*IT Operations Security*

*Policy*

Table of Contents

[Purpose 1](#_Toc3901955)

[Scope 1](#_Toc3901956)

[Policy 1](#_Toc3901957)

[Documented Operating Procedures 1](#_Toc3901958)

[System Documentation 1](#_Toc3901959)

[System Planning and Requirements 2](#_Toc3901960)

[Segregation of Duties 2](#_Toc3901961)

[System Testing and Acceptance 3](#_Toc3901962)

[System Rollout and Delivery 3](#_Toc3901963)

[Change Control 3](#_Toc3901964)

[Review and Testing 4](#_Toc3901965)

[Separation of Development, Test, and Operational Facilities 4](#_Toc3901966)

[Equipment Maintenance 4](#_Toc3901967)

[Equipment Delivery and Removal 4](#_Toc3901968)

[Violations 5](#_Toc3901969)

[Definitions 5](#_Toc3901970)

[References 6](#_Toc3901971)

[Related Documents 6](#_Toc3901972)

[Approval and Ownership 6](#_Toc3901973)

[Revision History 6](#_Toc3901974)

Purpose

This policy defines the requirements for managing changes to any CompanyX (the “Company”) Information system.

Scope

This policy applies to all information security analysts and system Managers responsible for the maintenance of CompanyX Information systems.

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 Documentation

**System Security Plan** – Each major “system” (as defined by the Information Security Department) must have a written System Security Plan. The plan must be updated at least once annually.

**System Remediation Plan** – Each major “system” must have a documented remediation plan to address any control deficiencies found during audits or control evaluations.

### 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 CompanyX 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 CompanyX information technology resources.

### Segregation of Duties

**Separation Of Duties** - Whenever a CompanyX 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.

**Separation Of Duty Instructions** - Whenever practical, every task involving sensitive, valuable, or critical information, must require at least two people to coordinate their information- handling activities, including completing a task from beginning to end and approving the results of the work project.

**Systems Administrators Don`t Handle Security Administration** - To achieve proper separation of duties, for all CompanyX production systems, Systems Administrators must not attend to, or otherwise be responsible for, information systems security administration. Security administration must instead be handled by Information Systems Security Administrators.

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

**Job Rotation** - All computer-related workers in significant positions of trust must be rotated to another position every 18 months.

**Technical Staff Privileges** - Computer operations staff must not be given any access to production data, production programs, or the operating system beyond that which they need to perform their jobs.

### 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 CompanyX 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.

### System Rollout and Delivery

**Software Conversion Contingency Plans** - Whenever the implementation of new or significantly modified production software introduces potential problems that could cause a loss to CompanyX 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.

### ****Change Control****

(Note: See Change Management Policy for more detailed policies.)

**Change Control Procedure** - All Information systems used for production processing at CompanyX must employ a formal change control procedure to authorize all significant changes to software, hardware, communications networks, and related procedures.

**Change Control Documentation** - Production application change control documentation must be maintained so that management can readily determine exactly what changed and allow any and all prior versions of production applications to be readily recreated and pressed into service if necessary.

**Change Logging** - The details of all changes to CompanyX information processing operating system software must be logged.

### Review and Testing

**Security Patch Testing** - All security patches must be tested before they are installed on production CompanyX production Information systems. This must include, but not limited to the validation of all input to prevent cross-site scripting, injection flaws, and malicious file execution, proper error handling, secure cryptographic storage, secure communications, and proper role-based access control.

**Development Testing For Software Patches, Fixes, And Updates** - Vendor-supplied software patches, fixes, and updates must not be installed on any CompanyX production system unless they have first been tested in a development environment according to the requirements of the Systems Development Methodology.

### Separation of Development, Test, and Operational Facilities

**Development and Testing** **Separation** - Production business application software in development must be kept strictly separate from this same type of software in testing through physically separate computer systems or separate directories or libraries with strictly enforced access controls.

**Production And Development Separation** - Business application software in development must be kept strictly separate from production application software through physically separate computer systems, or separate directories or libraries with strictly enforced access controls.

**Test System Environment** - The test system environment must emulate the operational system environment as closely as possible.

**User Profiles on Test and Operational Systems** - Users must use different user profiles for operational and test systems, and menus must display appropriate identification messages to reduce the risk of error.

**System Utility Access** - Compilers, editors, and other development tools or system utilities must not be accessible from operational systems when not required.

**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.

### Equipment Maintenance

**Equipment Maintenance** - All information systems equipment used for production processing must be maintained in accordance with the supplier’s recommended service intervals and specifications, with all repairs and servicing performed only by qualified and authorized maintenance personnel.

**Maintenance Personnel** - All equipment maintenance must be performed by internal employees or a contracted and bonded outside service.

### Equipment Delivery and Removal

**Off-Site Equipment Approval** - Management must authorize the use of any CompanyX production computer equipment outside of company premises.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

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

**Emergency Change** - When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

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

**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.

**Scheduled Change** – A modification to the information processing infrastructure where formal notification was submitted, reviewed, and approved in advance of the change being made.

**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 CompanyX who is contractually bound to provide some form of service to CompanyX.

**Unscheduled Change** – A modification to the information processing infrastructure where formal notification was not submitted, reviewed, and approved in advance of the change being made. Unscheduled changes may be implemented to maintain system integrity and security in a timely manner to prevent an emergency situation.

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

References

ISO 27002: 12.1 Operational procedures and responsibilities

PCI 2.2 Security Configuration Standards

NIST 800-53: (SA) System and Services Acquisition Policy and Procedures

US-CSF PR.IP-3: Configuration change control processes are in place

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 | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |