Wireless Access Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Staff shall use the proper security controls when using wireless devices to connect to ABC Company’s Information Systems.

# II. Purpose

ABC Company has developed a set of standards for the use and deployment of Wireless networks.

# III. Scope

This policy applies to all Staff that use and deploy wireless networks.

# IV. Policy

A. Introduction

This policy provides guidance to ABC Company System Administrators who deploy and manage wireless networks as well as to Staff who use wireless networks. Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media. The use of wireless connectivity for enterprise applications is not recommended.

By using personally owned devices within the ABC Company network for business purposes, Staff members are subject to ABC Company policies restricting their use. Any personally owned devices, such as Smartphones, Wearable Computing Devices, wireless devices, or other electronic transmitters determined to have contributed to a security incident may be subject to seizure and retention by ABC Company Staff.

B. Connectivity Considerations

Wireless networks are limited in speed, bandwidth, and coverage. Where possible, the use of a wired connection is preferred because it is faster and it does not compete with other wireless stations (clients) for bandwidth.

Weak signal strength can lead to reduced Staff productivity. The IT Department will perform a general site survey to determine the best placement strategies for wireless access points.

To reduce risks related to wireless networks

* Wireless networks shall not be connected to ABC Company’s internal network (LAN).
* Users inside the ABC Company firewall may not connect to the ABC Company network if they are using a wireless connection to connect to an external network.
* Wireless access points or devices with wireless capability are not allowed unless approved by the IT Department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to ABC Company’s internal network.

Wireless security best practices shall be implemented and include:

* Logical and physical user access to wireless network devices restricted to authorized personnel and devices.
* Perimeter firewalls shall be implemented and configured by IT security Staff to restrict unauthorized traffic.
* Vendor default settings (e.g. passwords, wireless encryption keys, SNMP community strings) are changed prior to installing wireless equipment in a production environment.
* Wireless security practices ensure security and include highest encryption possible, disabling of SSID, and strong passwords changed on a periodic basis.
* IT security Staff testing for the presence of ad-hoc wireless access points on a quarterly basis. Any findings, evidence, and actions taken should be documented and retained per ABC Company’s Data Retention Policy.

Network diagram(s) shall identify connections between internal networks and wireless networks.

C. Security

Wireless (Wi-Fi) transmissions that are used to access ABC Company mobile computing devices or wireless networks must be encrypted. If sent across the Internet (e.g. external to ABC Company's network) or other open networks such as wireless connections, both the authentication data (e.g. a user ID and password) and the data itself must be encrypted with strong encryption. Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.

The Chief Security Officer shall ensure:

* Sensitive information is encrypted using the strongest and most cost effective encryption available.
* Wireless networks transmitting sensitive data or connected to sensitive data environments shall use industry best practices (e.g., IEEE 802.11i or Advanced Encryption Standard) to implement strong encryption for authentication and transmission.
* A separate wireless network shall exist for personal or untrusted devices. Access to the internal network from this network should be treated as untrusted, filtered, and audited accordingly.
* Processes test for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.
* Procedures maintain an inventory of authorized wireless access points including a documented business justification.
* Incident response procedures are implemented in the event unauthorized wireless access points are detected.
* Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO03.06, APO12.02, APO13.07, BAI02.05, BAI10.07, DSS01.05, DSS05.07

GDPR Article 25, 32

HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(3)(ii)(B), 64.308(a)(4)(ii)(B), 164.310(c)

ISO 27001:2013 8.3, A.6.2, A.8.1.3, A.9.1.2, A.9.4.1, A.10.1.1, A.13.1

NIST SP 800-37

NIST SP 800-53 AC-2-4, AC-6, AC-17-18, AC-24, CA-3, PE-17, PL-4, SA-9, SC-7,-8, SC-10

NIST Cybersecurity Framework PR.AC-3-4, PR.AT-1, PR.DS-2, DE.CM-1, RS.RP-1

PCI 1.1.2, 1.2.3, 2.1.1, 4.1, 9.1.3, 11.1, 12.3, 12.10.3