Bluetooth 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

ABC Company’s Information Systems must be protected from communications related threats. Staff must use secure Bluetooth communications procedures.

# II. Purpose

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances using short-wavelength radio transmission. The purpose of this policy is to ensure ABC Company Information Systems are protected from Bluetooth communications threats.

# III. Scope

This policy applies to ABC Company Staff that use Bluetooth technology to connect to Information Resources.

# IV. Policy

A. Devices

To be deployed on ABC Company’s Information Systems, Bluetooth devices must meet current Bluetooth specifications. Any exceptions require written authorization from the Chief Security Officer (CSO). Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

B. Security

Due to continuous communications between devices, unauthorized individuals may be able to track devices and decode information using sniffers or smart phones. Bluetooth connectivity threats include device tracking, eaves dropping, and man-in-the-middle attacks. Staff shall follow the following security requirements specified in this policy to minimize Bluetooth related risks.

Staff shall ensure devices use the strongest Bluetooth security available. Staff shall select devices that use Security Mode 3 or higher. These devices ensure authentication and encryption is established before the physical link is complete. In addition, traffic is encrypted in both directions.

The CSO shall establish and maintain Bluetooth security guidelines. The Bluetooth security guidelines will include a list of approved Bluetooth technologies, types of information that may be transferred over Bluetooth, and requirements for selecting and using Bluetooth personal identification numbers (PINs).

Security training and awareness programs shall make Staff aware of Bluetooth security responsibilities and include:

* Steps to protect Bluetooth devices from loss or theft
* Pairing the Bluetooth devices only when needed
* Configuring the Bluetooth device to use the hidden mode
* Keeping devices turned off when not needed
* Updating device firmware when new releases are issued
* Unauthorized use or modification of Bluetooth devices

C. User Responsibilities

All Staff who use Bluetooth technology must comply with this policy. Staff shall refer to the list of approved Bluetooth technologies for appropriate hardware, software, and connectivity requirements. Only Bluetooth technologies specifically authorized are permitted to be deployed or connected to ABC Company owned equipment.

When dealing with Bluetooth technologies and related equipment, Staff shall follow instructions outlined in ABC Company’s security training and awareness programs. Staff must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment. Staff shall report any misuse, loss, or theft of Bluetooth devices or systems immediately to IT security Staff.

# 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 APO12.02, APO12.07, APO14.02, BAI10.07, DSS01.05

GDPR Article 25, 32

HIPAA 164.312(e)(2)(i), 164.312(e)(2)(ii)

ISO 27001 7.4, A.13

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 2.1, AC-4, AC-19

NIST Cybersecurity Framework ID.BE-4, PR.PT-4, DE.DP-2, DE.CM-3

PCI 1.3.4, 4.1, 6.5.4