*Security Awareness and Training*

*Policy*

Table of Contents

[Purpose 1](#_Toc3882339)

[Scope 1](#_Toc3882340)

[Policy 1](#_Toc3882341)

[Management Responsibilities 1](#_Toc3882342)

[Security Policy Training 1](#_Toc3882343)

[Security Awareness and Training 2](#_Toc3882344)

[Security Awareness 2](#_Toc3882345)

[Advanced Technical Training 2](#_Toc3882346)

[Violations 3](#_Toc3882347)

[Definitions 3](#_Toc3882348)

[References 3](#_Toc3882349)

[Related Documents 3](#_Toc3882350)

[Approval and Ownership 3](#_Toc3882351)

[Revision History 4](#_Toc3882352)

Purpose

This policy defines the information security-related requirements for training all personnel at CompanyX (the “Company”) with access to sensitive information.

Scope

This policy applies to all CompanyX employees and Third-Parties (personnel) with access to information or systems.

Policy

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

**Role-Based Information Security Training** - The Information Security Department must specify a minimum set of training and awareness raising requirements for all personnel, for all personnel who have access to CompanyX information systems, and for all personnel 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 CompanyX information systems to which they have been granted access.

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

### Security Policy Training

**Information Security Policy Distribution** - On or before their first day of work, all new CompanyX personnel 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.

**Security Policy Agreement** – All personnel must understand the CompanyX 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 CompanyX personnel must receive prompt notice of changes in the CompanyX 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.**

### Information Security Training

**Information Security Class** – All personnel must attend an information security awareness class within 5 days of the date when they began employment with CompanyX.

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

**Information Security Training** - All personnel must be provided with sufficient training and supporting reference material to permit them to properly protect CompanyX 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 CompanyX ’s information assets.**

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

**Security Awareness Reminders** - All CompanyX personnel 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 CompanyX 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. 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-Parties that result from violation of this policy.

Any employee or contractor 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

**Personnel** – Any employee or third-party contractor with access to information or systems.

**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 - 7.2.2 Information security awareness, education, and training

NIST: Awareness and Training (AT)

PCI-DSS: 12.6 Security Awareness

US-CSF: PR.AT-1: All users are informed and trained

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 |  |  |
|  |  |  |  |  |