Wearable Computing Device 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

Today's Wearable Computing Devices include advanced features such as the ability to connect to the Internet, run applications, take videos, use wireless connectivity, etc. While Wearable Computing Devices increase productivity, they also come with risks.

# II. Purpose

The purpose of this policy is to help manage Wearable Computing Device related risks Staff members and ABC Company.

# III. Scope

This policy applies to all ABC Company Staff that use Information Resources.

# IV. Policy

Only IT Department approved Wearable Computing Devices may be used to access ABC Company networks and Information Resources.

ABC Company uses a multi-layered approach to protecting Wearable Computing Devices and related "information assets". Securing Wearable Computing Devices is the responsibility of both the device user as well as ABC Company’s IT Department.

User activities can download malware to a Wearable Computing Device. Once installed, the malware can launch attacks against ABC Company’s internal network. Staff security education and awareness training should be provided on a regular basis. Staff should only download and install applications from trusted sources. In addition, Staff should not click on message links from unknown senders or visit unknown web sites.

If possible, Wearable Computing Device protection software should be installed on all devices that access the Internet and especially Wearable Computing Devices that access ABC Company’s Information Systems.

ABC Company’s IT Department shall establish standards for Wearable Computing Devices, phone protection software, etc. This reduces IT administration costs and offers better protection for the enterprise.

Wearable Computing Devices shall have security mechanisms that protect against unauthorized access to ABC Company’s Information Systems. Examples include passwords and devices equipped with sensors that read the electrocardiogram (ECG) of the person wearing the device to validate the person's own unique heartbeat signature prior to granting access to Information Resources.

The ABC Company IT Department shall perform periodic risk assessments to identify, manage, and reduce Wearable Computing Device related risks and access to Information Resources. Refer to the Risk Assessment Policy for more information.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from Wearable Computing Devices which are generally higher-risk than non-portable devices (e.g., desktop computers).

# 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 APO10.05, APO12.02, APO13.07, BAI02.05, BAI03.05, DSS01.05, DSS05.02

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 64.308(a)(4)(ii)(B), 164.310(b), 164.310(c)

ISO 27001:2013 8.2, A.6.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-19, AC-20, AU-6, CA-9, CM-8, MP-6, MP-7, SA-18, SC-8, SC-42, SC-43

NIST Cybersecurity Framework ID.AM-1, ID.GV-4, ID.RA-4, PR.AC-1-4, PR.AT-1, DE.DP-2

PCI 1.1.5, 1.1.6, 1.2.1, 1.2.3, 1.4, 2.2