Mobile 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

Mobile computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

# II. Purpose

The purpose of this Policy is to establish the rules for the use of Mobile devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of information.

# III. Scope

This policy applies to all ABC Company Staff that utilize portable (mobile) computing devices and access ABC Company Information Resources. All mobile devices, whether owned by ABC Company or owned by Staff, that have access to Information Resources are governed by this Mobile Device Policy. Applications, including cloud storage software, used by Staff on their own personal devices are also subject to this policy.

# IV. Policy

Only IT Department approved mobile computing devices may be used to access ABC Company networks and Information Resources.

All mobile computing devices must be protected with a password required at the time the device is powered on. The password must meet the requirements of ABC Company’s Password Policy.

Sensitive data shall not be stored on mobile computing devices. However, in the event that there is no alternative to local storage, all sensitive data must be encrypted using approved encryption techniques per the Encryption Policy.

Data must not be transmitted via wireless to or from a Mobile Device unless approved wireless transmission protocols along with approved encryption techniques are utilized. See the Wireless Access Policy for more information.

Non-ABC Company mobile computer devices that require network connectivity must conform to ABC Company IT standards and must be approved in writing by the IT Department.

Unattended mobile computing devices must be physically secured. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Laptops and other mobile computing devices that access ABC Company’s Network Infrastructure shall have active and up-to-date anti-malware and firewall protection. Personal firewalls shall be installed and activated on mobile and/or employee owned devices that connect to the Internet when outside ABC Company’s network and which are also used to access ABC Company’s network.

Annual security education and awareness training shall be provided to Staff that use mobile devices. Such training shall include:

* Minimum necessary. Staff shall only have access to the minimum amount of data necessary to perform their job duties.
* Lost devices. Staff must immediately report any lost or stolen devices.
* Unauthorized access. Any unauthorized access to the mobile device or company data must be immediately reported.
* Rooting devices. Mobile devices must not be “rooted”\* or have unauthorized software/firmware installed.
* Content. Staff shall not load illegal content or pirated software onto a mobile device.
* Software installs. Only approved applications are allowed on mobile devices that connect to ABC Company’s network and data.
* Patch management. Mobile devices and applications must be kept up-to-date. Patches should be installed within 30 days of release.
* Anti-malware. Mobile devices must have active and up-to-date anti-malware protection software. Encryption. Encryption shall be used to protect sensitive information.
* Firewalls. Where possible, personal firewalls shall be installed and active (i.e. not disabled).
* Work habits. Staff shall use ABC Company’s corporate e-mail system when sending or receiving company data.
* Backups. Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis.
* Management software. Mobile device management software will be used to enforce common security standards and configurations.

The Chief Security Officer (CSO) shall ensure:

* Firewalls. Specific configuration settings are defined for personal firewall software. Controls are established to ensure that personal firewall software is not alterable by users of mobile and/or employee-owned devices.
* Training. Annual security training is provided to users of mobile devices. Periodic security reminders may be used to reinforce mobile device security procedures.
* Mobile device management. An evaluation is performed to determine the appropriate Mobile Device Management software to be used to reduce costs and business risks related to mobile devices. Features of Mobile Device Management software include the ability to inventory devices, monitor devices (e.g. application installations), issue alerts (e.g. disabled passwords, out of date operating systems, rooted devices), and issue reports (e.g. installed applications, carriers). The CSO shall ensure Mobile Device Management software enforces security features such as encryption, password, and key lock on mobile devices. The CSO shall perform a review to determine if Mobile Device Management software should include the ability to distribute applications, data, and configuration settings.
* Security. The CSO shall remain up-to-date on industry standard security best practices for mobile devices. Resources can include NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST Special Publication 800-124).
* Exemptions. A risk assessment and risk analysis shall be performed for any requests for exemptions from this Policy.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from mobile 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