Portable Computing 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

Portable 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 portable computing 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.

# IV. Policy

Only IT Department approved portable 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 portable 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 portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized. See the Wireless Access Policy for more information.

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

Unattended portable 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 devices that access ABC Company’s Network Infrastructure shall have active and up-to-date anti-malware and firewall software.

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

The device shall be configured in such a way that if it is lost or stolen the IT Department can remotely wipe the device.

# 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