



BYOD Policy Template

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

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

Version 2.0

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
Policy	7
Device Requirements	7
Policy Definitions	8
Access Control	8
Security	9
Help & Support	10
Enterprise Mobile Device Infrastructure	10
BYOD Infrastructure	11
Disaster Recovery	11
Backups	11
Tablet Computer (iPads)	12
Internal Network Access	12
Repair Procedure	12
Upgrade Procedure	12
Patching Policy	12
BYOD Security Best Practices	13
Security Controls	13
Remote BYOD Management	13
Access Management Controls	13
Tablet and Smartphone Applications	14
BYOD Metrics and SLA Agreement	15
Executive management	15
Business unit executives	15
IT organization	15
Legal Considerations	17
Privacy	17
Record Retention	18
Appendix	20
Electronic Forms	21
BYOD Access and Use Agreement Form	
Mobile Device Security Access and Use Agreement Form	
Mobile Device Security and Compliance Checklist	
IT Job Descriptions	22
BYOD Support Specialist	
BYOD Support Supervisor	
Manager BYOD Support	
What's New	23

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
- ✚ 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.

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

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

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 detail 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 preference 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 evaluation of future devices
- ✚ Establish clear communication to users about which devices are allowed or not, and why

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

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

Global Positioning System (GPS)
over the use of these

BYOD Metrics and SLA Agreement

For CIOs and executive management, a balanced scorecard approach for BYOD service levels is an invaluable tool. That approach allows an enterprise to link the application of BYOD technology to enterprise operations using a "cause-and-effect" approach. Some have likened the balanced scorecard to an SLA solution which enables IT and business line managers to think together about what IT can do to support business performance.

Executive management often questions the benefits and risks associated with investments in IT and BYOD in particular. Below is a list of questions that executive management, business unit executives, and the IT organization as a whole have.

Executive management

- ✚ Does IT support the achievement of business objectives?
- ✚ What value does the expenditure on IT deliver?
- ✚ Are IT costs being managed effectively?
- ✚ Are IT risks being identified and managed?
- ✚ Are targeted intercompany IT synergies being achieved?

Business unit executives

- ✚ Are IT services delivered at a competitive cost?
- ✚ Does IT deliver on its service-level commitments?
- ✚ Do IT investments positively affect business productivity or the customer experience?
- ✚ Does IT contribute to the achievement of our business strategies?
- ✚ Corporate compliance internal audit
- ✚ Are the organization's assets and operations protected?
- ✚ Are the key business and technology risks being managed?
- ✚ Are proper processes, practices, and controls in place?

IT organization

- ✚ Does the enterprise develop the professional competencies needed for successful service delivery in a timely manner?
- ✚ Are we creating a positive workplace environment?
- ✚ Do we effectively measure and reward individual and team performance?

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

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

To that end, a balanced scorecard can be used to create effective SLA agreement between IT and the enterprise as a whole. An example of specific metrics is shown in the table that follows.

Component	SLA Metric
Customer Satisfaction	<ul style="list-style-type: none"> • Percentage customers satisfied with responsiveness • Percentage customers satisfied with cooperation • Percentage customers satisfied with communication with service support staff
Internal Infrastructure	<ul style="list-style-type: none"> • This is a sample of the final product and these pages are for your review and are protected by Janco's copyright. • https://www.e-janco.com
Quality of Information	<ul style="list-style-type: none"> • Range of information available on BYOD • Percentage of employees using BYOD effectively • Employee satisfaction with quality of work infrastructure • Percentage of employees satisfied with BYOD quality and scope of information
Financial Performance	<ul style="list-style-type: none"> • Cost per employee to support BYOD • Cost avoidance due to BYOD • ROI and productivity improvements due to BYOD • Percentage over/under IT budget • IT Budget as a percentage of revenue

Framework for a Balanced Scorecard for a BYOD SLA

A beneficial side effect of the use of the balanced scorecard is that, when all measures are reported, one can calculate the strength of relations between the various value drivers. For example, the relationship between BYOD usage and cost levels might infer that the usage of BYOD does not sufficiently contribute to results as expressed by the other (e.g., financial) performance measures.

Mobile Device Security and Compliance Checklist

Employee Name	_____	ID Number	_____
Job Title	_____	Location	_____
Device Type	<input type="checkbox"/> Phone <input type="checkbox"/> Tablet <input type="checkbox"/> Other	Description	_____

Security Controls

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	256 bit AES encryption per file at rest, 30-day rotating encryption key
<input type="checkbox"/>	<input type="checkbox"/>	256 bit SSL encryption data transfer
<input type="checkbox"/>	<input type="checkbox"/>	SSAE 16 Type II compliant, redundant data centers and DR policy
<input type="checkbox"/>	<input type="checkbox"/>	99.9% SLA Uptime Guarantee

Remote Device Management

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	Auto-timed screen logout on mobile devices
<input type="checkbox"/>	<input type="checkbox"/>	Custom 4-digit pass code
<input type="checkbox"/>	<input type="checkbox"/>	Immediate access restriction on device
<input type="checkbox"/>	<input type="checkbox"/>	Auto login to end user accounts for remote wipe

Access Management Controls

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	Prohibit access to App/Web UI from admin console
<input type="checkbox"/>	<input type="checkbox"/>	Prohibit access to content (folders and groups) from admin console
<input type="checkbox"/>	<input type="checkbox"/>	Domain Identity Control: SSO available on mobile apps

Compliance Disaster Recovery – Business Continuity

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	Has the user of this device completed all of the acknowledgement and use forms
<input type="checkbox"/>	<input type="checkbox"/>	Is this device and all of its data backed up
<input type="checkbox"/>	<input type="checkbox"/>	Is this device included in the Disaster Recovery Business Continuity Plan
<input type="checkbox"/>	<input type="checkbox"/>	Does this device meet the compliance requirements for the record management process
<input type="checkbox"/>	<input type="checkbox"/>	Has the user of this device completed all necessary training

Audit Trail

Yes	No
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

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

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

Employee Signature

Date

Manager BYOD Support

Position Purpose

The Manager BYOD Support is responsible for the overall coordination, control and maintenance of all personal mobile devices within the enterprise to ensure compatibility and integration with enterprise strategies. The supervisor reports to the Director Technical Services.

Problems and Challenges

The Manager BYOD Support is challenged with establishing and maintaining a high level of credibility for the function, enticing clients to consult with the function ensuring compatibility with enterprise strategies and maximize returns on investments. In meeting these challenges the Manager BYOD Support must constantly review, evaluate, plan and budget activities in this dramatically and constantly evolving technological arena. In addition, the manager must be cognizant of the latest releases of personal devices (hardware and software) and their security and application implications.

Essential Position Functions

Principal Accountabilities

- ▶ Identifies and initiates resolutions to user problems and concerns associated with the user's satisfaction.

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

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

- ▶ Presentation of mobile devices and procedures.
- ▶ Curriculum and provides to ensure maximum utilization
- ▶ to provide upgrades as necessary and ensure appropriate security levels are maintained.
- ▶ Upholds the enterprise policy guidelines as well as recommends new and improved guidelines to ensure compatibility and better serve users.
- ▶ Maintains current technical expertise in the rapidly changing technology of mobile devices.
- ▶ Utilizes state-of-the-art techniques when implementing hardware and software solutions.
- ▶ Interfaces with all of the various functions within IT and the enterprise to assure that the personal devices are utilized in a fashion that is consistent with the overall enterprise technology and business strategy.
- ▶ Prepares monthly status reports quantitatively reporting results of activities.
- ▶ Adheres and maintains a positive working relationship with all enterprise departments to optimize working relationships and communication.
- ▶ Fulfills department requirements in terms of providing work coverage and administrative notification during periods of personal illness, vacation or education.

What's New

Version 2.0

- ✚ Electronic Forms have been updated to meet the latest compliance requirements
- ✚ Added additional text for biometric security preferences
- ✚ Added 3 job descriptions
 - BYOD Support Specialist
 - BYOD Support Supervisor
 - Manager BYOD Support
- ✚ Electronic Forms and Job Description are provided as separate documents

Version 1.6

- ✚ Updated BYOD strategy and policy guidelines
- ✚ Updated all electronic forms
- ✚ Added Mobile Device and Compliance Checklist

Version 1.5

- ✚ Added SLA and Balance Scorecard metrics for BYOD

Version 1.4

- ✚ Updated to include strategy planning definition for BYOD policy
- ✚ Updated to include latest compliance requirements
- ✚ Updated BYOD best practices
- ✚ Updated BYOD Access and Use Agreement Form

Version 1.3

- ✚ Updated BYOD Access and Use Agreement Form
- ✚ Added Electronic Form Mobile Device Security and Compliance Checklist

Version 1.2

- ✚ Updated the BYOD Access and Use Agreement
- ✚ Added Device Access Security
- ✚ Added BYOD and Mobile Device Best of Breed Security Checklist
- ✚ Updated to meet all current compliance requirements

Version 1.1

- ✚ Added materials on disaster recovery
- ✚ Added materials on back-up of company intellectual properties

Version 1.0

- ✚ Policy Released