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

**Free Use Disclaimer:** This policy was created by or for the SANS Institute for the internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required.

**Last Update Status:** Updated August 2019

# Overview

A tablet can also enable a broker to make client presentations with the integration of photos and data to present information to clients. The security industry is experiencing changes in the industry, thanks to tablets and smartphones. Companies can create applications that give consumers the ability to monitor their homes from a mobile device.

# Purpose

Active scanning, agents, passive monitoring, cloud connectors and CMDB integrations provide unified visibility and a continuous view of all of your assets - both known and previously unknown.

# Scope

Tablets and smartphones are necessary business tools, and an increasing number of employees want to retire their company-owned hardware, opting instead to work from their personal devices. And while organizations are skeptical about letting workers save corporate data on the same gadgets. Approval will be received by IT personnel. Using the Company computer or network resources in violation of policy or for illegal activity is strictly prohibited. Prohibited uses may include, but are not limited to, harassment and intimidation of individuals in violation of the Company’s Nondiscrimination and Anti-Harassment Policy, obscenity, child pornography, threats, or theft. Examples of misuse also include attempting to gain unauthorized access to data, attempting to breach security measures on any electronic communications software or system, attempting to intercept electronic communication transmissions without proper authority, and violating intellectual property or defamation laws. Do not use computer or network resources to send, post, or display slanderous or defamatory messages, text, graphics, or images.

Network Access and Permissions (NAAP) is one way to reduce risk. There are many different access controls. I choose to pick the most used one which is user related controls.

# Policy

Pertaining to network security, the most critical PCI compliance network requirements are maintaining secure networks, encrypting open network transmissions, and testing critical networks. By default, each compliance policy includes the action for noncompliance of ark device noncompliant with a schedule of zero days (0). The result of this default is when Intune detects a device isn't compliant, Intune immediately marks the device as noncompliant.

# Policy Compliance

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, intrusion detection tools, business tool reports, internal and external audits, and feedback to the policy owner.

An employee found to have violated this policy may be subject to disciplinary actions up to and including termination of employment.

# Related Standards, Policies, and Processes

Some are required to comply with both HIPAA (Healthcare Information Portability and Accountability Act) and the PCI DSS (Payment Card Industry Data Security Standard), namely, covered entities and business associates that accept credit, debit, or other payment cards.

# Definitions and Terms

BYOD is the practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes, a mobile device is piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer, and CIA/ Central Intelligence Agency known informally as the Agency and historically as the Company, is a civilian foreign intelligence service of the federal government of the United States, officially tasked with gathering, processing, and analyzing national security information from around the world, primarily through the use of human intelligence (HUMINT) and performing covert actions.

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of change | Responsible | Summary of change |
| August 2019 | SANS policy team | Updated and converted to new format |
|  |  |  |