*System Configuration Management*

*Policy*

Table of Contents

[Purpose 1](#_Toc3894763)

[Scope 1](#_Toc3894764)

[Policy 1](#_Toc3894765)

[Configuration Controls 1](#_Toc3894766)

[Remote Management 2](#_Toc3894767)

[Patches and Updates 2](#_Toc3894768)

[Vulnerability Management 3](#_Toc3894769)

[Change Detection Software 3](#_Toc3894770)

[Violations 3](#_Toc3894771)

[Definitions 3](#_Toc3894772)

[References 4](#_Toc3894773)

[Related Documents 4](#_Toc3894774)

[Approval and Ownership 5](#_Toc3894775)

[Revision History 5](#_Toc3894776)

Purpose

This policy defines the requirements for managing defaults configurations and changes to CompanyX (the “Company”) application, Information systems.

Scope

This policy applies to all CompanyX applications, Information systems, with a target audience of CompanyX Information Technology employees and Third-Parties.

Policy

### ****Configuration Controls****

**Baseline Standards** – All information systems placed into product must conform to minimum security configurations standards defined by the Information Security Department.

**Default Passwords** - All vendor-supplied default passwords must be changed before any Information system is used for CompanyX business.

**User ID Review** - Before any production multi-user computer operating system is installed at CompanyX, all privileged user IDs that are not assigned to a specific employee or Third-Party must be renamed or disabled.

**Unnecessary Software** - Software features that could be used to compromise security, and that are clearly unnecessary in the CompanyX computing environment, must be disabled at the time when software is installed on multi-user systems.

**Unnecessary Functionality** - All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed from the CompanyX Information infrastructure.

**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.

### ****Remote Management****

**Access Encryption** – All non-local access to CompanyX systems must be encrypted using methods approved by the Information Security Department. All web-based access must use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

**Local Administration** – All CompanyX critical product systems must be configured to only allow local administration.

### ****Patches and Updates****

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

**Software Patches, Bug Fixes, And Upgrades** - All CompanyX networked production systems must have an adequately-staffed process for expediently and regularly reviewing and installing all newly released systems software patches, bug fixes, and upgrades.

**Digital Signature And Source Approval For Patches** - Systems Administrators are authorized to patch software only if the software is downloaded, or otherwise received, from a trusted and recognized source approved by the Information Security Department. All patch software which comes with a digital signature must have its digital signature positively verified prior to being installed.

**Security Patch Installation** - All CompanyX Information system components and software must have the latest vendor-supplied security patches installed.

**Security Patch Installation Timing** - All critical new security patches must be installed on CompanyX Information systems within one month or receipt.

**Frequency Of Installing Non-Emergency Patches, Fixes, And Upgrades** - Management in charge of every production information system at CompanyX must establish a time period for the non-emergency periodic installation of patches, fixes, and upgrades to software. This time period must be based on the checklist of considerations provided by the Information Security Department.

**Documenting Reasons Why Patches And Fixes Were Not Installed** - If a patch or fix is not installed due to application conflicts or other incompatibilities, the involved Systems Administrator must promptly document the reason and forward the documentation to the Information Security Department. These unpatched or unfixed vulnerabilities must be addressed and resolved to the satisfaction of the Information Security Manager during the next information security review.

**Vendor-Provided Systems Software Installation** - Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers must go through the established CompanyX change control process.

**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.

### Vulnerability Management

**Vulnerability Advisories** - On a weekly or more frequent basis, systems administration staff must review all information security vulnerability advisories issued by trusted organizations for items affecting CompanyX systems.

**Vulnerability Identification Software** - To ensure that CompanyX technical staff has taken appropriate preventive measures, all systems directly-connected to the Internet must be subjected to an automated risk analysis performed via vulnerability identification software at least once a month.

**Scan Reviews** – The results of all vulnerability assessments of production computer operating systems must be reviewed by technical personnel. All high-risk vulnerabilities must be addressed.

**Scanning Personnel** – All internal vulnerability scans on CompanyX production systems must be performed by qualified personnel who are properly trained in vulnerability management.

**Vulnerability Advisories** - On a weekly or more frequent basis, systems administration staff must review all information security vulnerability advisories issued by trusted organizations for items affecting CompanyX systems.

**Security Special Interest Groups** - CompanyX Information Security professionals must maintain memberships with security forums and professional associations to receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities.

### Change Detection Software

(PCI-DSS 11.5)

**System Integrity Checking Software** - All CompanyX servers must run, at the very least on a weekly basis, integrity checking software that detects changes in configuration files, system software files, application software files, and other system resources.

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

**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 –** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**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 CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002 - 14.2 Security in development and support processes

NIST: Configuration Management (CM)

PCI-DSS: R2. Do not use vendor-supplied default passwords

US-CSF: PR.IP-1: A baseline configuration of information technology/operational technology systems

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 |  |
|  |  |  |  |  |