*Wireless Security Management Policy*

Table of Contents

[Purpose 1](#_Toc525294648)

[Scope 1](#_Toc525294649)

[Policy 2](#_Toc525294650)

[Approval and Access 2](#_Toc525294651)

[Approved Technical Configuration of Wireless Devices 2](#_Toc525294652)

[Training Required for Wireless Access 2](#_Toc525294653)

[Guest Wireless Privileges 2](#_Toc525294654)

[Secure Default Configuration of Wireless Devices 3](#_Toc525294655)

[Physical Security 3](#_Toc525294656)

[Establishing Wireless Networks 3](#_Toc525294657)

[Automatic Discovery of Wireless Networks 4](#_Toc525294658)

[Installing & Configuring A Wireless Network 4](#_Toc525294659)

[Logical and Physical Security of Wireless Access Points 4](#_Toc525294660)

[Software Requirements for Wireless Access Points 5](#_Toc525294661)

[Testing of Wireless Networks 5](#_Toc525294662)

[Managing A Wireless Network 5](#_Toc525294663)

[Loss and Recovery of Wireless Technology 6](#_Toc525294664)

[Violations 6](#_Toc525294665)

[Definitions 6](#_Toc525294666)

[References 7](#_Toc525294667)

[Related Documents 7](#_Toc525294668)

[Approval and Ownership 7](#_Toc525294669)

[Revision History 7](#_Toc525294670)

Purpose

This policy defines requirements for the secure establishment, maintenance and use of wireless networks by CompanyX, including equipment devices (notebooks, handhelds, portables, personal digital assistants, smart phones, etc.) used to make wireless connections to CompanyX networks.

Scope

This policy applies to all workers involved in the establishment, maintenance and use of wireless networking technology.

Policy

### Approval and Access

**Approved Wireless Devices** - Only those devices (notebooks, handhelds, portables, personal digital assistants, smart phones, etc.) that have been issued by the Information Technology Department will be permitted to gain access to the CompanyX internal network via wireless technology.

**Technical Configurations** - All devices with wireless access must have been pre-configured with the necessary operating system and security software. This software includes, but is not limited to, software that provides an encrypted tunnel (virtual private network) for network traffic, that encrypts device hard drives, that screens for and eradicates computer viruses and other malware, that supports extended user authentication dialogs, that supports remote file backups, that updates software when the software resident on the device is out-of-date, that prevents the user from reconfiguring a device's software, and that logs security-relevant events.

### Approved Technical Configuration of Wireless Devices

**Management Approval** - Only those users who have requested and received Information Technology Department approval for wireless network access will be granted such access.

**Approved Devices** – Only machines whose internal hardware address (MAC address) is recognized by the wireless network, must be allowed to successfully gain wireless network access.

**Personal Networks Prohibited** - Users are prohibited from setting up their own wireless networks without this approval process, whether or not these networks connect with the CompanyX internal network.

Extended Authentication Required - Access to CompanyX internal networks via a wireless connection will furthermore only be permitted in those instances in which the end user employs extended user authentication technology approved by the Information Security Department (dynamic password tokens, biometrics, etc.).

Lost Connection Authentication - Users who have lost a connection to an internal wireless network for five minutes, perhaps because they moved beyond the wireless network coverage area, will be in all instances be required to reauthenticate themselves with this same technology when they reestablish a connection.

### Training Required for Wireless Access

**Wireless Device Training** - All users granted wireless access to CompanyX's internal network must complete a brief wireless network training and awareness program developed by and delivered by the Information Security Department.

### Guest Wireless Privileges

**Public Guess Access** - As the above policy statements imply, guest access to CompanyX wireless networks is not supported or allowed. An exception is made in certain public areas, such as the headquarters building reception and meeting room area. For the establishment of all of these exception areas, previous approval must be obtained from the Information Security Department. Wireless networks in these exception areas must provide only public Internet access, not any direct access to internal CompanyX computers or networks.

### Secure Default Configuration of Wireless Devices

**Secure Default Configurations** - Systems that automatically exchange data between devices via wireless connections -- such as a data synchronization process (also known as a docking process) between a personal digital assistant and a desktop personal computer -- must not be enabled unless these systems have been evaluated and approved by the Information Security Department. Users should be aware that the use of this and all other types of wireless technology, if it has not been approved as mentioned above, could subject the transmitted data to interception by unauthorized parties, as well as generate signals that could interfere with authorized wireless networks in the immediate vicinity.

**Disabled by Default** - For these same reasons, the wireless communications capabilities found in desktop machines and all other CompanyX computers must remain disabled until they have been evaluated and approved by the Information Security Department.

### Physical Security

**Inventory of Wireless Equipment -** The Information Technology Department must keep an up-to-date inventory of all internal-network-connected equipment including authorized wireless access points and authorized mobile devices that have wireless computing interfaces. This inventory must also indicate the software resident on these devices. Auto-discovery systems must be employed to download the most up-to-date software to these same systems.

**Physical IDs** - All wireless access points and mobile devices must also be etched with identifiers that will allow them to be readily returned to CompanyX if they are recovered by police or other Third-Parties following an incident where the devices were lost or stolen.

**Physical Protection of Wireless Devices** - Users must diligently protect wireless-enabled computing devices from loss, theft, and tampering. This effort includes not leaving unattended devices in the open in public areas such as airports or trains, and not leaving these devices in hotel rooms when the rooms are unattended. These devices should be deposited in hotel room safes when not in use, locked in file cabinets when not being used in the office, and locked-up in the trunk of a car whenever the car is parked.

### Establishing Wireless Networks

**Requesting Approval For A Wireless Network** - If a wireless network appears to be a good solution to a business problem, a request for a feasibility study examining the use of a wireless network must first be submitted to the Information Technology Department. If this study indicates that a wireless network is a prudent technology that will serve CompanyX business needs, a risk assessment must then be performed by the Information Security Department prior to the deployment of any wireless networks. Workers who are considering the use of wireless networks for production applications, should be aware that the cost of these systems exceeds that of the wireless network alone.

**Failover Networks** - All wireless networks used for production applications must also employ an alternative fail-over networking technology. This will allow business activities to continue when the wireless network is inoperable (for instance due to radio frequency interference). Such a fail-over network must be built, thoroughly tested, and then approved by the Information Security Department before a wireless network will be permitted to operate with a production application.

### Automatic Discovery of Wireless Networks

**Automatic Discovery** - To enforce this policy, CompanyX automatically detects the presence of all internal-network-connected devices, and it refuses network communication services to those devices that have not been formally approved by both the Information Technology Department and the Information Security Department. To further ensure that all internal wireless networks have been registered and approved, CompanyX periodically conducts "war driving" tests to discover unauthorized wireless access points.

**Procurement of wireless technology** - Users must not purchase, rent, or otherwise procure wireless equipment on their own. These procurements of hardware, software, and services related to wireless networks must be channeled through the Purchasing Department. This process helps to ensure that these purchases are consistent with existing internal technical standards and security requirements.

**Wireless Networks Must Not Process Sensitive** **Data** - Wireless networks are not appropriate for CompanyX applications that process sensitive data (credit card numbers, bank account numbers, mergers and acquisitions plans, etc.). Reflecting the fact that the security of wireless networks is not as strong as the security of wired networks, the Information Technology Department will deny all requests for wireless networks that are intended to transmit or receive sensitive information.

### Installing & Configuring A Wireless Network

**Approved Personnel Only** - All wireless access points must be installed by and configured by an authorized member of CompanyX systems administration staff or authorized contractors. These people must follow the Information Security Department's installation, configuration, and management guide for wireless networks.

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

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

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

**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.

### Logical and Physical Security of Wireless Access Points

**Secure Network Access Points** - To prevent tampering, reconfiguration, theft, and other unauthorized activity, all wireless network access points must be physically secured in areas accessible only by authorized personnel. Wireless network access points must also be placed, and the wireless coverage area designed, so that the possibility of unauthorized signal interception is minimized.

**Logical and Physical Separation** - All wireless access points must be logically distinguished from, and walled off from, the main internal CompanyX internal network using configurations approved by the Information Security Department.

**Encryption and Intrusion Controls** - CompanyX wireless network access points must always be configured so that they consistently employ communications encryption, firewalls, hardware device address (MAC address) filtering, intrusion detection systems, and other security measures defined by the Information Security Department.

### Software Requirements for Wireless Access Points

**Latest Software Patches** - All wireless access points must be running the latest version of the vendor-supplied operating system and security software. Likewise, all mobile devices authorized to access CompanyX wireless networks must be running an up-to-date suite of operating system and security software defined by the Information Security Department. Those wireless access points or mobile devices that are not running up-to-date software will be blocked from accessing the CompanyX internal network.

**Automatic Downloads** - Automatic download facilities must be provided to enable these machines to quickly and securely update their software. In the event that the security of any wireless device has been compromised, these devices will be isolated from the internal network using the same blocking technology, so that further problems are prevented.

**No Backward Compatibility** - Security measures on CompanyX production wireless connected systems must not be backward compatible. By forbidding the backwards compatibility of software, CompanyX helps to ensure that only the latest versions of operating system and security software is employed. Backwards compatibility means that older software can still be used, and this also means that certain security measures are turned off, unavailable, or inactivated.

### Testing of Wireless Networks

**Test of Wireless Networks** - Prior to cut-over to production usage of a wireless network, an extensive test must be performed to ensure that all security and availability control mechanisms are working as they are intended to work. Only after the Information Security Department approves the successful completion of these tests can a wireless network be used for production information processing activities.

### Managing A Wireless Network

**Authorized Personnel** - The management, repair and administration of CompanyX wireless networks must be performed by authorized CompanyX systems administration staff or authorized contractors. These efforts must follow the procedures defined in the Information Security Department's installation, configuration, and management guide for wireless networks. To ensure that wireless networks have been properly configured and managed, periodic audits will be conducted by the Internal Audit Department.

**Change Control** - Changes to the configuration or set-up of a wireless network must follow the standard change control process that is required for other production information systems. Those authorized systems administrators or authorized contractors who make changes without going through the change control process will find that the involved machines will be blocked from accessing CompanyX's internal network. This blocking will be provided with the aid of both network-based auto-discovery software and security auditing software.

**Logging Support** - All wireless access points must have sufficient disk space and internal resources to support the logging and systems monitoring software specified by the Information Security Department. Intrusion detection and incident response activities must be managed by and coordinated with the Information Security Department. Systems administrators responsible for wireless access points must follow the lead of the Information Security Department in response to all security relevant events such as a denial of service attack, a computer virus infestation, or an intrusion by an unauthorized party.

### Loss and Recovery of Wireless Technology

**Reporting Lost Technology** - Whenever a wireless-enabled computing device (notebook, portable, personal digital assistant, smart phone, etc.) that has been granted access to the CompanyX internal network is lost or stolen, this fact must immediately be reported to the Physical Security Department.

**Access Denial** - Mobile devices with wireless communications interfaces that have been reported as lost or stolen must be automatically barred from accessing the CompanyX internal network. Poison pill technology must also be employed such that the data resident on these machines will be automatically erased whenever the devices have been reported as lost or stolen.

### Guest Wireless Privileges

**Public Guess Access** - Guest access to CompanyX wireless networks is not supported or allowed. Guest access must be provided via a separate dedicated network that provides only public Internet access, not any direct access to internal CompanyX computers or networks.

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.

**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: PCI: 4.1.1 Wireless Networks

NIST: AC-19 Access Control for Mobile Devices, 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 |  |
|  |  |  |  |  |