|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Network Security Management Policy | | | | | |
| Policy # | CPL-09 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc457840806)

[Scope 1](#_Toc457840807)

[Policy 1](#_Toc457840808)

[Authorization 1](#_Toc457840809)

[Configuration 2](#_Toc457840810)

[Diagrams 2](#_Toc457840811)

[System Configuration 2](#_Toc457840812)

[Access Control 3](#_Toc457840813)

[Third Party Network Access 3](#_Toc457840814)

[Firewalls and Traffic Control 3](#_Toc457840815)

[Network Segregation 4](#_Toc457840816)

[Phones and PBX 4](#_Toc457840817)

[Domain Management 4](#_Toc457840818)

[Wireless – Access Points 5](#_Toc457840819)

[Wireless – Configuration 5](#_Toc457840820)

[Domain Management 6](#_Toc457840821)

[Violations 6](#_Toc457840822)

[Definitions 6](#_Toc457840823)

[References 7](#_Toc457840824)

[Related Documents 7](#_Toc457840825)

[Approval and Ownership 7](#_Toc457840826)

[Revision History 7](#_Toc457840827)

Purpose

This policy defines the requirements for establishing the network controls related to the Company X computer and communications systems infrastructure.

Scope

This policy applies to all Company X computer systems and networks, including networks managed by third parties on behalf of Company X. The target audience of this policy is Company X Information Technology employees and partners.

Policy

### ****Authorization****

**Network Security Configuration** - Configurations and set-up parameters on all hosts attached to the Company X 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 computer 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 Company X intranet.

**Internal Network Access** - Only Company X provided computers will be able to access the Company X 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 Company X provided machines.

### ****Configuration****

**Network Central Point Of Failure** - Management must design Company X 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 Company X 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 Company X must have its own dedicated computers and networks, unless approved in advance by the Information Security Manager.

### ****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 Company X networked computer systems must be restricted such that both systems and users outside the Company X 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 partner networks, wireless networks, extranets, and the Internet.

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

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

**Systems Interfacing External Networks** - All Company X 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 Company X computer that is Internet connected or directly reachable through the Internet must be approved by the Information Security Manager.

**External Network Interfaces** - Company X 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-Connected Computers Access Control** - All Company X computers that can be reached by third-party networks must be protected by a privilege access control system approved by the Information Security Manager.

**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 Company X 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 Company X 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 Company X internal networks or multi-user computer systems must pass through an additional access control point.

**Unsecured Remote Computer Connections Denied** - At the time that they make a connection with the Company X 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 Company X 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** - Company X 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 Company X security requirements.

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

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

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

**Internet Traffic Control** - Company X must monitor Internet traffic without blocking or filtering web sites visited by workers or censoring transmissions sent or received.

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

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

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

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

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

**Internal Address Limitation** - The Company X 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 Company X 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 Company X 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 Company X 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, Company X must register and control all Internet domain names which might be confused with Company X'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.

### ****Wireless – Access Points****

**Wireless Network Gateways** - Company X wireless network gateways must always be configured so that they employ firewalls to filter communications with remote devices.

**Wireless Access Points Disabled Unless Approved** - Wireless network access points must be disabled on all Company X computers that handle production information unless the prior approval of the Information Security Manager has been obtained.

**War Driving To Discover Unauthorized Wireless Access Points** - Wireless networks, if improperly configured and secured, can provide entry points for unauthorized people to gain access to Company X's internal network. To ensure that all wireless networks have been registered with, as well as reviewed and approved by the Information Security Department, Company X must periodically conduct war driving tests to discover unauthorized wireless access points.

**Wireless Network Installation, Configuration And Administration** - All wireless access points must be installed by, configured by, and administered by an authorized member of Company X systems administration staff or authorized contractors.

**Minimizing Wireless Network Unauthorized Signal Interception** - Wireless network access points must be placed and the coverage area designed so that the possibility of unauthorized signal interception is minimized.

**Logical Isolation of Wireless Access Points** - All wireless access points must be logically distinguished from, and walled off from, the main internal Company X internal network using configurations approved by the Information Security Department.

**Authorization And Registration Of Wireless Network Devices** - To gain access to the Company X internal network, all wireless access points, handheld wireless computers, and all other wireless devices, must be both authorized by the Information Security Department and registered with the Network Operations Group.

### ****Wireless**** – ****Configuration****

**Vendor Defaults - Wireless** - All vendor default settings on wireless equipment must be changed.

**Wireless Encryption Key** - All wireless networks must be configured to encrypt network communications using a long and complex Wi-Fi Protected Access 2 (WPA2) key.

**Wireless Data Access** - All Company X wireless networks that are connected to any system component that contains confidential information, e.g., cardholder data must use industry best practices to implement strong encryption for authentication and transmission.

**Wireless Network Administration** - All wireless networks must be configured so that they can only be administered locally.

**Wireless Service Set Identifiers Broadcasts** - All wireless networks must be configured to not broadcast the service set identifiers (SSIDs).

**Wireless Default Service Set Identifiers** - All default service set identifiers (SSIDs) on wireless networks must be changed.

**Wireless Network Card Access** - Where technically feasible all wireless networks must be configured to permit access for only particular wireless network cards.

**Wireless Encryption Configuration** - All wireless networks must be configured to encrypt network communications using the Wi-Fi Protected Access 2 (WPA2) certification with the Advanced Encryption Security (AES) algorithm.

**Bluetooth Devices Disabled by default** - All personal wireless-enabled devices, including cellular phones and PDAs, must have default security settings that prohibit automatic discovery of networks.

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

**Internet Domain Name Registration** - Payments and paperwork for Internet domain name registrations for all of Company X 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, Company X must register and control all Internet domain names which might be confused with Company X'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. 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 conduct 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

**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 (Partner)** - Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**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 partner who is responsible for managing a Company X 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 Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 9.0 Network Security Management

ISO/IEC 27002: 13. Communications security

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

HIPAA: Transmission Security 164.312(e)(1)

SC-7 Boundary Protection

Related Documents

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 |  |
|  |  |  |  |  |