|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Personnel Security Management Policy | | | | | |
| Policy # | CPL-07 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

**Table of Content**

[Purpose 1](#_Toc442134102)

[Scope 1](#_Toc442134103)

[Policy 1](#_Toc442134104)

[Roles and Responsibilities 1](#_Toc442134105)

[Pre-Employment Screening 1](#_Toc442134106)

[Terms and Conditions of Employment 2](#_Toc442134107)

[Security Awareness and Training 2](#_Toc442134108)

[Personnel Transfers and Changes 2](#_Toc442134109)

[Personnel Terminations 2](#_Toc442134110)

[Violations 2](#_Toc442134111)

[Definitions 2](#_Toc442134112)

[References 2](#_Toc442134113)

[Approval and Ownership 2](#_Toc442134114)

Purpose

This policy defines the information security-related requirements that impact the hiring, ongoing management and termination of personnel at Company X.

Scope

This policy applies to all Company X employees and partners.

Policy

### ****Roles and Responsibilities****

**Job Descriptions** - Specific information security responsibilities must be incorporated into all worker job descriptions if such workers have access to sensitive information.

**Performance Evaluations** - Compliance with information security policies and procedures must be considered in all employee performance evaluations.

### Pre-Employment Screening

**Background Checks** - All workers to be placed in computer-related positions of trust must pass a background check. This process shall include examination of criminal conviction records, lawsuit records, credit bureau records, driver’s license records, and verification of previous employment.

**Prospective Employee Information** - Personal information about a prospective employee may not be gathered unless it is necessary to make an employment decision and relevant to the job. This policy addresses marital status, family planning objectives, off-hours activities, political affiliations, performance on previous jobs, previous employers, credit history, education, and other personal details.

**Revealing Information To Prospective Employees** - Information systems technical details, such as network addresses, network diagrams, and security software employed, must not be revealed to job applicants until they have signed a confidentiality agreement and also have been hired or retained.

### Terms and Conditions of Employment

**Security Policy 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.

**Non-Disclosure Agreements** - All workers must personally sign a Company X non-disclosure agreement before work begins. If a worker has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

**Intellectual Property Rights Agreement** - While employees of Company X, all staff members grant to Company X exclusive rights to patents, copyrights, inventions, and all other intellectual property they originate or develop.

**Code Of Conduct Acknowledgement** - All workers must indicate their understanding of the code of conduct by annually signing a form acknowledging that they agree to subscribe to the code.

**Conflicts of Interest** - All workers must avoid the actual or apparent conflict of interest in their business-related dealings with Company X. Should there be any doubt as to the existence of a potential conflict of interest, the worker must consult his or her manager.

### Security Awareness and Training

**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 Policy Distribution** - 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.

**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.

**Annual Information Security Class** - All employees and partners must complete an information security training course and pass a corresponding test on an annual basis. New workers must attend and pass the course within 15 days of the date when they begin employment with Company X.

**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.**

### ****Segregation of Duties****

**Separation of Request and Approval** - For any significant transaction, administrative procedure or change to Company X information systems falling under the scope of this policy, the one(s) approving the change must be separate from the one(s) initiating the request.

**Separate Security Administration Functions** - Accordingly, the functions of information technology security administration and the functions of security infrastructure changes are to be kept separate. All security administration processes are to be designed and implemented so that no one person, alone, can compromise a security control, either inadvertently or deliberately.

**Separation Of Duties** - Whenever a Company X computer-based process involves confidential valuable, or critical information, the system must include controls involving a separation of duties or other compensating control measures that ensure that no one individual has exclusive control over these types of information.

### Personnel Transfers and Changes

**Reporting Status Changes** - Employees have a duty to promptly report to their immediate manager all changes in their personal status which might affect their eligibility to maintain their current position. Examples of such status changes include convictions for job-related crimes and outside business activities.

### ****Personnel Terminations****

**Worker Termination Responsibility** - In the event that an employee, consultant, or contractor is terminating his or her relationship with Company X, the Company X Office Manager must ensure that all property in the custody of the worker is returned before the worker leaves Company X, notify all administrators handling the computer and communications accounts used by the worker as soon as the termination is known, and terminate all other work-related privileges of the individual at the time that the termination takes place.

**Involuntary Terminations** - In all cases where information technology support workers are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all Company X equipment and information, and escorted while they pack their belongings and walk out of Company X facilities.

**Recovery Of Organization Property** - Employees, temporaries, contractors, and consultants must not receive their final paycheck unless they have returned all hardware, software, working materials, confidential information, and other property belonging to Company X.

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 willful and deliberate conduct that is 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

**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 (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: 7.1. Personnel Security Management

ISO/IEC 27002: 7. Human Resources Security

NIST: Personnel Security (PS)

PCI-DSS: PCI: 12.6.1 Employee Training

HIPAA: Workforce Security 164.308(a)(3)

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 |  |
|  |  |  |  |  |