|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Application Development Policy | | | | | |
| Policy # | CPL-12-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457846415)

[Scope 1](#_Toc457846416)

[Policy 1](#_Toc457846417)

[Roles and Responsibilities 1](#_Toc457846418)

[Application Acquisition 2](#_Toc457846419)

[Application Development Specification 2](#_Toc457846420)

[Training Requirements 3](#_Toc457846421)

[Outsourced (Third Party Contractor) Development 3](#_Toc457846422)

[Secure Application Coding 4](#_Toc457846423)

[Application Security Requirements 4](#_Toc457846424)

[Open Source Software 4](#_Toc457846425)

[Application Testing 5](#_Toc457846426)

[Vulnerability Analysis and Testing 5](#_Toc457846427)

[Special Requirements for PCI-DSS 5](#_Toc457846428)

[Application Decommission and Disposal 6](#_Toc457846429)

[Documentation and Source Code 6](#_Toc457846430)

[Violations 6](#_Toc457846431)

[Definitions 6](#_Toc457846432)

[References 7](#_Toc457846433)

[Approval and Ownership 7](#_Toc457846434)

[Revision History 7](#_Toc457846435)

Purpose

This policy defines the Company X requirements for the secure development, testing and deployment of applications developed in-house or by third parties.

Scope

This policy applies to all Company X information assets and facilities, with a target audience of Company X management, Information Technology employees and partners.

Policy

### Roles and Responsibilities

**Employee Responsibilities** – All employees who are involved the specification, development, testing or documentation of Company X applications must be familiar with this policy.

**Manager Responsibilities** – Company X managers responsible for developing applications must assure that each development team member has read and understood this policy and is given the proper resources to implement the controls outlined in this policy.

**Information Security Department** – To support this policy, the Information Security department must delegate an individual responsible for being the liaison with the application development teams. This individual must possess specific knowledge about the risks of application development and specific secure development practices.

**Assigned Application Security Responsibility** – Each application developed or acquired by Company X must have a designated individual responsible for the overall security of the system. This designation must be included as part of all system documentation used during design and development.

### Application Acquisition

[Note: Organizations often fail into include information security requirements early in the development cycle. Any requests for proposal, or other project that requires bidding by contractors, should explicitly require security controls.]

**Security Requirements in RFP** – All Company X Requests for Proposal (RFP) or Requests for Information (FRI) must include basic information security requirements established by the Information Security Department.

### Application Development Specification

**Sensitive Data Review** – Each Company X application must include a review to identify any sensitive Company X data that will be processed as part of the application. A list of sensitive data types will be supplied by the Information Security Department and may include any of the following: Credit card numbers, Driver’s License Numbers, Financial Information, Health Records, other Personally Identifiable Information (PII).

**Security Requirements** – To reduce cost and maintain effective security, applications must be designed with security and privacy in mind. Each development specification document produced for Company X applications must include information security and data privacy requirements. Security and data privacy requirements must be identified as such within the specification document.

[Note: The Common Criteria methodology can provide a standard vocabulary and format for expressing the security requirements of a system. When an organization’s requirements are developed during the Acquisition/Development phase, the organization’s requirements regarding system performance are expressed as “specifications.” Because the CC does not observe the subtle difference between specification and requirement, some modification is necessary.]

**Security Department Review** – The information security and data privacy requirements within the application specifications and design must be reviewed with a member of the information security department.

**Initial Application Criticality Classification** – Each application built or acquired by Company X must have an initial application criticality classification. This rating will specify the overall level of security of the system, as well as the required recovery time for any system disruption.

**Document Sensitivity** – All specification, design, coding and testing documentation used in developing Company X applications must have an appropriate sensitivity label. By default, each document should be labeled for “CONFIDENTIAL: Internal Use Only”.

**Open Source and Third-Party Library Inventory** – Part of the required documentation for each Company X application is a list of all third-party software packages used within the application. These include but are not limited to linked libraries, database applications, and encryption packages.

**Encryption Algorithms** – If any Company X application (1) uses encryption libraries and (2) will export the application across any international boundary, the methods and types of encryption must be included within the documentation and reported to the Legal Department.

**Logging of Security Events** – All application code developed or purchased by Company X must produce a log of security-related events in an industry-standard format that supports monitoring by security audit programs.

### Training Requirements

[Note: Application security requires specialized training above and beyond training in traditional software development. To build and maintain secure applications, an organization must provide proper training to the individuals responsible for secure code development and auditing.]

**Training Required** - All employees involved in the coding of Company X business applications must receive training on secure coding principles.

**Certification Required** – At least one employee on each development team must receive a third-party certification in secure application development principles. The Manager responsible for application development will coordinate with the Information Security department to select a proper certification and cost estimates.

**Training Budget** - Company X management will establish an annual budget for application security training, including the non-vacation time required to perform the training and certification by chose employees.

### Outsourced (Third Party Contractor) Development

**Approval of Personnel** – Company X reserves the right of final approval for all contractors performing application development on Company X premises.

**Policy Acknowledgement** – All third-party contractors involved in the development of Company X applications must read and acknowledge understanding of the controls listed in this application security policy.

**Restrictions on Third-Party Libraries** – Only licensed software and in-house developed and authorized code (including government and contractor developed) shall be used on <system name(s)>. Public domain, shareware, or freeware software shall only be installed after prior written approval is obtained from the responsible development manager.

**Restricted Disclosure** - The contractor shall not publish or disclose in any manner, without the contracting officer’s written consent, the details of any safeguards either designed or developed by the contractor.

**Proof of License** - The contractor shall provide proof of license for all software used to perform development of this application and for all third-party libraries included within the application.

### Secure Application Coding

**Code Reviews** – Company X application development teams must perform periodic reviews of source code for possible security and privacy flaws. Reviewers must possess special training in application security techniques or use a third-party authorized to review application security.

**Source Code Labeling** – All programming source code developed by Company X employees must be considered proprietary to the company and must be labeled as “Trade Secret.”

**Secure Coding Methods** – All source code created by Company X developers must use secure coding methods approved by the development team and the Information Security Department.

**Automated Tools** – Company X will provide all development staff with access to automated vulnerability scanning tools which can assess source code for possible security flaws.

**Code Obfuscation** – All non-compiled, production source code used for web-based applications facing the public internet (such as PHP) must be “obfuscated” to hide the true business logic behind the application.

**Source Code Management** - All program source code used for Company X production systems must be stored in a secure source code management system with access controls approved by the Information Security Department.

### Application Security Requirements

**Input Data Validation And Rejected Item Handling** - All transactions to be input to a multi-user production computer system must be subjected to reasonableness checks, edit checks, or validation checks, and transactions that fail such checks must either be rejected with a notification of the rejection sent to the submitter, corrected and resubmitted, or suspended pending further investigation.

**Passwords Into Software** - Passwords must never be hard-coded in software developed by or modified by Company X workers.

**Secret User IDs Or Passwords** - Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.

**Private Data Number Usage** – Personal information considered Confidential (such as Credit card numbers or Social Security Numbers) must not be used for customer identification or any other purpose other than processing payments for goods and/or services.

### Open Source Software

**Conditions for Use of Open Source** - Company X must not employ open source software for any production information system unless this software has been available for at least six months, is known to have been used and tested by at least fifty other organizations, and also is issued by a reputable organization known to have an on-going commitment to providing timely upgrades, patches, and fixes.

**Open Source Software Widely Supported** - Company X production computers must not employ open source software unless this software is known to have passed a rigorous security testing process undertaken by an independent and reputable third party. Additionally, this same software is known to be readily supported by a wide variety of technical consultants from different organizations.

### Application Testing

**Testing Data Sets** – To maintain the security and privacy of its customers, Company X must limit the amount of sensitive data that gets duplicated, stored and transmitted. Applications that process sensitive Company X data (such as customer medical data, financial data, credit cards, etc.) testing must not use real customer data for testing purposes.

**Sanitized Data Sets** - Unless written permission is first obtained from the Information Security Department manager, all software testing for systems designed to handle private information must be accomplished with "sanitized" production information. Sanitized information is production information which no longer contains specific details that might be valuable, critical, sensitive, or private.

**Third-Party Testing** – Company X must not employ any third party to test applications which process sensitive data unless test data has been sanitized to mask the true customer data.

**Web Code Review Tools** - Prior to being moved to production status, all custom software to be run on web servers or commerce servers must be analyzed by web code review tools specified by the Information Security Department. All security vulnerabilities discovered by these tools must be fixed prior to cut-over to production operation.

**Test Data Removal** - Test data and accounts must be removed before a production system becomes active.

### Vulnerability Analysis and Testing

**Vulnerability Analysis before Release** – Before being released into production, all Company X business applications must undergo a vulnerability analysis and penetration test by either (1) a member of Company X staff trained under this discipline, or (2) a trusted third-party.

**Regular Vulnerability Analysis for Web-Based Production Applications** – All Company X web applications that are available to the public internet must have period monitoring for vulnerabilities by a trusted third-party. Vulnerability analysis must be based on, at a minimum, the most recent list of common vulnerabilities available from Open Web Application Security Project (OWASP).

### Special Requirements for PCI-DSS

[Applications that store or process credit card data are subject to the security requirements of the Payment Card Data Security Standard (PCI-DSS). In addition to code reviews, the following policies can address some of the PCI-DSS application requirements.]

**PCI Identification Required** – Any Company X application that will process, transmit or store credit cards must be clearly identified within the application development lifecycle as being subject to the requirements of the Payment Card Industry Data Security Standard (PCI-DSS).

**Quarterly Vulnerability Scan** – Any Company X application that will process, transmit or store credit cards must be subject to a vulnerability scan approved by the Information Security Department. This scan must be done at least quarterly.

**Web Application Firewall** – Any Company X application which can be accessed via the internet must include an application layer firewall approved by the Information Security Department.

### Application Decommission and Disposal

**Information Preservation** – Before any Company X product applications are taken out of production, a final backup of all sensitive production data must be preserved for at least three (3) years. Backup media that store this production data must contain a classification label which matches the highest (most sensitive) classification of the data being stored.

**Media Sanitization** – After any Company X application is taken out of production, all media which stores application code or data must be sanitized according to Company X media sanitization guidelines.

**Hardware/Software Disposal** – Hardware and other media which contained production application code or data must not be disposed or resold unless it has both (1) been properly sanitized and (2) has been approved by the Information Security Department.

### ****Documentation and Source Code****

**Systems Documentation Release** - Prior to being released to third parties, all documentation that describes Company X information systems or systems procedures must be reviewed and approved by the Information Security Manager.

**Documentation Confidentiality** - All Company X computer related documentation is confidential, and must not be taken elsewhere when a worker leaves the employ of Company X.

**Software Features And Functions Documentation** - All features and functions of software released to the public must be fully revealed in the documentation provided to users. Covert software features or functions are incompatible with the honest and forthright manner in which Company X conducts its business.

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

**Application** -A program or group of programs designed to perform a specific function directly for the user or, in some cases, for another application program.

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

**Sanitized Information** - Production information that no longer contains specific details that might be valuable, critical, sensitive, or private.

**System Administrator –** An employee or partner who is responsible for managing a Company X multi-user comp**u**ting 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.

References

CPL: 12.1.2. Application Development Security

ISO/IEC 27002: 14.0 Information Systems Acquisition, Development and Maintenance

PCI: R6. Develop and maintain secure systems and applications

NIST: System and Services Acquisition (SA)

HIPAA: Security Management Process 164.308(a)(1)

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 |  |
|  |  |  |  |  |