|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Security Incident Management Policy | | | | | |
| Policy # | CPL-13 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457886447)

[Scope 1](#_Toc457886448)

[Policy 1](#_Toc457886449)

[Program Organization 1](#_Toc457886450)

[Computer Emergency Response Team (CERT) 2](#_Toc457886451)

[Roles and Responsibilities 2](#_Toc457886452)

[Program Communication 3](#_Toc457886453)

[Incident Response and Recovery 3](#_Toc457886454)

[Event Monitoring 3](#_Toc457886455)

[Reporting Information Security Events 4](#_Toc457886456)

[Events to Report 4](#_Toc457886457)

[Reporting to Third Parties 5](#_Toc457886458)

[Contact with Authorities 5](#_Toc457886459)

[Data Breach Management 5](#_Toc457886460)

[Incident Review 6](#_Toc457886461)

[Collection of Evidence 6](#_Toc457886462)

[Investigation and Forensics 6](#_Toc457886463)

[Violations 7](#_Toc457886464)

[Definitions 7](#_Toc457886465)

[References 8](#_Toc457886466)

[Related Documents 8](#_Toc457886467)

[Approval and Ownership 8](#_Toc457886468)

[Revision History 8](#_Toc457886469)

Purpose

This policy defines the requirements for reporting and responding to incidents related to Company X information systems and operations.

Scope

This policy applies to all employees and partners of Company X entities including, but not limited to, business units and subsidiaries.

Policy

### ****Program Organization****

**Computer Emergency Response Plans** - Company X management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service.

**Incident Response Plan Contents** - The Company X incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners. Specific areas covered in the plan include:

* Specific incident response procedures.
* Business recovery and continuity procedures.
* Data backup processes.
* Analysis of legal requirements for reporting compromises.
* Identification and coverage for all critical system components.
* Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers.

**Annual Incident Response Testing** - At least once every year, the Information Security Department must utilize simulated incidents to mobilize and test the adequacy of the Company X Computer Emergency Response Team.

### ****Computer Emergency Response Team (CERT)****

**Computer Emergency Response Team** - Information Technology Department management must organize and maintain an in-house computer emergency response team (CERT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins.

**Computer Incident Response Team Availability** - The Company X Computer Emergency Response Team must be available at all times to respond to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.

**Testing The Computer Emergency Response Team** - At least once every three months, the Information Security Department must utilize simulated incidents to mobilize and test the adequacy of the Company X Computer Emergency Response Team.

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

**Incident Management Responsibilities** - The individuals responsible for handling information systems security incidents must be clearly defined by the Information Security Manager. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents.

**Designated Contact Person for All Disasters And Security Events** - Unless expressly recognized as an authorized spokesperson for Company X, no worker may speak with the press or any other outside parties about the current status of a disaster, an emergency, or a security event that has been recently experienced.

**Providing Information In Legal Proceedings** - Workers are prohibited from providing any Company X records, or any copies thereof, to third parties outside of Company X or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of the Chief Legal Counsel has first been obtained. Likewise, workers are prohibited from testifying to facts coming to their knowledge while performing in their official Company X capacities, unless the prior permission of the Chief Legal Counsel has first been obtained.

### ****Program Communication****

**Display of Incident Reporting Contact Information** - Company X contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters and the intranet.

### ****Incident Response and Recovery****

**Intrusion Response Procedures** - The Information Technology Department must document and periodically revise intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

**Information Security Problem Resolution** - All information security problems must be handled with the involvement and cooperation of in-house information security staff, the Company X Computer Emergency Response Team, or others who have been authorized by the Company X Information Security Department.

**Security Changes After System Compromise** - Whenever a system has been compromised, or suspected of being compromised by an unauthorized party, System Administrators must immediately reload a trusted version of the operating system and all security-related software, and all recent changes to user and system privileges must be reviewed for unauthorized modifications.

**Suspected System Intrusions** - Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and predetermined procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

**Unauthorized Access Problems** - Whenever unauthorized system access is suspected or known to be occurring, Company X personnel must take immediate action to terminate the access or request assistance from the Corporate Information Systems Help Desk.

**Internal Investigations Information Confidentiality** - Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

**Legal Proceeding Participation** - Any Company X worker called by a subpoena or in any other manner called to appear or testify before a judicial board or government agency must immediately notify the chief legal counsel in writing about the call.

### ****Event Monitoring****

**Monitoring And Recording Usage Of Shared Computing Resources** - The usage of all Company X shared computing resources employed for production activities must be continuously monitored and recorded. This usage history data must in turn be provided in real-time to those security alert systems designated by the Information Security Department (intrusion detection systems, virus detection systems, spam detection systems, etc.).

**Intrusion Detection Systems** - On all internal servers containing sensitive data, Company X must establish and operate application system logs, intrusion detection systems, and other unauthorized activity detection mechanisms specified by the Information Security Department.

### ****Reporting Information Security Events****

**Incident Reporting** - All suspected information security incidents must be reported as quickly as possible through the approved Company X internal channels.

**Information Security Alert System** - Information Systems Department management must establish, maintain, and periodically test a communications system permitting workers to promptly notify appropriate staff about suspected information security problems.

**Violation And Problem Reporting Protection** - Company X will protect workers who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. This means that such workers will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

**Violation And Problem Reporting Identity** - Workers who report to the Information Security Department a security problem, vulnerability, or an unethical condition within Company X may, at their sole discretion, have their identity held in strict confidence. This means that the whistleblower's immediate supervisor, other members of the management team, as well as other Company X workers who are not directly involved in the receipt of the report, will not be given the whistleblower's identity.

### **Events to Report**

**Off-Site Systems Damage And Loss** - Workers must promptly report to their manager any damage to or loss of Company X computer hardware, software, or information that has been entrusted to their care.

**System Alerts and Warnings** - Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Systems Help Desk. Users are prohibited from utilizing Company X systems to forward such information to other users, whether the other users are internal or external to Company X.

**Unauthorized Activity** - Users of Company X information systems must immediately report to the Information Security Manager any unauthorized loss of, or changes to computerized production data. Any questionable usage of files, databases, or communications networks must likewise be immediately reported to the same manager.

**Unexpected Requests For Log-In Information** - Other than the regular and expected Company X log-in screens, users must be suspicious of all pop-up windows, web sites, instant messages, and other requests for a Company X user ID and password. Users encountering these requests must refrain from providing their Company X user ID and password, as well as promptly report the circumstances to the Help Desk.

**Missing Access Devices** - Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Information Security Department immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen--or are suspected of being lost or stolen--must be reported immediately.

**Unintended Sensitive Information Disclosures** - Unintended disclosures of sensitive Company X information are serious matters, and they must all be immediately reported to both the Chief Legal Counsel and the Information Security Manager. Such reporting must take place whenever such a disclosure is known to have taken place, or whenever there is a reasonable basis to believe that such a disclosure has taken place.

**Software Malfunctions** - All apparent software malfunctions must be immediately reported to line management or the information system service provider.

**Unauthorized Wireless Access Points** - If an unauthorized wireless access point is detected on the Company X network the Computer Incident Response Team must be notified.

### ****Reporting to Third Parties****

**External Violation Reporting** - Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with representatives from the Legal Department and the Information Security Department must weigh the pros and cons of external disclosure before reporting these violations.

**Reporting Suspected Security Breaches To Third Parties** - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

**Loss Or Disclosure Of Sensitive Information** - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Information Security Department must be notified immediately.

**System Vulnerability Exploitation And Victim Data** - Company X staff must not publicly disclose information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses. Likewise, the specific methods used to exploit certain system vulnerabilities must not be disclosed publicly.

### ****Contact with Authorities****

**Criminal Justice Community Contact** - Technical information systems staff must not contact the police or other members of the criminal justice community about any information systems problems unless they have received permission from the Chief Legal Counsel.

**Law Enforcement Inquiries** - Even if the requesting party alleges to be a member of the law enforcement community, Company X workers must not reveal any internal Company X information through any communications mechanism unless they have established the authenticity of the individual’s identity and the legitimacy of the inquiry.

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

**Requests To Cooperate In Investigations** - Company X workers must immediately report every request to participate in an information security investigation to the Chief Legal Counsel. Any sort of cooperation with the requesting party is prohibited until such time that the Chief Legal Counsel has determined that the participation is legal, is unlikely to cause problems for Company X, and is requested by an authorized party.

### ****Data Breach Management****

**Data Breach Response Plan Required** - Company X management must prepare, test and annually update a Data Breach Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

### ****Incident Review****

**Incident Response Plan Evolution - Lessons Learned** - The incident response plan must be updated to reflect the lessons learned from actual incidents.

**Incident Response Plan Evolution - Industry Developments** - The incident response plan must be updated to reflect developments in the industry.

**Violation And Problem Analysis** - An annual analysis of reported information security problems and violations must be prepared by the Information Security Department.

### ****Collection of Evidence****

**Computer Crime Or Abuse Evidence** - To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. The information to be immediately collected includes the current system configuration as well as backup copies of all potentially involved files.

**Evidence Storage** -The relevant information for computer investigation must then be securely stored off-line until official custody is given to another authorized person or the chief legal counsel determines that Company X will no longer need the information.

**Sources Of Digital Evidence** - For every production computer system, the Information Security Department must identify the sources of digital evidence that reasonably could be expected to be used in a court case. These sources of evidence must then be subject a standardized capture, retention, and destruction process comparable to that used for vital records.

**Responsibility for Electronic Evidence Production** - Company X will appoint a single individual responsible for coordinating the discovery and presentation of electronic evidence that may be required to support litigation.

**Information Classification** - Company X data that may be considered electronic evidence must be classified as CONFIDENTIAL and viewed only by authorized representatives of the CERT or approved third parties involved in the investigation.

### ****Investigation and Forensics****

**Computer Crime Investigation** - Whenever evidence clearly shows that Company X has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

**Extended Investigations** - Extended investigations of security breaches must be performed while the suspected worker is given leave without pay. The reason for a suspect’s leave without pay must not be disclosed to co-workers without the express permission of the Director of Security.

**Forensic Analysis Process** - Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.

**Investigation Status Reports** - The status of information security investigations must be communicated to management only by the lead investigator or the management representative of the investigation team.

**Computer Crime Investigation Information** - All evidence, ideas, and hypotheses about computer crimes experienced by Company X, including possible attack methods and perpetrator intentions, must be communicated to the Chief Legal Counsel and treated as restricted and legally privileged information.

**Information Security Investigations** - All Company X internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Manager.

**Information Security Investigation Teams** - Any person who personally knows the suspects, or who is friendly with them, for conflict of interest reasons is barred from participating on an information security incident investigation team.

**Intrusion Investigations Details** - Details about investigations of information system intrusions that may be still underway must not be sent via electronic mail. Likewise, to prevent such information from falling into the hands of intruders, files which describe an investigation now underway must not be stored on potentially compromised systems or anywhere on a related network where they could be reasonably expected to be viewed by intruders.

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

**Incident** - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [FIPS 200]

**Reported Event** – An “event” is a possible information security incident that has been reported or detected via automated event detection software. Events are analyzed to determine if they are part of a computer-related security incident.

**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: 13 Incident Detection & Management

ISO/IEC 27002: 16.0 Information Security Incident Management

NIST: Incident Response (IR)

HIPAA: Security Incident Procedures 164.308(a)(6)

PCI-DSS: 12.10 Incident Response Plan

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 | MM/DD/YYYY |  |
|  |  |  |  |  |