*Personnel Security Management Policy*

Table of Contents

[Purpose 1](#_Toc385339820)

[Scope 1](#_Toc385339821)

[Policy 1](#_Toc385339822)

[Roles and Responsibilities 1](#_Toc385339823)

[Pre-Employment Screening 2](#_Toc385339824)

[Terms and Conditions of Employment 2](#_Toc385339825)

[Security Awareness and Training 3](#_Toc385339826)

[Segregation of Duties 4](#_Toc385339827)

[Personnel Transfers and Changes 4](#_Toc385339828)

[Personnel Terminations 4](#_Toc385339829)

[Violations 5](#_Toc385339830)

[Definitions 5](#_Toc385339831)

[References 5](#_Toc385339832)

[Related Documents 6](#_Toc385339833)

[Approval and Ownership 6](#_Toc385339834)

[Revision History 6](#_Toc385339835)

Purpose

This policy defines the information security-related requirements that impact the hiring, ongoing management and termination of personnel at CompanyX (the “Company”).

Scope

This policy applies to all CompanyX employees and partners.

Policy

### **Roles and Responsibilities**

I**nformation Security** **Responsibility** - Responsibility for information security on a day-to-day basis is every worker's duty. Specific responsibility for information security is NOT solely vested in the Information Security Department.

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

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

**Personnel Record Distributions** - To permit each employee an opportunity to acquaint himself or herself with the information, and to ensure that it contains no errors, every employee must be given a copy of his or her personnel file once a year.

**Health And Safety Information** - Management must fully disclose to the involved workers the results of toxic substance tests and other information relating to the health and safety of workers.

**Worker Status Changes** - Every change in the employment status of CompanyX workers including, but not limited to, permanent employees, consultants, contractors, and temporaries, must be immediately reported by the individual's immediate manager to the Human Resources Department. The Human Resources Department must then immediately notify the involved information Systems Administrators.

### 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.

**Non-Employee Background Checks** - Temporaries, consultants, contractors, and outsourcing organization staff must not be given access to sensitive information, or be allowed to access critical information systems, unless they have gone through a background check commensurate with the background checks given to regular employees.

**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.

**Convicted Felons** - Job offers must not be extended to individuals who have been convicted of either a felony or other crimes involving violence that, if repeated, would pose a physical danger to CompanyX employees or property.

**Sensitive Product Information** - All workers who will have access to sensitive product information such as marketing plans, engineering specifications, or manufacturing procedures, must pass a standardized background check performed by the Human Resources Department.

### Terms and Conditions of Employment

**Required User ID Forms** - Users must sign both a confidentiality agreement and an information system security agreement prior to being issued a user ID permitting access to CompanyX systems.

**Property Rights** - Without specific written exceptions, all programs and documentation generated by, or provided by any worker for the benefit of CompanyX are the property of CompanyX. Management must ensure that all workers providing such programs or documentation sign a statement to this effect prior to the delivery of these materials to CompanyX.

**Non-Disclosure Agreements — Organization** - All workers must personally sign a CompanyX 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.

**Non-Compete Agreements** - At the time they join CompanyX, all employees must sign an agreement not to compete for six months after their separation from CompanyX.

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

**Compliance Agreement** - As a condition of continued employment, employees, consultants, and contractors must annually sign an information security compliance agreement.

**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 CompanyX. 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** - On or before their first day of work, all new CompanyX 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 Work Agreement** - Every worker 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 workers 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.

**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 CompanyX.

**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.**

### **Segregation of Duties**

**Separation of Request and Approval** - For any significant transaction, administrative procedure or change to CompanyX 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 CompanyX 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**

**Temporary Worker Transfers** - Workers who have given notice of their intention to leave the employment of CompanyX, as well as those who are aware of an impending involuntary employment termination, must be transferred to positions where they can do minimal damage to CompanyX assets. This policy also applies to those workers who are known to be disgruntled. At the worker's supervisor's option, these individuals may alternatively be placed on a paid leave of absence.

**Immediate Terminations** - Unless the special permission of a Senior Vice President is obtained, all workers who have stolen CompanyX property, acted with insubordination, or been convicted of a felony, must be terminated immediately. Such instant terminations must involve both escort of the individual off CompanyX premises, as well as assistance in collecting and removing the individual's personal effects.

**Worker Termination Responsibility** - In the event that an employee, consultant, or contractor is terminating his or her relationship with CompanyX, the worker’s immediate manager must ensure that all property in the custody of the worker is returned before the worker leaves CompanyX, 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.

**Notification Of Worker Terminations** - All employees must be immediately notified as soon as a worker has been terminated. With each such notice, the Human Resources Department must regularly remind employees that departed workers are no longer permitted to: be on CompanyX property (unless escorted by an employee), use CompanyX resources, or in any other way be affiliated with CompanyX.

**Notification To Third Parties Of Worker Terminations** - If a terminated worker had authority to direct contractors, consultants, or temporaries, or if this same worker had the authority to bind CompanyX in a purchase or another transaction, then the Human Resources Department must promptly notify all relevant third parties that the terminated worker is no longer employed by CompanyX.

**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 CompanyX equipment and information, and escorted while they pack their belongings and walk out of CompanyX facilities.

**Information Retention At Employment Termination** - Upon termination of employment, workers may not retain, give away or remove from CompanyX premises any CompanyX information other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other CompanyX information in the custody of the departing worker must be provided to the worker's immediate supervisor at the time of departure.

**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 CompanyX.

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 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, CompanyX reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

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

**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 CompanyX 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.

**User –** Any CompanyX employee or partner who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002: 7. Human Resources Security

NIST: Personnel Security (PS)

PCI-DSS: PCI: 12.6.1 Employee Training  
US-CSF: PR.AT-1: All users are informed and trained

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Author | Title |  |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title |  |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 |  |  |
|  |  |  |  |  |