BRING YOUR OWN DEVICE POLICY (BYOD)

Summary

The-bring your-own-device (BYOD) movement has helped streamline IT operations by allowing employees to connect personal devices such as laptops, smartphones, and tablets to organizational resources. Businesses have saved money by reducing or eliminating the need to purchase devices for their workers, and workers have benefited from the familiarity of using their own electronics to do their jobs.

Of course, this flexibility comes with another sort of price: the need to establish proper 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 recreational activities, this can pose more risk for the organization than the exclusive use of business-owned devices. This policy describes the steps that the company and its employees will follow when connecting personal computers and devices to organization systems and networks.

Purpose

This policy outlines requirements for BYOD usage and establishes the steps that both users and the IT department should follow to initialize, support, and remove devices from company access. These requirements must be followed as

documented to protect company systems and data from unauthorized access or misuse.

Scope

This policy covers all full-time and part-time employees, contract workers, consultants, temporary workers, and other personnel granted access to organizational systems, networks, software, and/or data.

Policy details

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 WiFi networks
- Entertainment and gaming consoles that connect to Wi-Fi networks and are used to access organization email and systems

- Wearable devices such as watches, VR headsets, and augmented reality glasses with WiFi or Bluetooth

Policy guidelines

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

- Introducing viruses, spyware, or other malware.
- Purposefully or inadvertently copying sensitive and/or proprietary organization information to unauthorized devices.
- Introducing a technical or network incompatibility to the organization that the user is not even aware of.
- Loss of data that may adversely affect the organization if it falls into the wrong hands.

As a result of any of these circumstances, a user connecting their own device to organization resources, systems, or networks could interrupt business operations, cause unplanned downtime for multiple users, and/or cause a data breach releasing organization, client, and/or partner data to unauthorized parties. In worst-case scenarios (and in events entirely realized at other organizations), civil and criminal penalties for the user and/or substantial costs and expenses to the organization could arise.

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 that 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 that 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 that 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.

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 that 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 that 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 that 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 organization 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. It will also confirm that the user's device does not contain any traces of protected, sensitive, corporate, or proprietary information and will delete any that remains 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 organization's resources, systems, or networks might be infected with a virus, spyware infection, or other malware threat or might be somehow compromised, they must immediately notify the IT department in writing of the potential security risk.
- If a user loses or misplaces a personally owned or personally provided device that is authorized to connect to the organization's resources, systems, or networks, they 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 authorized for organization use, the user must notify the IT department that the device will no longer be used to connect to organization resources, systems, or networks.
- Users may not discard previously authorized devices until the IT department approves the device for disposal.

Acknowledgement of BYOD Policy

This form is used to acknowledge receipt of and compliance with the company's BYOD 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 Human Resources department.

Signature

Your signature attests that you agree to the following terms:

- I have received and read a copy of the BYOD Policy and I understand and agree to the same.
- I understand the organization may monitor the implementation of and adherence to this policy to review the results.
- I understand that violations of the BYOD Policy could result in termination of my employment and legal action against me.

Employee Signature Title

Employee Name Date

Department/Location