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

**Table of Content**

[Purpose 1](#_Toc457919064)

[Scope 1](#_Toc457919065)

[Policy 1](#_Toc457919066)

[Documented Operating Procedures 1](#_Toc457919067)

[System Planning and Requirements 1](#_Toc457919068)

[Segregation of Duties 2](#_Toc457919069)

[System Testing and Acceptance 2](#_Toc457919070)

[System Rollout and Delivery 3](#_Toc457919071)

[Encryption Management 3](#_Toc457919072)

[Violations 3](#_Toc457919073)

[Definitions 4](#_Toc457919074)

[References 5](#_Toc457919075)

[Approval and Ownership 5](#_Toc457919076)

[Revision History 5](#_Toc457919077)

Purpose

This policy defines the requirements for the secure operations and management Company X computer and communications systems.

Scope

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

Policy

### Documented Operating Procedures

**Standard Operating Procedures** - Operating procedures must be maintained and made available to all users who need them that document processing and handling of information.

### System Planning and Requirements

**New System Approval** - Prior to being placed into production use, each new, or significantly modified production system must be approved in advance by the Information Technology Department.

**Security Impact Statements** - Prior to being placed into production use, each new, or significantly modified, or enhanced business application system must include a brief security impact statement that has been prepared according to standard procedures.

**Privacy Impact Reviews** - Every major systems development or enhancement 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.

**Performance Requirements** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include performance requirements.

**Capacity Requirements** - Capacity requirements must be identified for each new and ongoing activity that requires the use of Company X information technology resources.

### Segregation of Duties

**Separation Of Duties** - Whenever a Company X computer-based process involves confidential 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.

**Systems Administrators Install/Update Server Software** - Only authorized Systems Administrators are permitted to install and/or update software on Company X servers.

### System Testing and Acceptance

**Sanitizing Software Testing Information** - 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.

**Externally-Provided Software Testing** - Executable programs provided by external entities must be tested in accordance with Company standards and must also be properly documented before installation on any Company X production system.

**Production System Written Approval** - Before being used for production processing, new or substantially changed business application systems must have received written approval from the Information Security Department Manager.

**Production Application Acceptance** - The acceptance and sign-off of the Information Technology Department, the involved user department, the Information Security Department, and Information Technology Audit Department must be obtained before a program will be granted production status on a multi-user computer.

**System Security Status Tools** - Every multi-user system must include sufficient automated tools to assist the Security Administrator in verifying the security status of the computer and must include mechanisms for the correction of security problems.

**User Processes, Sessions, And Files** - Company X systems administration staff may, at any time and without notice, alter the priority of, or terminate the execution of, any user process that it believes is consuming excessive system resources or is significantly degrading system response time, terminate user sessions or connections if this usage is deemed to be in violation of security policies or consuming excessive system resources, or remove or compress user disk files if it believes these files consume excessive disk space.

### System Rollout and Delivery

**Security Impact Statements** - Prior to being placed into production use, each new, or significantly modified, or enhanced business application system must include a brief security impact statement that has been prepared according to standard procedures.

**Software Conversion Contingency Plans** - Whenever the implementation of new or significantly modified production software introduces potential problems that could cause a loss to Company X of over [$1,000,000.00 USD] management must prepare a conversion-related contingency plan that reflects ways to insure continued service to potentially-affected users.

**Projects Involving Human Safety Issues** - All new application software projects that involve human safety risks must have a system development project manager’s signature on the testing approval forms prior to being used for production business purposes.

### ****Encryption Management****

**Standard Encryption Algorithm And Implementation** – Company X must only use encryption tools and algorithms that have been approved by the Information Technology Department.

**Publicly-Evaluated Encryption Algorithms** - Every general purpose encryption algorithm used to protect Company X production information and information systems must be open (that is, the specific mechanisms are publicly disclosed) and must have been evaluated by cryptography experts.

**User-Chosen Encryption Key Length** - Whenever user-chosen encryption keys are employed, the encryption system must prevent users from employing keys made-up of less than 10 characters.

**Systems Design Encryption Key Length** - Company X production system encryption systems employing symmetric algorithms must have a key length of at least 256 bits. Asymmetric algorithms must employ a key length which, in the estimation of the Information Security Team, provides a comparable level of security.

**Only Approved Cryptographic Libraries Used in Development** - All in-house or third-party developed applications must only use cryptographic controls documented and approved by the Information Security Team.

**At Least Two People With Access To Master Keys** - At all times, at least two trusted and authorized people must have access to the encryption master keys used to protect production information.

**Encryption Key Life** - Keys used for encrypting Company X data must be changed at least every 180 days.

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 willful and deliberate conduct that is 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

**Capacity Planning** - The process of determining the information processing capacity needed by an organization to meet changing demands for its products or services.

**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.

**Information Asset –** Any Company X data in any form, and the equipment used to manage, process, or store Company X data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**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.

**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.

**System Acceptance, User Acceptance** - The demonstrable willingness within a user group to employ information technology for the tasks it is designed to support.

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

**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: 11 Security Operations

ISO 27002: 14.1 Security requirements of information systems

HIPAA: Organizational Requirements 164.314 (R)

PCI 2.2 Security Configuration Standards

NIST: Planning (PL)

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 |  |
|  |  |  |  |  |