facilitate coordination and support for the information security function, the Information Security Manager or an approved delegate must define the specific duties of each department or organization unit (i.e. human resources, audit, Information Technology) that is required to support this effort.

**Assigning Specific Security Roles** – Company X must explicitly define at least one individual responsible for the duties of the information security specific roles.

**Assigning Security Officer** – Company X must explicitly define at least one individual responsible for the duties of the information security function. This role will be entitled “Information Security Manager.”

### Department Responsibilities

**Information Security Team** - Guidance, direction, and authority for information security activities are centralized for Company X within the Information Security Team. Information Security is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.

**Incident Response Team** - Investigations of system intrusions and other information security incidents are the responsibility of the Information Security Team.

**Internal Audit Team**- Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of the Information Technology Audit Team.

**Human Resources** - Disciplinary matters resulting from violations of information security requirements are handled by local managers working in conjunction with the Human Resources department.

### Contact with Authorities

**Contacting Law Enforcement** - Every decision about the involvement of law enforcement with information security incidents or problems must be made by a Company X senior partner in conjunction with the Information Security Manager.

**Relationships with Emergency Personnel and Law Enforcement** - As part of establishing the roles and responsibilities for both information systems contingency planning and information systems recovery, working relationships with local emergency personnel (fire and rescue, utilities, etc.) and law enforcement should be made prior to any contingency requiring them.

### Contact with Special Interest Groups

**Special Interest Groups** - Company X information security professionals must maintain memberships with security forums and professional associations to improve knowledge about best practices and staying up to date with relevant security information.

**Information Security Technical Training And Professional Development** - To ensure that information security technical staff members remain aware of important recent developments, each member must have an annual technical training and professional development plan. Company X management must provide a significant amount of paid time off so that these staff members can pursue parts of this plan, as well as participate in information security professional associations and special interest groups.

### Employee Information Security Roles

**Three Categories Of Responsibilities** - To coordinate a team effort, Company X has established three categories, at least one of which applies to each employee or third-party with access to sensitive information. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

**Owner Responsibilities** - Information Owners are the department managers, members of the top management team, or their delegates within Company X who bear responsibility for the acquisition, development, and maintenance of production applications that process Company X information. Production applications are computer programs that regularly provide reports in support of decision making and other business activities. All production application system information must have a designated Owner. For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

**Custodian Responsibilities** - Custodians are in physical or logical possession of either Company X information or information that has been entrusted to Company X. While Information Technology department staff members clearly are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

**User Responsibilities** - Users are responsible for familiarizing themselves with and complying with all Company X policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information.

**Information Owner Training** - The Information Security department will provide Owners with training, reference material, and consulting assistance so that they may appropriately make these and related decisions and distinctions. Owners also must make decisions about the permissible uses of information including relevant business rules. Owners are responsible for choosing appropriate information systems, and relevant controls for information handled by these systems, consistent with policies and standards issued by the Information Security department [an intranet link to these policies can be inserted here]. For example, Owners must define the validation rules used to verify the correctness and acceptability of input data. These validation rules and other controls for protecting information must be formally approved in writing by the relevant Owner before major modifications can be made to production application systems. Owners must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security-related control deficiencies pertaining to the information for which they are the designated Owner.

### Role Delegation

**Owner Delegation** - An Owner’s roles and responsibilities may be delegated to any full-time manager in the Owner’s business unit. An Owner’s roles and responsibilities may not be assigned or delegated to contractors, consultants, or individuals at outsourcing organizations or external service bureaus.

**Designating Custodians** - Owners are responsible for identifying all those individuals who are in possession of the information for which they are the designated Owner. These individuals by default become Custodians. Although special care must be taken to clearly specify security-related roles and responsibilities when outsiders are involved, it is permissible for Custodians to be contractors, consultants, or individuals at outsourcing organizations or external service bureaus.

**Designating Users** - Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements, such as non-disclosure agreements, have been made [a link to a non-disclosure form could be inserted here]. All users must be known to and authorized by Owners.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X 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, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Confidential Information (Sensitive Information)** – Any Company X 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, confidential litigation documents, medical records, and attorney-client privilege documents.

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

**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.

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

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

References

CPL: 3.0 – Information Security Organization

ISO 27002: 6. Organization of information security

HIPAA: Security Management Process 164.308(a)(1)

NIST: PL-1 Security Planning Policy and Procedures

PCI: R12. Maintain a security policy for all personnel

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 |  |
|  |  |  |  |  |