Bring Your Own Device And Technology 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

Many Staff have personal hardware devices, software applications, utilities, tools, software development kits, and related products that do not meet ABC Company's security requirements.

# II. Purpose

The purpose of this Policy is to establish the rules for the use of Staff owned devices and technologies that utilize and access ABC Company Information Resources.

# III. Scope

This policy applies to all ABC Company Staff that utilize Staff owned devices and technologies that utilize and access ABC Company Information Resources.

# IV. Policy

While ABC Company has a Bring Your Own Device (BYOD) and Bring Your Own Technology (BYOT) culture, risks related to these devices must be managed.

On an annual basis the IT Department shall survey ABC Company Staff about devices, operating systems, applications, browsers, tools, utilities, scripts, software development kits, cloud services, and related technologies used. The IT Department shall perform a BYODT analysis to determine:

* If the devices and/or technologies used pose a risk to ABC Company's Information Systems.
* Changes or configurations necessary to minimize risks to ABC Company's Information Resources.
* Mandatory security components (e.g. firewall, anti-malware protection, passwords, browser security settings, patch management, encryption, physical controls) needed as a condition for allowing BYODT devices and technologies to access ABC Company Information Resources.
* Prohibited devices and technologies.
* Devices and technologies allowed to access ABC Company’s Information Resources.
* Level of access (e.g. restricted, full, guest, admin) granted to the devices and technologies.
* Staff permitted and not permitted to use BYODT devices and technologies.

The IT Department shall implement controls that mitigate risks:

* The IT Department shall ensure Staff access to sensitive data from BYODT devices and technologies have strict password and encryption controls in place. See the Encryption Policy for more information.
* Anti-malware software shall be used and updated on a regular basis. See the Anti-Malware Policy for more information.
* In some instances, the IT Department may identify applications that, due to their sensitive nature, may not be accessed by Staff BYODT devices and technologies.
* Limit Staff activities performed on BYODT devices and technologies (e.g. no access to personal e-mail or social media).
* The IT Department may restrict access to ABC Company Information Resources based upon Staff position responsibilities, geographical location, and lack of management approval.
* The IT Department will keep the Chief Security Officer (CSO) informed of BYODT threats so that the security awareness and training program can be updated.

In the event a device is lost or stolen, the IT Department shall quickly block access to Information Resources from the device. In addition, the IT Department shall:

* Remotely wipe ABC Company data and applications, and/or
* Remotely wipe the entire BYOD device if deemed necessary to ensure the security of ABC Company Information Resources. Wiping the entire BYOD device may have Staff implications including the inability to make calls, loss of contacts, need to have the device restored, etc.

ABC Company shall not be held liable for the loss of use or restoring of device, operating system, software applications, tools, scripts, data, etc. Staff should take the proper precautions (e.g. physical controls over devices, backing up of contacts and files, etc.) to minimize any disruptions.

BYODT devices and technologies shall employ controls that meet the following requirements:

* Password required at start up (power on).
* Inactivity timeout (per the Access Control Policy).
* Password change frequency (per the Password Policy).
* Safeguards ensure only approved users of BYODT devices and technologies can access ABC Company Information Resources.

Staff shall not:

* “Root” or “jailbreak” a BYODT device and technology to free it from pre-defined limitations. This process modifies the system files and can result in an unstable and insecure device.
* Modify BOYDT device and technology hardware and/or software beyond installation of updates provided by the device maker or service provider.
* Disable BYODT device and technology protection systems including passwords, encryption, firewalls, and anti-malware without the approval of the IT Department.

The IT Department shall prepare a list of authorized BYODT devices and technologies that are allowed to utilize and access ABC Company's Information Resources. In addition, the IT Department shall specify specific configurations and circumstances under which BYODT devices and technologies may connect to ABC Company's Information Resources.

Per the Mobile Device Policy, only IT Department approved portable computing devices may be used to access ABC Company networks and Information Resources. Per the Smartphone Policy, only IT Department approved Smartphones may be used to access ABC Company networks and Information Resources. Per the Approved Application Policy, only approved software applications are allowed to access ABC Company networks and Information Resources.

Staff shall be responsible for adhering to the requirements of this Policy. Staff shall notify the IT Department when:

* A new BYODT device or technology is acquired and needs access to ABC Company Information Resources.
* A BYODT device or technology is taken out of service and is no longer used.
* The Staff member’s role changes requiring a change in access (e.g. Staff member changes positions, Staff member on a leave of absence).

When choosing an appropriate plan, Staff should consider the additional voice minutes and data traffic that may be incurred. Except as otherwise consistent with this Policy, ABC Company does not assume any financial responsibility for BYODT devices or technologies. ABC Company shall not reimburse Staff for the following expenses:

* BYODT device or technology initial cost, maintenance, or replacement
* Recurring costs related to voice and data usage, roaming, etc.
* Connectivity charges including Wi-Fi hotspots usage
* Insurance
* Expenses related to restoring BYODT devices or technologies if lost, corrupted (e.g. Malware, incompatible applications, changes to operating system), or damaged.

ABC Company shall reimburse Staff for the following expenses related to BYODT devices or technologies:

* Approved app software for use with corporate systems (e.g. e-mail apps).
* Approved anti-malware software.
* Approved encryption software for use with corporate systems (e.g. VPN software).

The ABC Company IT Department shall perform periodic risk assessments to identify, manage, and reduce BYODT device and technology 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 BYODT devices and technologies 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 APO12.02, APO12.07, APO14.02, BAI10.07, DSS01.05

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 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-2, ID.GV-4, ID.RA-1, ID.RA-4, PR.AC, PR.AT-1, DE.DP-2

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