|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Systems Acquisition Security Policy | | | | | |
| Policy # | CPL-11-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457907092)

[Scope 1](#_Toc457907093)

[Policy 2](#_Toc457907094)

[System Planning and Requirements Definition 2](#_Toc457907095)

[System Purchasing and Supply Chain 2](#_Toc457907096)

[Supplier Review and Assessment 3](#_Toc457907097)

[System Documentation 3](#_Toc457907098)

[Violations 4](#_Toc457907099)

[Definitions 4](#_Toc457907100)

[References 5](#_Toc457907101)

[Related Documents 5](#_Toc457907102)

[Approval and Ownership 5](#_Toc457907103)

[Revision History 5](#_Toc457907104)

Purpose

The purpose of this policy is to facilitate the acquisition of information systems and related technology components that conform to Company X information security policies, standards and procedures. Unless Company X uses due-diligence in monitoring the acquisition of these systems, vulnerabilities can be introduced into the Company X networks and systems due to improper configurations or other lax security and privacy controls. Some of the risk factors mitigated within this policy include:

* Supply Chain Risks
* Insecure OS configurations
* Insecure software applications
* Software copyright licenses
* System Connectivity Risks
* Storage of sensitive data
* Testing with sensitive data
* Insufficient Logging Parameters

Scope

This policy covers all information technology hardware, software, and computer-related components that are purchased by Company X and process or store sensitive Company X data.

Specifically, the following Company X technology resources are within the scope of this policy:

* Application Software
* Configurable Hardware – Including Servers, Desktops, laptops, personal digital assistants, cell phones, and servers.
* Software running on the devices mentioned above.
* Peripheral equipment with electronic storage, such as printers and scanners.

(Note: This policy does not cover the purchase of other items that do not require or support configuration parameters. See the Company X Purchasing Policy for guidelines on purchasing these items. )

Policy

### System Planning and Requirements Definition

**Security Requirements Identification** - Before a new information system is developed or acquired, management of the involved user department, working with the Information Security Department, must have clearly specified and documented the relevant security requirements.

**Information Security Impact Analysis** - Whenever sensitive information is to be placed on newly acquired computer systems, a risk assessment of the potential security-related impacts must be performed. The results of the risk assessment must be reviewed by the Information Security Department before systems are purchased and deployed.

**Privacy Impact Reviews** - Every major systems acquisition project that could materially affect the privacy of individuals must be reviewed in advance by an independent committee, which must determine whether individuals will be placed at risk or at a disadvantage as a result of the project. If the committee determines that this may happen, they must then recommend remedial measures, perhaps including cancellation of the project.

**Business Applications Security Functionality** - Whenever feasible, third-party business systems must rely on system services for security functionality rather than incorporating such functionality into applications. Examples of system services include operating systems, network operating systems, database management systems, access control packages, front-end processors, firewalls, gateways, and routers. Any exceptions to this policy must be clearly documented as part of the production system documentation.

**Security Standards for Application Service Providers** - The Information Security Department must develop an associated Application Service Provider (ASP) Security Standards that sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use as an approved vendor.

### System Purchasing and Supply Chain

**Justification for Purchasing Information Security Solutions** - Company X must purchase commercially-available information security solutions rather than build the solutions in-house, unless the cost-effectiveness of an in-house solution has been clearly analyzed, documented, and approved by the Information Security Manager.

**Purchasing Requests** - All purchase requests for hardware, software, or computer-related components must first be approved by a department head (or designate) before submission to the IT department. Use the IT Purchase Request Form to detail and submit the request. In all cases, the request for purchase must be justified in the space provided on the *IT Purchase Request Form.*

**Supplier Diversity** - For every major information system, information system component and information system service purchase by Company X, Company X maintains at least one additional supplier of these components.

**Spare Components** – As part of the initial purchase of any information system, an additional spare component must be purchased for each additional critical system component. Stockpiling information system components and spares avoids the need to use less trustworthy secondary or resale markets in future years.

**Anonymous Purchasing** – For highly-sensitive information systems (including those that process or store TRADE SECRETS), Company X will purchase via a third party or other mechanism that hides the true identity of Company X from the vendor. This policy prevents information leakage through the supply chain which could lead to competitive intelligence about Company X purchases, and also protects against supply chain attacks.

### Supplier Review and Assessment

**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 Escrow** - If third-party software is to be used for critical business activity, the vendor must either license source code to Company X, or the vendor must provide accessibility to the source code through a software escrow agreement with a third party.

**Escrow Validation** - For each major release of software critical to Company X business and held in third-party escrow facilities, an independent third party must verify that all necessary software and documentation have been received by the escrow agent.

**Operating Systems Must Be Deemed Trustworthy** - Operating systems software may not be used for any Company X production system unless it has first been evaluated by a government agency and officially declared to be "trusted."

### System Documentation

**System Document Classification** - All Company X computer related documentation is confidential, and must be treated with the corresponding level of control for this type of information.

**Production Systems Documentation** - Every software or hardware system to be used for Company X production business activities must be clearly documented in advance of its deployment.

**Training And Operating Documentation** - Business application systems being acquired or substantially updated must not be moved into a production processing environment without having adequate training materials and operating documentation. The adequacy of these materials must be determined by management of the target business user group.

(Note: The following policies are related to NIST SA-5)

**Backups** - Monthly backups of information system documentation including security-related documentation must be conducted.

**Access Attempts** - Attempts to obtain information system documentation when such documentation is either unavailable or nonexistent must be documented.

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

**Custodian** - Guardian or caretaker of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Owner** - The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

**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.

.

**Privacy Impact Assessment** - An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Sanitization:** A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

**Security Impact Analysis** - The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

**System Baseline** - The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

**Trusted Computer System** - An information system employing sufficient hardware and software assurance measures to allow simultaneous processing of a range of sensitive information.

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

References

CPL: 11.01.01 System Acquisition

ISO 27002: 14.1 Security requirements of information systems

HIPAA: Organizational Requirements 164.314 (R)

PCI 2.2 Security Configuration Standards

NIST: System and Services Acquisition (SA)

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 | 04/01/2014 |  |
|  |  |  |  |  |