Bring Your Own Device Policy

Summary

Bring Your Own Device (BYOD) is when employees connect personal devices such as laptops, smartphones and tablets to resources within their employer's IT infrastructure. Companies have saved money by decreasing or even removing the need to purchase devices for their staff, and staff have benefited from the familiarity of using their own electronic devices to do their jobs.

Along with the benefits of using their own devices there is of course another side to this emerging practice and that is the need to establish appropriate guidelines for usage and control of these devices as well as what they *can* access and what steps should be followed in the event of loss, theft or employment termination. Since employees use their devices for personal and/or leisure activities, this can pose more risk for the employer than the exclusive use of business-owned devices.

This policy describes the steps that the employer and its employees should follow when connecting personal computers and devices to their employment's IT systems and networks.

Purpose

The purpose of this policy is to provide guidelines for BYOD usage and establish the steps that both users and IT departments should follow to prepare, support, and remove devices from the Company's infrastructure in order to protect company systems and data from unauthorized access or misuse.

Who is this document for?

All full-time employees, contract workers, consultants, part-time staff, temporary workers and other personnel granted access to Company systems, networks, software, and/or data are covered by this policy.
This policy is not applicable to devices which connect to the Company's public wireless local area network, since it is a separate environment which cannot access Company systems, networks, and/or data.

Equipment covered by this policy includes (but is not limited to):

- Desktops, laptops, and tablet computers
- Smartphones (defined as any cellular telephone that connects to the Internet via Wi-Fi or a mobile provider network)
- Flash, memory and/or thumb drives
- External hard disks
- iPods, iTouches, and similar entertainment and portable music devices that connect to Wi-Fi networks
- Entertainment and gaming consoles (Xbox, PlayStation, Wii, etc.) that connect to Wi-Fi networks and are used to access Company email and systems

BYOD Policy Guidelines

All workers must understand that whenever a computer device is connected to the Company's network, systems, or computers, opportunities exist for:

Introducing viruses, spyware, or other malware:

- Purposefully or unintentionally copying sensitive and/or proprietary Company information to unauthorised devices.
- Introduces a technical or network incompatibility to the Company that the user is not even aware of.
- Loss of data which may adversely impact the Company if it falls into the wrong hands.

As a result of any of these circumstances, a user connecting his or her own device to Company resources, systems, or networks could interrupt business operations, cause unplanned downtime for multiple users, and / or cause a data breach releasing Company, client, and /or partner data to unauthorised parties.

In worst-case scenarios (and in events entirely realised at other companies), civil and criminal penalties for the user and / or substantial costs and expenses to the Company could arise.

The BYOD Checklist and Approval form (see below) must be used to identify employee needs and approve access before any personal device is connected to company systems or networks, or permitted to contain company data. No individual, staff member, or user other than the Company's IT director may authorize a personally owned or personally provided device for use within the Company.

IT Department Responsibilities

Where applicable, the IT department will ensure the following to facilitate BYOD access as requested for a user device:

- The device does not have a static IP address that could introduce network incompatibilities.

- The device does not have a virus, spyware, or malware infection. The device does not have any third-party software or applications which pose a threat to the systems and networks or that could introduce application incompatibilities (any such findings should be removed before proceeding). The IT department reserves the right to make judgment calls regarding which applications (current or future) are appropriate for devices associated with company systems, networks and data.

- The device is properly protected against viruses, spyware, and other malware infections and that the system has properly licensed anti-malware software, when appropriate.

If this involves a mobile device such as a smartphone or tablet which will be associated with company systems, a security policy should be applied to this device (such as via an Exchange server) to enforce a password/biometric policy which will automatically lock the device after one- minute period of inactivity and erase the contents of memory and storage after a maximum of 10 failed authentication attempts. The policy should also include the ability to remotely erase (wipe) these devices in the event of loss or theft.

If such a company-wide policy does not exist:

- The above screen lock/password settings should be individually applied.
- The device has all critical and security patches installed.
- The device is properly encrypted if the potential exists for the device to save, cache, or even temporarily store Company data.
- The device is properly configured to access resources remotely and that it does so in the most *secure fashion possible such as through a VPN connection*.
- When a device is to be decommissioned, the IT department will remove any required encryption, VPN, and anti-malware licensing from the user's device. They will also confirm that the user's device does not contain any traces of protected, sensitive, corporate, or proprietary information and delete any protected, sensitive, corporate and/or proprietary data, licensing, and information remaining on the device.

The IT department reserves the right (and should proceed) to remotely wipe a device if it has been lost or the employee has been terminated and has not brought their device to the IT department for decommissioning.

User Responsibilities

- The user should not attempt to change or disable any security settings applied to the device by the IT department.

- The user should consult the manufacturer/vendor/carrier for support of their device before requesting assistance from the IT department.

- In the event that a user believes a personally owned or personally provided device that is authorized to connect to the Company's resources, systems, and networks might be infected with a virus, spyware infection, or other malware threat or might be somehow compromised, he or she must immediately notify the IT department, in writing, of the potential security risk.

- In the event that a user loses or misplaces a personally owned or personally provided device that is authorized to connect to the Company's resources, systems, and networks, he or she must immediately notify the IT department, in writing, of the potential security risk.

- Whenever a user decommissions, prepares to return, or otherwise ceases using a personally owned or personally provided device that the IT director has authorised for Company use, the user must notify the IT department that the device will no longer be used to connect to Company resources, systems, and networks.

- Users may not discard previously authorised devices until the IT department approves the device for disposal.

This checklist should be used before any personally owned device is connected to the Company's resources, systems, networks, and devices. It should be signed by the user's manager and the IT department manager before proceeding to connect the device.

User's full name:

User's title:

User's mobile telephone:

User's home telephone:

User's email address:

User's department:

Date of request:

Device user wants to connect to Company resources, systems, or networks:

Company's resources, systems, or networks to which user wishes to connect:

Purpose for the request:

Manager's approval:

IT Director's approval:

Decommission Steps

Date user requested decommissioning:
Date IT department decommissioned device:
Method used to decommission device (disassociate/remove from company systems, wipe operating system, physical destruction, etc.):

Completed by (name): ----------

Completed Date: ----------

Acknowledgment of BYOD Policy

This form is used to acknowledge receipt of, and compliance with, the Company's Severance Policy.

Procedure

Complete the following steps:

1. Read the BYOD Policy.
2. Sign and date in the spaces provided.
3. Return a copy of this signed document to the IT department manager.

Signature

Your signature attests that you agree to the following terms:

1. I have received and read a copy of the BYOD Policy and I understand and agree to the same.
2. I understand the Company may monitor the implementation of and adherence to this policy to ensure compliance.
3. I understand that violations of the BYOD Policy could result in termination of my employment and legal action against me.

Employee Signature: ----------

Employee Title: ----------

Employee Name: ----------

Date: ----------

Department: ----------

Location: ----------

Disclaimer: This policy is not a substitute for legal advice.