**Bring Your Own Device (BYOD) Security Policy**

# Overview

Today, a business only allowing their company to use given devices hinders flexibility and consumes company income. The Bring Your Own Device (BYOD) approach would eliminate such arrests. It will enable a company to drop its focus on device distribution/collection controls and use that focus on missions that develop company growth. However, with great progression comes great responsibility, so a policy must be made to ensure all security measures are considered before proceeding.

This fast-growing BYOD approach benefits companies worldwide, assuming all precautions are taken to secure network connectivity. Today, remote work is becoming more popular from both physical and mental standpoints, as well as strategically and financially, in the competitive business world. The growing use of personal devices only furthers the necessity of an effective control policy. This policy is meant to highlight the security understanding, concerns, and procedures to ensure network security while on the company network.

# Purpose

It is essential to know where vulnerabilities lie to ensure that a company’s data is protected. When agreeing to use your personal phones, tablets, laptops, and wearables in a company network, you should remember that all devices connected to a network via the internet have vulnerabilities. Your job as a BYOD policy user is actively detecting, denying, and deterring data accessibility threats through your device that would leave your company network open to attacks.

It is the responsibility of both users and IT support personnel to manage device control through enabling and disabling devices on a network in consideration of necessity. It is also the responsibility of users and IT support staff to monitor the security of said devices. When a device on the network is no longer necessary, please ensure that the device is immediately and securely disconnected from the network to prevent unnecessary attack vantage points. The disconnected device should be cleared of company data and disconnected through the IT team. The IT team and user will ensure no data is kept outside of network storage or that said data can be accessed after disconnect.

# Scope

This security policy is created for and must be followed by individuals in direct or indirect control of devices connected to the company network. It is required that all devices accessing the network are up to date in both hardware and software security standards, as stated by the IT team, through verified and scheduled email announcements. If a device cannot complete the update by the established deadline, the device will lose its rights to the network.

Users must submit all devices they wish to add to the network to the IT support team for evaluation and approval. The devices can include but are not limited to smartphones, tablets, PC, and wearables. Keep in mind that all devices entering the network must have a valid reason to connect to the network to be approved. Valid reasons to connect devices to the company network would require a positive impact on corporate growth. If a device remains inactive for more than five unreported consecutive business days, then the device will be disconnected, and a reevaluation will be established.

Access to the company network would be granted to individuals upon recorded arrival time (clock in) and departure time (clock out). Working on the network outside of business hours requires a written request to the team member's team lead, which will then follow granted permission from the group manager. If a device attempts access outside of these permissions, the device will be denied and flagged. Should a device get flagged three times, the device will be locked, and an investigation will be conducted.

All permissions will be granted and monitored via groups through the Identity Access Management team (IAM). Special permissions may only be granted if absolutely necessary and not be completed without approvals from the direct manager or higher authorities.

# Policy

All personal devices must meet required hardware and software standards. A device must pass an ethical hack test established by the IT support team to be considered compliant. This test is to be upgraded monthly on account of recent attacks and trends and conducted randomly with a 24hr notice. If a device fails the test, it will be strictly monitored by IT support and will have five business days to upgrade to necessary security standards. Should the device be unable to meet these standards, the device will be disconnected from the network, and a company replacement will be given to the employee. This replacement will no longer fall under the BYOD policy and will be considered the company’s device and follow a company device policy.

# Policy Compliance

Security policy breaches will be classified as either accidental, intentional without critical intent, or intentional with critical intent. Accidental breaches will enable a device to be flagged, and the individual will have verbal counseling from the IT support lead. All violations that expose pertinent data on employees or companies will be considered critical and trigger an investigation of user and user devices.

The breach will be considered intentional without critical intent if a device acquires three or more flags. Breaches considered intentional without critical intent will enable a temporary network device lockout until the user completes and passes the company’s online cybersecurity assessment. If an employee continues to breach security policies after training, the employee will be at risk for termination of employment.

An intentional breach with critical intent will immediately lock all user devices out of the company network. Users responsible for intentional breaches with critical intent will be investigated along with all user devices.

# Related Standards, Policies, and Processes

For more guidelines on network safety, please review and apply Cyber Security Policy, Data Protection Policy, and Employee Exit Checklist. These policies will further explain safety precautions and device-to-network care.

# Definitions and Terms

Bring Your Own Device (BYOD)

Identity Access Management (IAM)

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of change | Responsible | Summary of change |
| August 2019 | SANS policy team | Updated and converted to new format |
| September 2022 | Kassandra Moreno | Sections 1-7 |