|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Third Party Security Management Policy | | | | | |
| Policy # | CPL-06 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457853000)

[Scope 1](#_Toc457853001)

[Policy 1](#_Toc457853002)

[Third Party Service Providers 1](#_Toc457853003)

[Third-Party Security Requirements 2](#_Toc457853004)

[Third-Party Access Control 2](#_Toc457853005)

[Information Exchange 2](#_Toc457853006)

[Third-Party Contracts 3](#_Toc457853007)

[Personnel Security 3](#_Toc457853008)

[Software Procurement 4](#_Toc457853009)

[Assessment, Monitoring and Audits 4](#_Toc457853010)

[Contingency Plans 5](#_Toc457853011)

[Foreign Countries 5](#_Toc457853012)

[Violations 5](#_Toc457853013)

[Definitions 6](#_Toc457853014)

[References 6](#_Toc457853015)

[Related Documents 6](#_Toc457853016)

[Approval and Ownership 6](#_Toc457853017)

[Revision History 6](#_Toc457853018)

Purpose

This policy defines the requirements for the management of third-party services that handle sensitive information for Company X in any manner.

Scope

This policy applies to all Company X computer systems and facilities, including those managed for Company X customers. This policy applies to all employees, partners and third-parties with access to Company X information assets.

Policy

### ****Third Party Service Providers****

**Third Party Vendor Inventory -Company X must annually perform an inventory of all third-party contractors used to store or process sensitive data.**

**Third Party Risk Profile - Company X must annually perform a risk-based profile assessment to classify all third-party vendor into one of three risk categories: High, Medium or Low. Each risk category will be assigned a specific set of validation requirements which are jointly defined by the Information Security Department and the Legal Department.**

**Third**-**Party Control Assignment** – Company X must keep a record of which (PCI-DSS) related controls are to be managed by each third-party and which will be handled in-house.

### ****Third-Party Security Requirements****

**Third-Party Risk Assessment** – The Information Security Department or an approved delegate must conduct an annual review of the information security risks of all third-parties with access to Company X sensitive information.

**Third Party Risk Assessment Team** – Company X must create a team of individuals responsible for performing third-party risk assessments. The team must consist of at least one member from the IT department and information security department.

**Third-Party Risk Screening** - When using a third-party contractor to manage information processing facilities, all risks must be identified in advance, mitigating controls must be established, and all contractor expectations must be incorporated into the contract for these services.

**Third-Party Information Security Responsibilities** - All Company X business partners, suppliers, customers, and other business associates must be made aware of their information security responsibilities through specific language appearing in contracts that define their relationship with Company X.

**Third-Party Security Policy Acknowledgement** - All Company X business partners, suppliers, customers, and other business associates must be made aware of the Company X security policies and agree to follow Company X information security policies.

**Security Requirements in Outsourced Network Services** - All third-party agreements with network service providers must contain define security requirements so that external networks are at least as secure as Company X internal networks.

### ****Third-Party Access Control****

**Third-Party Access Terms And Conditions** - Before any third-party is given access to Company X systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager at the third-party organization and be approved by Company X's Information Security Manager.

**Third-Party Access Approval** - Third-party access to any Company X internal computer systems that are not clearly public must be approved in advance by a designated information security coordinator.

**Third-Party User IDs** - Before a user ID can be issued to a third party, documentary evidence of an information security system or process must be provided to, and approved by, Company X's Information Security Manager and the third party must agree in writing to maintain this system or process to prevent unauthorized and improper use of Company X systems.

### ****Information Exchange****

**Third-Party Sensitive Information Handling** - All disclosures of secret, confidential, or private Company X information to third parties must be accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used.

**Third-Party Non-Disclosure Agreements** - Prior to sending any secret, confidential, or private information to a third party for copying, printing, formatting, or other handling, the third party must sign a Company X non-disclosure agreement.

**Third-Party Security Policy** - Before any sensitive Company X information is disclosed to a third party, this third party must sign a Company X confidentiality agreement and submit a copy of its information security policy for approval by Company X's Information Security Manager

**Receiving Third-Party Information** – If an agent, employee, consultant, or contractor is to receive secret or confidential information from a third party on behalf of Company X, this disclosure must be preceded by the third-party signature of a release form approved by the Legal Department.

**Information Handling At Contract Termination** - If Company X terminates its contract with any third-party organization that is handling Company X sensitive information, this same third-party organization must immediately thereafter destroy or return all of the Company X sensitive data in its possession.

**Third Party Information Disposal** - If the third-party destroys the information, Company X must receive notice that the data was disposed according to the procedures established or approved by Company X.

### ****Third-Party Contracts****

**Control Measures in Outsourcing Contracts** - All Information Technology outsourcing contracts must include specific words defining the control measures that will be provided and maintained. In addition, these contracts must specify a clear and expedient mechanism that Company X management can employ to immediately update these controls without bureaucratic delays, protracted negotiations, or outsourcing firm management objections.

**Outsourcing Contract Approvals** - All information-systems-related outsourcing contracts must be reviewed and approved by the Information Security Manager who is responsible for ensuring that these contracts sufficiently define information security responsibilities, how to respond to a variety of potential security problems and the right to terminate the contract for cause if it can be shown that the outsourcing organization does not abide by the information-security-related contractual terms.

**Reporting Third-Party Security Violations** - All outsourcing contracts must stipulate that the third parties must notify Company X immediately of any security incident likely to impact sensitive Company X information under their control. Company X will retain the right to aid in the investigation of these incidents.

**Outsourcing Security Violations** - All third-party outsourcing contracts must stipulate that the contract may be terminated due to information security violations by the outsourcing partner.

**Outsourcing Firm Penalties** - All outsourcing firm contracts must include fiscal penalties, approved by the Information Security Manager, for not maintaining information systems controls in a manner consistent with Company X requirements.

### Personnel Security

**Right to Approve Personnel for Key Outsourced Positions** - Company X has the right to approve or reject any personnel hired by third-parties and which will perform duties on Company X premises or handle Company X sensitive data. This requirement must be included in any contracts with third parties performing IT or security-related duties for Company X.

**Non-Employee Background Checks** - Temporaries, consultants, contractors, and other third-party 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.

**Third-Party Notice Of Worker Terminations** – If a terminated employee had authority to direct third-party contractors, or otherwise bind Company X in a purchase or another transaction, then Company X management must promptly notify all relevant third parties that the terminated worker is no longer employed by Company X.

**Personnel Cross Training with Key Outsourced Positions** - All key technical positions staffed by outsourced personnel must provide cross-training for in-house personnel for at least six months before contract expiration.

### ****Software Procurement****

**Software Integrity Statements** - If procurement of third-party software is being considered, management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise the software’s security, and will not require the modification or abandonment of controls found in the affected operating system.

**Third-Party Software Development** - All third parties who develop custom software on behalf of Company X must be bound by a contract approved by the Information Security Manager. This contract, at a minimum, must include a clear and explicit definition of property rights, licensing arrangements, functional requirements, security measures, escrow arrangements, auditing rights, and testing processes.

### ****Assessment, Monitoring and Audits****

**Independent Security Control Reports** - All agreements with third-party outsourcing organizations must stipulate that Company X will annually receive a report expressing an independent opinion about the adequacy of the controls in use at the outsourcing organization.

**Independent Security Scans of Outsourced Systems** - For all Company X product systems managed by third parties, Company X must hire a qualified, independent third party to validate the security of these systems.

**Critical Vendor Financial Review** - The Chief Information Officer (CIO) or an individual designated by the CIO must review the financial condition of vendors providing or supporting critical Company X production information systems annually.

**Third-Party Auditing Agreements** - All agreements dealing with the handling of Company X information by third parties must include a clause granting permission to Company X for the periodic auditing of the controls used for these information handling activities, and specifying the ways in which Company X information will be protected.

**Third-Party Notice Of Business And Technical Changes** - Arrangements with information systems outsourcing firms must be structured such that Information Technology Department and Information Security Department management both receive notices of all material changes in the outsourcing firm business and technical environment. Such notices must be received well in advance of such changes actually taking effect.

### ****Contingency Plans****

**Service Provider Contingency Plans** - All contracts with web site hosting organizations, application service providers, managed systems security providers, and other information systems outsourcing organizations must include both a documented backup plan and a periodic third-party testing schedule.

**Outsourced Production Systems Back-Out Plans** - An effective and regularly-tested back-out plan, that permits Company X to revert to internal processing and has been approved by the Information Security Manager, must be prepared and tested before any production information system processing may be transferred to an outsourcing organization.

**Continuity Service Level Agreements with Third Parties** - All agreements with third-parties, such as suppliers, service providers, and business partners, which could negatively impact the business processes of Company X must define service level agreements and require minimum standards of contingency planning and preparation on the part of these third parties.

**Priority Contingency Service in Agreements with Third Parties** - All agreements with third-parties -- such as suppliers, service providers, and business partners -- upon which the business processes of Company X will depend in an emergency or contingency and for whose attention Company X will likely have to compete with other entities, should specify the priority of service that the Company will require from the third party.

**Contract Failure Remedies** - In addition, the contract language of these priority and Service Level Agreements (SLA) should specify remedies to Company X in compensation for losses incurred by failure to put the Company’s needs at the specified priority or service level.

### ****Foreign Countries****

**Production Processing Outsourced To Foreign Companies** - Company X management must not outsource any aspect of production information systems management including, but not limited to, systems design, development, testing, operation, and maintenance to an organization that is based in a foreign country or owned by a foreign company.

**Sensitive Business Activities Performed In Foreign Countries** - Research, development, manufacturing, assembly, and strategic planning related to those Company X products which embody its most sensitive technology must not be performed in any foreign country. The definition of the products which fall into this category will be made by Company X's chief legal counsel.

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

**Third Party (Partner) –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**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.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 6.0 Third Party Security

ISO/IEC 27002: 15. Supplier relationships

HIPAA: Business Associate Contracts and Other Arrangement 164.308(b)(1)

NIST: SA-9 External Information System Services

PCI-DSS: 12.8 Service Provider Management

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 |  |
|  |  |  |  |  |