*Remote*

*Access Security Policy*

Table of Contents

[Purpose 1](#_Toc3883250)

[Scope 1](#_Toc3883251)

[Policy 1](#_Toc3883252)

[Program Requirements 1](#_Toc3883253)

[Documentation and Process 2](#_Toc3883254)

[Server Configuration 2](#_Toc3883255)

[Authentication and Access 2](#_Toc3883256)

[Data Integrity 2](#_Toc3883257)

[Server and Device Management 2](#_Toc3883258)

[Remote Access Devices 3](#_Toc3883259)

[Client Software 3](#_Toc3883260)

[Violations 3](#_Toc3883261)

[Definitions 4](#_Toc3883262)

[References 4](#_Toc3883263)

[Related Documents 4](#_Toc3883264)

[Approval and Ownership 5](#_Toc3883265)

[Revision History 5](#_Toc3883266)

Purpose

This policy defines the requirements for establishing the framework and ongoing management of the CompanyX (the “Company”) remote access infrastructure.

Scope

This policy applies to all remote access systems, i.e., servers, devices and all things related, that are configured and implemented to remotely access any CompanyX Information systems or networks. The target audience of this policy is all CompanyX employees who have remote access management responsibilities or who have been given remote access to any CompanyX Information system.

Policy

### Program Requirements

**Remote Access Strategy Development** - Prior to permitting or implementing any remote access to CompanyX Information systems a detailed analysis must be performed that includes an examination of the risks associated with each solution.

**Remote Access Strategy Testing** - Before implementing a remote access solution a prototype of the design must be tested and evaluated for security and performance compatibility.

**Integrated Remote Access Strategy** - The security aspects of the remote access solution design must be documented in the CompanyX system security plan.

### Documentation and Process

**Remote Access Processes** - Operational processes must be regularly performed to maintain the security of the remote access infrastructure.

**Remote Access Assessments** - Audits or assessments must be performed at least annually to ensure that the CompanyX remote access policies, processes, and procedures are being followed.

### Server Configuration

**Remote Access Server Isolation** - CompanyX remote access servers must not be run on the same host as other services and applications.

**Remote Access Server Placement** - Remote access servers must be placed at the network perimeter unless there are compelling reasons to do otherwise.

### Authentication and Access

**Two-Factor User Authentication** -All in-bound access through a public network to every CompanyX computer must employ two-factor user authentication with at least one of the factors not subject to replay.

**Remote Access Passwords** - User IDs with blank or null passwords (passwords with no characters) must not be permitted to gain remote access to any CompanyX computer or network.

### Data Integrity

**Secret Data Transmission** - All CompanyX sensitive data transmitted over any communication network must be encrypted.

**Standard Encryption Algorithm And Implementation** - If encryption is used, government-approved standard algorithms and standard implementations must be consistently employed.

**Transportable Computers With Sensitive Information** - All portables, laptops, notebooks, and other transportable computers containing sensitive CompanyX information must consistently employ both hard disk encryption for all files, as well as startup and screen-saver based boot protection.

**Remote Device Encryption Keys** - The creation and use of cryptographic keys for encrypting data stored on remote devices must follow the same CompanyX policies for encrypting data stored on non-remote systems.

### Server and Device Management

**Remote Access Server and Device Security** - All CompanyX remote access servers and devices must be kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators.

[**Remote Administration**](http://policyshield.com/policy/policydetail.php?id=1037)- Remote administration of Internet-connected computers must employ one-time passwords and must be performed only over encrypted links.

**Remote Access Device Management Training** - All CompanyX employees who are responsible for the management of any remote access devices must be trained to properly secure these devices.

**Remote Server and Device Disposal** - All sensitive information must be removed from any remote server or device prior to its disposal.

### ****Remote Access Devices****

**Remote Access Device and Access Levels** - A list of approved remote access devices and the permitted access level of each device must be documented, maintained and distributed in a controlled fashion.

**Remote Access Client Software Management** - Remote access client software must be configured to have all security features and settings remotely managed by a CompanyX system administrator.

**Remote Access Client Device Support** - Help desk personnel must be properly trained to support remote access users and the devices that are used.

### Client Software

**Remote Access Client Software Configuration** - Remote access client software must be configured to provide CompanyX with nearly complete control over the remote access environment.

**Security Standard for Home User Computers** -The CompanyX Information Security Department must issue a standard for the security configuration of home computers which employees use for remote access to CompanyX networks. The standard must include a list of required and prohibited software packages**.**

[**Remote Client Machines Automatically Disabled If Lost/Stolen**](http://policyshield.com/policy/policydetail.php?id=1162) - All portable computers containing CompanyX information must include software approved by the Information Security Department that will automatically erase the data resident on the machine after the machine has been reported to be lost or stolen.

**Personal Computer And Workstation Firewalls** -All personal computers and workstations that connect to the Internet through dial-up, digital subscriber line (DSL), integrated services digital network (ISDN), cable modem, or similar connections must have their own approved firewalls installed and continuously enabled.

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

**Confidential Information (Sensitive Information)** - Any CompanyX 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 CompanyX from a Third-Party under a non-disclosure agreement.

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

**Remote Access Device** - Any electronic mechanism that is used to connect and transmit information to and from a remote access server, e.g., personal and portable computers, personal digital assistants, smart phones, etc.

**Remote Access Server** - The computer and associated software that is set up to handle users seeking access to a network from a location that is not directly connected to that network. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

**Two-Factor Authentication** - A security process in which the user provides two means of identification, one of which is typically a physical token, such as a card or one-time password generator, and the other of which is typically something memorized, such as a security code that is directly associated with the token. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A common example of two-factor authentication is a bank card: the card, something you have, and the personal identification number (PIN), something you know.

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

References

ISO/IEC 27002: 6.2 Mobile devices and teleworking

NIST: AC-17 Remote Access

PCI-DSS: 12.3.9 Remote Access Technology

US-CSF: PR.AC-3: Remote access is managed

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 |  |
|  |  |  |  |  |