Smartphone 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 Smartphones include advanced features such as the ability to connect to the Internet, download applications, take videos, use wireless connectivity, access network data, etc. While Smartphones increase productivity, they also come with risks.

# II. Purpose

The purpose of this policy is to help manage Smartphone 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 Smartphones may be used to access ABC Company networks and Information Resources.

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

User activities can download malware to a Smartphone. 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.

To reduce IT administration costs and offer better protection for the enterprise, ABC Company’s IT Department shall establish standards for Smartphones and security protection software. Smartphone protection software should be installed on all devices that access the Internet and especially Smartphones that access ABC Company’s Information Systems. If possible, the IT Department shall use a single console to protect and manage Smartphone devices. Smartphone security protection software shall include the following features:

* Protection against Malware
* Periodic scan of installed applications to ensure they are safe
* Block malicious websites that can compromise the device
* Identify applications that allow access to user private information
* Remotely wipe Smartphone data in the event the device is lost or stolen
* Block web-based Malware and phishing attacks by scanning e-mails and text messages

Smartphones shall have a very strong password and a short screen timeout. This helps prevent an unauthorized person from downloading and installing unwanted applications.

The ABC Company IT Department shall perform periodic risk assessments to identify, manage, and reduce Smartphone 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 Smartphones 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