Bring Your Own Device (BYOD) Policy

Version – 1.0

Revision History

Version	Date	Author	Major Changes
1.0	01/11/2023	Ashish Christian	Initial Version

Contents

1. Introduction, Benefits & Scope: 3
2. Applicability: 3
3. BYOD Challenges: 4
4. Risks & Liabilities: 4
5. Responsibilities: 5
6. Expectations: 6
7. Enforcement: 6

1. Introduction, Benefits & Scope:

Allowing employees to use their own electronic devices while working, whether at home, at the office, or while travelling, has the following advantages, according to Techforce.

- Reduction in procurement overhead.
- End user comfort level with their own devices.
- Support Remote & Flexible working.
- Increased productivity.
- Provides Operational redundancy.

Bring your own device, or BYOD, is the term used to describe the use of gadgets like laptops, cellphones, and tablets. As a result, employees continue to own hardware assets, while organizations continue to control information assets. Techforce wants to safeguard the availability, confidentiality, and integrity of data and technology by creating this policy.

The following framework and legal requirements should be considered, even if this policy won't go into detail:

- PCI DSS 3.2.1 / 4.0
- ISO 27001:2013 / ISO 27002:2022.
- NIST Cyber Security Framework V 1.1.
- Cloud Security Alliance – Level 1 (CAIQ v4)

2. Applicability:

- This policy is only applicable for all permanent (Full-time) employees of Techforce Infotech Pvt. Ltd.
- This policy can also be applied to specific contractors depending on their roles and responsibilities. This benefit can be offered at the time of the Contract.

3. BYOD Challenges:

BYOD residual hazards may be decreased to a manageable level by implementing strict administrative, physical & technical restrictions and better monitoring. Here are a few difficulties:

- Contractual complexity and adherence to the law.
- Conflict with an employee's right to privacy.
- More complicated measures for safeguarding information assets.
- Wide variety of devices supported.
- Checking that employee devices adhere to the security guidelines set forth by the firm.

4. Risks & Liabilities:

- While the IT team will take every reasonable precaution to safeguard employee data in the event of a remote wipe, it is the employee's responsibility to take additional safety measures, such as backing up their email, contacts, and other information.
- Lost or stolen devices must be reported to the company within 24 hours.
- The company maintains the right to disconnect devices or disable services without notice.
- It is the responsibility of the employee to contact the cell carrier right away if a device is lost.
- The employee is required to follow the company's acceptable use policy and to always use their devices in an ethical manner.
- The employee is entirely responsible for all expenses related to their device.
- The risk of losing company and personal data entirely or partially because of an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming mistakes that render the device unusable, is fully assumed by the employee.
- Techforce reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

5. Responsibilities:

- Every employee should be aware of their device's security measures so they can protect their personal information as well as Techforce data.
- Make that the device is not utilized for any activity that might violate a Techforce Policy.
- While Techforce will always try to help staff members where it can, Techforce cannot be held liable for maintaining devices that it does not supply.
- Employees who use BYOD must:
  - Configure passwords, passcodes, passkeys, or their biometric counterparts. This ought to be sophisticated enough and long enough for the gadget.
  - Always keep your operating system, antivirus software, and firmware up to date.
  - If you have the option, set up remote wipe tools and use them if they lose the device.
  - When necessary, encrypt data or devices.
  - Holding sensitive, private, confidential, or commercially valuable information on privately owned devices should be avoided wherever possible.
  - If Techforce information must be kept on a personal device but is critical, it should be destroyed as soon as it is no longer needed.
  - Inform **infra@techforceglobal.com** about any security event.
  - Don't let any Techforce data remain on a personal device indefinitely.
  - If a gadget is thrown away, sold, or given to someone else, caution must be exercised.
  - As per the Antivirus and Threat Protection policy, install Threat Protection software on a personal device.
  - Manage Engine agent will be installed in order to check vulnerability status of machine and also keep track of installed software. This will be mandatory to your own device.
- Employees adopting BYOD must take all necessary precautions to:
  - Prevent data loss and theft.
  - Information should be kept private as necessary.
  - Ensure the accuracy of all data and information.
  - Be accountable for whatever software they install on their device.
  - If the gadget is left idle for three minutes, it must lock itself with a password or PIN.

  - The device will lock after three unsuccessful login attempts.

6. Exceptions:

Exceptions to the policy statements in this text are only permitted if it is approved by CEO or Co-Founder or Techforce Management

7. Enforcement:

- For Employees temporary workers, and consultants, violating this policy may result in termination of employment relations; for contractors and consultants, violating this policy may result in termination of access and/or disciplinary action, which may include termination; and it may also result in additional legal or criminal action.