*Network Security Management Policy*

Table of Contents

[Purpose 1](#_Toc4679193)

[Scope 1](#_Toc4679194)

[Policy 1](#_Toc4679195)

[Firewalls and Traffic Control 1](#_Toc4679196)

[Network Perimeter 2](#_Toc4679197)

[System Authorization 2](#_Toc4679198)

[Network Configuration 2](#_Toc4679199)

[Network Diagrams 2](#_Toc4679200)

[System Configuration 3](#_Toc4679201)

[Access Control 3](#_Toc4679202)

[Third-Party Network Access 3](#_Toc4679203)

[Network Segregation 4](#_Toc4679204)

[Phones and PBX 4](#_Toc4679205)

[Domain Management 4](#_Toc4679206)

[Violations 5](#_Toc4679207)

[Definitions 5](#_Toc4679208)

[References 6](#_Toc4679209)

[Related Documents 6](#_Toc4679210)

[Approval and Ownership 6](#_Toc4679211)

[Revision History 6](#_Toc4679212)

Purpose

This policy defines the requirements for establishing the network controls related to the CompanyX (the “Company”Information systems infrastructure.

Scope

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

Policy

### ****Firewalls and Traffic Control****

**Internet Access** - All Internet access using computers in CompanyX offices must be routed through a firewall or similar device that provide firewall functionality.

**Network Traffic Restriction** - All inbound and outbound traffic must be restricted to that which is necessary for the CompanyX data environment.

### ****Network Perimeter****

**Boundary Protection** – All CompanyX networks that connect to the internet or other networks must be protected by a firewall.

**Intrusion Detection** – All networks which provide access to CompanyX production applications must be protected by an intrusion detection system (IDS) that is periodically updated to detect the latest threats.

**Firewall Management Definition** - Network configuration standards must include a description of groups, roles, and responsibilities for the logical management of firewalls and routers.

### ****System Authorization****

**Network Security Configuration** - Configurations and set-up parameters on all hosts attached to the CompanyX network must comply with in-house security policies and standards.

**New Network Connection Process** - All new network connections must be approved and tested prior to production implementation.

**Intranet Connection Security Criteria** - All Information systems and network segments must meet the security criteria established by the Information Security Manager including, but not limited to, having an acceptable firewall, an acceptable user-authentication system, an acceptable user privilege control system, an established change control process, a clearly-written definition of system management responsibilities, and adequate operational documentation, before it can be connected to the CompanyX intranet.

**Internal Network Access** - Only CompanyX provided computers will be able to access the CompanyX internal network. Computers owned by workers (even though these workers may be authorized to access the internal network), will not be able to log-in because these computers lack special software which is installed only on CompanyX provided machines.

### ****Network Configuration****

**Network Central Point Of Failure** - Management must design CompanyX communications networks so that no single point of failure could cause network services to be unavailable.

**Network Connection Configuration** - All internal networks must be configured such that they can prevent or detect attempts to connect unauthorized computers.

**Network Domains** - All large networks crossing national or organizational boundaries must have separately-defined logical domains, each protected with suitable security perimeters and access control mechanisms.

**Multiple Carriers** - Management must design CompanyX communications systems so that critical communications may immediately be sent through multiple long distance carriers over physically diverse routes.

**High-Security And High-Reliability Computers And Networks** - Every high-security and high-reliability system managed by or owned by CompanyX must have its own dedicated computers and networks, unless approved in advance by the Information Security Manager.

### ****Network Diagrams****

**Network Diagram** - A network diagram that illustrates all connections to components that process or store confidential information (including any wireless networks) must be developed and maintained.

**Hidden Internal Network Addresses** - The internal system addresses, configurations, and related system design information for CompanyX networked Information systems must be restricted such that both systems and users outside the CompanyX internal network cannot access this information.

**External Network Connection Inventory** - The Information Security Department must maintain a current inventory of all connections to external networks including, but not limited to, telephone networks, EDI networks, Internet trading Third-Party networks, wireless networks, extranets, and the Internet.

### ****System Configuration****

**Systems Interfacing External Networks** - All CompanyX systems interfacing external networks must be running the latest version of the vendor-supplied operating system software.

**Shared Directory Systems** - The use of shared directory systems on any CompanyX computer that is Internet connected or directly reachable through the Internet must be approved by the Information Security Manager.

**External Network Interfaces** - CompanyX systems designers and developers must restrict their usage of external network interfaces and protocols to those that have been expressly approved by the Information Security Manager.

### ****Access Control****

**Network Ports In Vacant Offices** - All network ports in vacant offices and other areas that are not customarily in use must be promptly disconnected at the wiring closet or at another centralized location.

**Internal Network Device Passwords** - All CompanyX internal network devices including, but not limited to, routers, firewalls, and access control servers, must have unique passwords or other access control mechanisms.

**Access Control System For Fax Machines, Copiers And Printers** - All computerized devices accessible via the CompanyX internal network must have an operational access control system approved by the Information Security Department. These devices include, but are not restricted to, fax machines, copiers, printers, routers, servers, and desktop personal computers.

**Real-Time External Network Connections** - All in-bound real-time external connections to CompanyX internal networks or multi-user Information systems must pass through an additional access control point.

**Unsecured Remote Computer Connections Denied** - At the time that they make a connection with the CompanyX internal network, all external computers will be automatically scanned to determine whether they have adequate security measures installed and operating. Computers that cannot be scanned, as well as those that are not adequately secured, will be denied network access.

### ****Third-Party Network Access****

**Network Connections with Outside Organizations** - The establishment of a direct connection between CompanyX systems and computers at external organizations, through the Internet or any other public network, must be approved by the Information Security Manager.

**Connecting Third-Party Networks** - CompanyX computers or networks must be connected only to Third-Party computers or networks after the Information Security Manager has determined that the combined system is in compliance with CompanyX security requirements.

### ****Network Segregation****

**Network Security Zones** - All CompanyX internal data networks must be divided into security zones.

**Public Internet Servers** - Public Internet servers must be placed on subnets, separate from internal CompanyX networks, and to which public traffic is restricted by routers or firewalls.

**Network Protocol Restriction** - All inbound and outbound traffic must be protected by a DMZ that permits only the protocols that are necessary for the CompanyX data environment.

**Inbound Internet Traffic Limitation** - Inbound Internet traffic must be limited to IP addresses within the DMZ.

**Internal Address Limitation** - The CompanyX network must be configured such that no internal addresses are permitted to pass from the Internet into the DMZ.

**Outbound Internet Traffic Limitation** - Outbound traffic from any subnet that contains confidential information must be limited to access IP addresses within the DMZ.

**Database Segregation** - Any database that contains confidential CompanyX information must be placed in an internal network zone, segregated from the DMZ.

**Walk-Up Network Connections** - All walk-up network access for visitors to connect back to their home networks must employ a separate subnet that has no connection to the CompanyX internal network.

### ****Phones and PBX****

**Communication Line Changes** - Workers and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not obtained approval from the Telecommunications Manager.

**Terminating Communications Lines As Soon As Possible** - Phone circuits must be terminated as soon as they are shown to be no longer used for business purposes.

### ****Domain Management****

**Internet Domain Name Registration** - Payments and paperwork for Internet domain name registrations for all of CompanyX official sites must be handled in a timely manner and promptly confirmed by the Information Technology Manager.

**Monitoring Shadow Internet Domain Names** - To reduce customer and prospect confusion, CompanyX must register and control all Internet domain names which might be confused with CompanyX's corporate name, trademarks, or service marks. The Telecommunications Manger must establish and maintain a process which inventories all existing and desired domain names, monitors their registration status, and takes action as need be to gain greater control over these same domain names.

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

**Advanced Encryption Standard (AES)** - An encryption methodology developed by the United States National Institute of Standards and Technology (NIST) designed to replace the Data Encryption Standard (DES) and also to be more secure than its predecessor. The AES has variable key lengths, with algorithms specifying a 128-bit key (the default), a 192-bit key, and a 256-bit key.

**Demilitarized Zone (DMZ)** - An interface on a routing firewall leading to a protected network that is different from the main network protected by the firewall. Traffic bound for the DMZ still goes through the firewall and can have the firewall’s protection policies applied.

**Firewall** - A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

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

**Service Set Identifier (SSID)** - A sequence of characters that uniquely names a wireless local area network. An SSID is sometimes referred to as a network name. This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

**Wi-Fi Protected Access (WPA)** - A security scheme for wireless networks, developed by the networking industry in response to the shortcomings of Wired Equivalent Privacy (WEP). WPA uses Temporal Key Integrity Protocol encryption and provides built-in authentication, giving security comparable to VPN tunneling with WEP, with the benefit of easier administration and use.

**System Administrator –** An employee or Third-Party who is responsible for managing a CompanyX multi-user computing 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.

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

References

ISO/IEC 27002: 13. Communications security

PCI-DSS: R1. Install and maintain a firewall configuration

NIST: SC-7 Boundary Protection

US-CSF: PR.AC-5: Network integrity is protected

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 |  |
|  |  |  |  |  |