|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Security Awareness and Training Policy | | | | | |
| Policy # | CPL-07-02 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc457845623)

[Scope 1](#_Toc457845624)

[Policy 1](#_Toc457845625)

[Management Responsibilities 1](#_Toc457845626)

[Security Policy Awareness 2](#_Toc457845627)

[Security Awareness and Training 2](#_Toc457845628)

[Security Awareness 2](#_Toc457845629)

[Advanced Technical Training 2](#_Toc457845630)

[Violations 3](#_Toc457845631)

[Definitions 3](#_Toc457845632)

[References 3](#_Toc457845633)

[Related Documents 3](#_Toc457845634)

[Approval and Ownership 4](#_Toc457845635)

[Revision History 4](#_Toc457845636)

Purpose

This policy defines the information security-related requirements for training all personnel at Company X with access to sensitive information.

Scope

This policy applies to all Company X employees and third parties with access to information assets and systems.

Policy

### ****Management Responsibilities****

**Specification Of Minimum Information Security Training** - The Information Security Department must specify a minimum set of training and awareness raising requirements for all workers, for all workers who have access to Company X information systems, and for all workers who are in computer-related positions of trust. Managers must additionally make sure that their direct reports have sufficient training and technical skills to be able to securely operate Company X information systems to which they have been granted access.

**Security Training Time** - Management must allocate sufficient on-the-job time for workers to acquaint themselves with Company X security policies, procedures, and related ways of doing business.

**Security Training Responsibility** - The Information Security Department must provide refresher courses and other materials to regularly remind workers about their obligations and responsibilities with respect to information security.

### Security Policy Awareness

**Information Security Policy Distribution** - On or before their first day of work, all new Company X workers must receive a copy of the information security policy (policies) and be made aware that they must comply with the requirements described in these policies as a condition of continued employment.

**Policy Compliance Agreement** - Every worker must understand the Company X policies and procedures about information security, and must agree in writing to perform his or her work according to these same policies and procedures.

**Information Security Policy Changes** - All Company X workers must receive prompt notice of changes in the Company X information security policy, including how these changes may affect them, and how to obtain additional information.

**Security Violations and Reporting - Users must be clearly informed about the actions that constitute security violations as well as informed that all such violations will be logged and how to properly report possible security incidents.**

### Security Awareness and Training

**Information Security Class** - Every worker must attend an information security awareness class within 5 days of the date when they began employment with Company X.

**Annual Training Update** - All employees and partners must complete an information security training course and pass a corresponding test on an annual basis.

**Information Security Training** - All workers must be provided with sufficient training and supporting reference material to permit them to properly protect Company X information resources.

**Training Verification Record** - To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

**Training Records List - Management must maintain a listing of the training provided to all users of Company X’s information assets.**

### ****Security Awareness Reminders****

**Security Awareness Reminders** - All Company X employees and contractors must be regularly or continually exposed to information security awareness techniques (e.g., posters, awareness tools, periodic e-mail, warning messages, tips of the day upon accessing an information system, computer/information security day events).

### Advanced Technical Training

**Technical Training And Continuing Education** - All technical information systems staff must have sufficient initial training as well as continuing education in all critical aspects of their jobs including security, quality assurance, and customer relations.

**Technical Training And Apprenticeship** - Systems Administrators at Company X may be placed in a position of responsibility for production information systems only after they have completed training approved by the Information Security Manager which adequately prepares them for the tasks they will perform. Before they take on this responsibility they must also have satisfactorily completed a period of three months apprenticeship with a senior Systems Administrator.

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, 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 Company X from a third party under a non-disclosure agreement

**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.

**System Administrator –** An employee or partner who is responsible for managing a Company X multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

Third Party (Partner) – 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: 7.2 Security Awareness and Training

ISO/IEC 27002 - 7.2.2 Information security awareness, education, and training

NIST: Awareness and Training (AT)

PCI-DSS: 12.6 Security Awareness

HIPAA: Security Awareness and Training 164.308(a)(5)

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 | 04/01/2014 |  |
|  |  |  |  |  |