Wearable Device Policy

2024

Janco Associates, Inc.

Table of Contents

Wearable Device Policy

Overview

The purpose of this policy is to define standards, procedures, and restrictions for wearable devices that can capture, display, and or broadcast video, audio, WiFi data, and GPS location presenting new challenges for the enterprise.

There are clear benefits and risks to these devices in the workplace.

- They can be used for alerts and notifications as pagers and smartphones. Wearers can see the alert, and in many cases respond to it, while continuing to do whatever it is they were doing, even if they were in a meeting.
- Drivers, warehouse workers, and others who use both hands during work will benefit enormously. Wearable devices essentially give them the basic tools of a white-collar

here others can direct

sabled employees.

There are als he expressed consent of the enterpris tion is located.

The policy applies to any device that could be used in such a manner, even when the equipment is not approved, owned, or supplied by ENTERPRISE.

Policy

Use of these wearable devices is allowable under the following conditions:

- The privacy and confidentiality of Enterprise facilities, systems, information, property, employees, guests, suppliers, and customers are maintained.
- Devices will not be used in any manner that compromises any individual or processes at enterprise locations.
- If the device is enterprise-owned and approved, it is not to be used away from enterprise locations unless it is specifically authorized by the enterprise.

There can be limited personal use of the device:

- Imposes no tangible cost to ENTERPRISE;
- Exposes ENTERPRISE to any liability or risk;
- Does not unduly burden ENTERPRISE's computer or network resources;
- Has no adverse effect on an employee's job performance?

Upon entry in any location noted with a sign that Wearable Devices are not permitted, the device should be removed and powered off. This includes facilities that are open to the public,

All users shall be required to acknowledge receipt and understanding of all regulations governing the use of Wearable Devices and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with ENTERPRISE policies.

Wearable Devices Security Best Practices

For Wearable Devices content management includes robust security and device management capabilities are the definition of best practices. CIOs and CSOs should implement the following:

Security Controls

- 256-bit AES encryption per file at rest, 30-day rotating encryption key - Advanced
  of electronic data. It has
  vide.
- ovides an extra layer of
  st login and password

Remote Wea

- Automatic timed screen logout on devices that can display information
- At least a 4-digit passcode for each device
- Biometric security processes where possible like fingerprint or retina scanning for connectivity to the enterprise network
- Immediate access restriction on the device
- Automatic login to end-user accounts which includes the facility to remotely wipe all connection protocols, data, and software from the device
- Automatic shutdown and locking of a device after a security breach from a device
- Security breach reporting

Top 10 WYOD Best Practices

Employees bringing their smartphones into the workplace started the BYOD trend requiring enterprises to deal with the serious security implications that come from these devices. The decision for employees to wear their device (WYOD), such as an Apple watch that can link to your WiFi; capture audio, video, and data; store; and transmit poses similar problems for IT departments. Employees and individuals outside of the enterprise can use these devices, sometimes discretely, to access and share business content.

This puts corporate data and infrastructure at risk and reinforces the need for IT managers to focus on securing the content, rather than the device that's in use. Wearable devices simply add another level of access and security concern to what we've already seen with the BYOD trend.

Here are the top 10 best practices for WYOD.

1. **Have a strategy for how, when, and why WYOD devices can be used**. This should include both internal operations and external ones that are available to the general public.
2. **Implement an acceptable use policy**. Include legal references and methods of communication of that policy to those outside of the organization.
3. **Identify the connectivity options that are available to both internal and external users**. Include security
4. **ure access points**. There should have
5. devices are designed to be managed by utside of the control of IT they need to ol as well as a very advanced piece of often as powerful and capable as an he corporate walls, they are often sitting on the table at a coffee house or beside a pool at a hotel.
6. **Plan for the activity WYOD devices will add to the network**. Consumer devices are voice, video, high-definition image, and application-rich. Employees using these devices will devour bandwidth and network resources. Assess your existing switch and router networks, your wired and wireless access in-branch and home offices, the size of your internet pipes, and connections to remote locations. Make adjustments in advance of the increased demands that are inevitable on your IT network infrastructure grid.
7. **Make collaboration tools a priority**. Although consumer devices offer social and digital options natively, don't be content with just consumer-grade capabilities, extend your organization's collaboration tools for enterprise mobility, integrated voice, video, messaging, conferencing, application sharing, presence, and single number reach to realize even greater productivity gains.
8. **Secure the endpoints and isolate sensitive/confidential information and locations**. What is your strategy, especially important in highly regulated industries such as healthcare and finance that require strict security and compliance controls? Review WiFi security, VPN access, and perhaps add-on software to protect against malware. Consider two-factor authentication technologies.
9. **Be prepared for little to no advance notice of upgrades**. Third parties like Apple and Samsung are not part of your company's Change Management Process. Expect new code to be dropped on your corporate endpoints overnight creating connectivity, application, and security issues.
10. **Formalize your 7 x 24 support**. If employees are going to work in the evening, on weekends, or take time away from a family vacation, IT systems must be available when they do. Downtime is no longer an option. Either bring in tools and staff around the clock or engage an IT-managed service organization to provide the coverage you need.

Electronic Forms

Three (3) Electronic forms are included with this policy template. It comes separately in its directory.

Mobile Device Access and Use Agreement

Mobile Device Security and Compliance Checklist

Wearable Device Access and Use Agreement

What's New

2024 Edition

- Update to meet the latest mandated requirements and security standards
- Updated all included forms

2023 Edition

- Update to meet the latest mandated requirements and ISO compliance standards
- Updated all included forms

2022 Edition

- Update to meet the latest mandated requirements and ISO compliance standards
- Updated all included forms

2021 Edition

- Added two electronic forms
  - Mobile Device Access and Use Agreement
  - Mobile Device Security and Compliance Checklist
- Updated all included forms
- Added section on device and data ownership – focus on WFH

2020 Edition

- Updated to meet GDPR and CCPA-mandated requirements
- Updated included electronic form