



**This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**

<https://e-janco.com>

# **BYOD Policy Template**



**Table of Contents**

Bring Your Own Device (BYOD) Access and Use Policy .....3

    Overview .....3

    Components of the BYOD Strategy and Basics for BYOD Policy.....4

    Device Ownership Issues .....7

    Policy .....8

        Device Requirements .....8

        Policy Definitions .....9

        Access Control.....9

        Security .....10

        Help & Support .....11

        Enterprise Mobile Device Infrastructure .....11

        BYOD Infrastructure.....12

        Disaster Recovery .....12

        Termination.....12

        Backups .....12

        Tablet Computer (iPads) .....13

        Internal Network Access .....13

        Repair Procedure .....13

        Upgrade Procedure.....13

        Patching Policy .....13

    BYOD Security Best Practices .....14

    Work From Home - Best Practices.....16

BYOD Metrics and SLA Agreement .....17

Legal Considerations.....19

Appendix.....22

    BYOD Policy Decision Table .....23

    Electronic Forms .....24

        BYOD Access and Use Agreement Form

        Employee Termination Checklist

        Mobile Device Security Access and Use Agreement Form

        Mobile Device Security and Compliance Checklist

        Telecommuting IT Checklist

        Telecommuting Work Agreement

        Work From Home IT Checklist

        Work From Home Work Agreement

    IT Job Descriptions .....25

        BYOD Support Specialist

        BYOD Support Supervisor

        Manager BYOD Support

        Manager WFH Support

What’s New .....26

## Bring Your Own Device (BYOD) Access and Use Policy

### Overview

The purpose of this policy is to define standards, procedures, and restrictions for end-users who have specific and authorized business requirements to access enterprise data from a personal device - BYOD (Bring Your Own DEVICE) - connected via a wired, wireless, or unmanaged network outside of ENTERPRISE's direct control. This policy applies to, but is not limited to, all devices and media that fit the following device classifications:

Smartphones

**This is a sample of the final product  
and these pages are for your review  
and are protected by Janco's copyright.**

**<https://e-janco.com>**

ices  
ecting to an unmanaged

The policy applies to any hardware and related software that could be used to access enterprise resources, even when the equipment is not approved, owned, or supplied by ENTERPRISE.

Once you implement a BYOD policy, it's important to have a written agreement in place with every mobile device user. An agreement raises consciousness about the critical nature of mobile IT operations, and it protects organizations in the event of a BYOD policy violation. Like your BYOD policy itself, this agreement should be as clear as possible, to prevent misunderstandings that could generate a wide range of problems and IT headaches.

Components of the BYOD Strategy and Basics for BYOD Policy



The BYOD strategy and resultant policy are driven by 8 factors: device choice options; user experience and privacy; internal marketing and training; liability; economics; application design and infrastructure; maintainability; and trust security compliance. Each of these factors has been considered in the creation of this policy. A detailed description of each of these factors is provided later in this policy. Everyone in the company must be on the same page about what you can and can't access on personal devices. Policy guidelines need to be clear and compliance mandatory.

*Device Choices*

- ✚ Analyze employee preferences and understand which devices they already have.
- ✚ Define an acceptance baseline of what security and supportability features a bring-your-own-device program should support
- ✚ Understand the operating system, hardware, and regional variances around that baseline.
- ✚ Develop an “easy” certification process for the evaluation of future devices.
- ✚ Establish clear communication to users about which devices are allowed or not, and why
- ✚ Policies need to be established for device features from Global Positioning System (GPS) receivers to cameras and audio recorders. Policies should cover the use of these features as they relate to work.

BYOD Policy Decision Table

**Device Choice** **User Experience and Privacy**

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>Analyzing employee preferences and understanding which devices they have already bought</li> <li>Defining an acceptable baseline of what security and supportability features a bring-your-own-device program should support</li> <li>Understanding the operating system, hardware, and regional variances around that baseline</li> <li>Developing a baseline of what security and supportability features a bring-your-own-device program should support</li> <li>Evaluation of devices are a</li> <li>Establishing the</li> <li>Ensuring the</li> </ul> | <ul style="list-style-type: none"> <li>Identifying the activities and data IT will monitor</li> <li>Clarifying the actions IT will take and under which circumstances</li> <li>Defining the BYOD privacy policy</li> <li>Critically assessing security policies and restrictions for sustainability</li> <li>Deploying core services (email, critical apps, WLAN access)</li> </ul> |
|---|---|

**This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**

**<https://e-janco.com>**

**Governance**

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>Identifying a</li> <li>issues on personal devices</li> <li>Defining remediation options (notification, access control, quarantine, selective wipe)</li> <li>Setting tiered policy</li> <li>Establishing the identity of the user and device</li> <li>Lending a critical eye to the sustainability of the security policy being instituted</li> </ul> | <ul style="list-style-type: none"> <li>Matching the trust level of personal devices</li> <li>Modifying app catalog availability based on device ownership</li> <li>Committing to the resource investment of building apps with personal devices in mind</li> <li>Updating app acceptable-use policies</li> <li>Defining enforcement levels for app violations (notification, access control, quarantine, or destruction)</li> </ul> |
|---|---|

**Liability** **Economics**

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>Defining the elements of baseline protection for enterprise data on BYOD devices</li> <li>Assessing liability for personal web and app usage</li> <li>Assessing liability for usage onsite vs. offsite, and inside work hours vs. outside work hours</li> <li>Evaluating whether the nature of BYOD reimbursement affects liability (partial stipend vs. full payment of service costs)</li> <li>Quantifying the monitoring, enforcement, and audit costs of the BYOD compliance policy</li> <li>Assessing the risk and resulting liability of accessing and damaging personal data (for example, doing a full instead of a selective wipe by mistake)</li> </ul> | <ul style="list-style-type: none"> <li>Shifting the cost of device hardware to the user and moving to a stipend model</li> <li>Controlling excess service charges through more responsible usage</li> <li>Establishing appropriate service plans, realizing some negotiating leverage might be lost</li> <li>Assessing the productivity impact of users being able to use their desired platforms</li> <li>Changing the help desk model (with BYOD, employees use the help desk as the last resort instead of a first resort)</li> <li>Reducing compliance and audit costs, <i>if</i> the legal assessment shows lower liability with personal devices)</li> <li>Assessing tax Implications</li> </ul> |
|--|--|

**Sustainability** **Internal Marketing**

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>Securing corporate data</li> <li>Minimizing the cost of implementation and enforcement</li> <li>Preserving the native user experience</li> <li>Staying up to date with user preferences and technology innovations</li> </ul> | <ul style="list-style-type: none"> <li>Communicating why the company is moving to BYOD</li> <li>Understanding BYOD is an HR initiative as much as an IT initiative</li> <li>Defining IT's "brand"</li> <li>Supporting the brand message with the appropriate action(s)</li> </ul> |
|--|---|

## Electronic Forms

Eight (8) Electronic forms are included with this policy template. They come separately in their directory.

BYOD Access and Use Agreement Form

Employee Termination Checklist

Mobile Device Security Access and Use Agreement Form

Mobile Device Security and Compliance Checklist

Telecommuting IT Checklist

Telecommuting Work Agreement

Work From Home IT Checklist

Work From Home Work Agreement

**This is a sample of the final product  
and these pages are for your review  
and are protected by Janco's copyright.**

**<https://e-janco.com>**

## IT Job Descriptions

Four (4) detailed job descriptions are included with this policy template. They come separately in their directory.

BYOD Support Specialist

BYOD Support Supervisor

Manager BYOD Support

Manager WFH Support

**This is a sample of the final product  
and these pages are for your review  
and are protected by Janco's copyright.**

**<https://e-janco.com>**

## What's New

### 2025 Edition

- ✚ Updated all included forms
- ✚ Updated all included job descriptions

### 2024 Edition

- ✚ Updated all included forms
- ✚ Updated all included job descriptions

### 2023 Edition

- ✚ Termination/end of relationship process added to the policy
  - Added Employee Termination Checklist
- ✚ Updated all included forms
- ✚ Updated all included job descriptions

### 2022 Edition

- ✚ Updated all included forms
- ✚ Updated all included job descriptions

### 2021 Edition

- ✚ Added Work From Home Best Practices
- ✚ Added four (4) electronic forms:
  - Telecommuting IT Checklist
  - Telecommuting Work Agreement
  - Work From Home IT Checklist
  - Work From Home Work Agreement
- ✚ Added a job description for Manager WFH Support
- ✚ Updated all included forms
- ✚ Updated all included job descriptions

### 2020 Edition

- ✚ Update section on device ownership options
- ✚ Updated all electronic forms
- ✚ Updated all attached job descriptions
- ✚ Updated all the included procedures to meet compliance mandates