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
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
- PDAs
- USB devices and data
- Laptop/notebook/tablet computers
- Ultra-mobile PCs (UMPC)
- Mobile/cellular phones
- Wearable devices
- Home or personal computers used to access enterprise resources
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

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
- Definite 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.

https://e-janco.com

© 2023 Copyright Janco Associates, Inc. -- ALL RIGHTS RESERVED -- e-janco.com
## BYOD Policy Decision Table

<table>
<thead>
<tr>
<th>Device Choice</th>
<th>User Experience and Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Analyzing employee preferences and understanding which devices they have already bought</td>
<td>• Identifying the activities and data IT will monitor</td>
</tr>
<tr>
<td>• Defining an acceptable baseline of what security and supportability features a bring-your-own-device program should support</td>
<td>• Clarifying the actions IT will take and under which circumstances</td>
</tr>
<tr>
<td>• Understanding the operating system, hardware, and regional variances around that baseline</td>
<td>• Defining the BYOD privacy policy</td>
</tr>
<tr>
<td>• Developing a light-touch certification plan for the evaluation of future devices</td>
<td>• Critically assessing security policies and restrictions for sustainability</td>
</tr>
<tr>
<td>• Establishing clear communication to users about which devices are allowed or not, and why</td>
<td>• Deploying core services (email, critical apps, WLAN access) to the employee</td>
</tr>
<tr>
<td>• Ensuring the IT team has the bandwidth</td>
<td>• Preserving the native experience</td>
</tr>
<tr>
<td></td>
<td>• Communicating compliance issues clearly to the employee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trust Model</th>
<th>App Design and Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identifying and assessing risk for common security posture issues on personal devices</td>
<td>• Designing mobile apps to match the trust level of personal devices</td>
</tr>
<tr>
<td>• Defining remediation options (notification, access control, quarantine, selective wipe)</td>
<td>• Modifying app catalog availability based on device ownership</td>
</tr>
<tr>
<td>• Setting tiered policy</td>
<td>• Committing to the resource investment of building apps with personal devices in mind</td>
</tr>
<tr>
<td>• Establishing the identity of the user and device</td>
<td>• Updating app acceptable-use policies</td>
</tr>
<tr>
<td>• Lending a critical eye to the sustainability of the security policy being instituted</td>
<td>• Defining enforcement levels for app violations (notification, access control, quarantine, or destruction)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liability</th>
<th>Economics</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Defining the elements of baseline protection for enterprise data on BYOD devices</td>
<td>• Reducing compliance and audit costs, if the legal assessment shows lower liability with personal devices</td>
</tr>
<tr>
<td>• Assessing liability for personal web and app usage</td>
<td>• Assessing tax implications</td>
</tr>
<tr>
<td>• Assessing liability for usage onsite vs. offsite, and inside work hours vs. outside work hours</td>
<td>• Assessing the productivity impact of users being able to use their desired platforms</td>
</tr>
<tr>
<td>• Evaluating what affects liability and costs (for example, hardware costs)</td>
<td>• Changing the help desk model (with BYOD, employees use the help desk as the last resort instead of a first resort)</td>
</tr>
<tr>
<td>• Quantifying the impact of users accessing and damaging personal data (for example, doing a full instead of a selective wipe by mistake)</td>
<td>• Establishing appropriate service plans, realizing some leverage might be lost</td>
</tr>
<tr>
<td>• Assessing the risk and resulting liability of accessing and damaging personal data (for example, doing a full instead of a selective wipe by mistake)</td>
<td>• Controlling excess service charges through more</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sustainability</th>
<th>Internal Marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Securing corporate data</td>
<td>• Communicating why the company is moving to BYOD</td>
</tr>
<tr>
<td>• Minimizing the cost of implementation and enforcement</td>
<td>• Understanding BYOD is an HR initiative as much as an IT initiative</td>
</tr>
<tr>
<td>• Preserving the native user experience</td>
<td>• Defining IT's &quot;brand&quot;</td>
</tr>
<tr>
<td>• Staying up to date with user preferences and technology innovations</td>
<td>• Supporting the brand message with the appropriate action(s)</td>
</tr>
</tbody>
</table>
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

2023

- 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

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