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 Choices ................................................................................................................................... 4

User Experience and Privacy ................................................................................................................ 5

Trust Security Compliance .................................................................................................................. 5

Application Design and Infrastructure ................................................................................................. 5

Economics ......................................................................................................................................... 6

Liability .............................................................................................................................................. 6

Maintainability ................................................................................................................................... 6

Internal marketing and training ........................................................................................................... 6

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

BYOD Access and Use Agreement Form ........................................................................................... 21

BYOD and Mobile Content Best of Breed Security Checklist ............................................................. 22

Mobile Device Security and Compliance Checklist ............................................................................. 23

What’s New ......................................................................................................................................... 24
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.
The BYOD strategy and resultant policy is 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 have been considered in 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
- 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 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 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 a 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?
- Do IT investments positively affect business performance or the customer experience?

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?
- Do we capture organizational knowledge to continuously improve performance?
- Can we attract/retain the talent we need to support the business?
To that end a balanced scorecard can be used to create effective SLA agreement between IT and the enterprise as a whole. An example with specific metrics is show in the table that follows.

<table>
<thead>
<tr>
<th>Component</th>
<th>SLA Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Satisfaction</td>
<td>• Percentage customers satisfied with responsiveness</td>
</tr>
<tr>
<td></td>
<td>• Percentage customers satisfied with cooperation</td>
</tr>
<tr>
<td></td>
<td>• Percentage customers satisfied with communication with service support staff</td>
</tr>
<tr>
<td>Internal Infrastructure</td>
<td>• Number of problems with BYOD devices and/or services</td>
</tr>
<tr>
<td></td>
<td>• Number of employees with BYOD</td>
</tr>
<tr>
<td></td>
<td>• Number of employees using enterprise BYOD devices</td>
</tr>
<tr>
<td></td>
<td>• Percentage of BYOD meeting information security compliance requirements</td>
</tr>
<tr>
<td></td>
<td>• Percentage of BYOD meeting records management needs</td>
</tr>
<tr>
<td>Quality of Information</td>
<td>• Range of information available on BYOD</td>
</tr>
<tr>
<td></td>
<td>• Percentage of employees using BYOD effectively</td>
</tr>
<tr>
<td></td>
<td>• Employee satisfaction with quality of work infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Percentage of employees satisfied with BYOD quality and scope of information</td>
</tr>
<tr>
<td>Financial Performance</td>
<td>• Cost per employee to support BYOD</td>
</tr>
<tr>
<td></td>
<td>• Cost avoidance due to BYOD</td>
</tr>
<tr>
<td></td>
<td>• ROI and productivity improvements due to BYOD</td>
</tr>
<tr>
<td></td>
<td>• Percentage over/under IT budget</td>
</tr>
<tr>
<td></td>
<td>• IT Budget as a percentage of revenue</td>
</tr>
</tbody>
</table>

**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.
## BYOD Access and Use Agreement Form

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>ID Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title</td>
<td>Location</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Tablet</td>
</tr>
</tbody>
</table>

Employee agrees to adhere to the BYOD and Mobile Device Access and Use Policy

- [ ] Yes
- [ ] No

ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices

- [ ] Yes
- [ ] No

A copy of the ENTERPRISE BYOD and Mobile Device Access and Use Policy has been given to the employee

- [ ] Yes
- [ ] No

### Equipment/Expenses

- Employee agrees to protect such equipment in accordance with ENTERPRISE guidelines.
- Employee is responsible for servicing and maintaining their own equipment.
- This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED
- www.e-janco.com
- ENTERPRISE will compensate the employee for any incremental costs associated with connectivity and upgrade of equipment to support the BYOD’s use on ENTERPRISE network or applications.

### Confidentiality/Security

- Employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage, and will comply with the privacy requirements set forth in the ENTERPRISE policy or procedure
- ENTERPRISE has the right to remotely wipe the contents of the device
- A pin number of at least 4 characters or numbers (or biometric scan i.e. fingerprint) will be utilized by the Employee and after 10 consecutive failed attempts ENTERPRISE has the right to automatically wipe the device
- All backups of the device will be to ENTERPRISE’s network and remain the property of ENTERPRISE

By signing this form, I affirm my willingness to abide by ENTERPRISE’s BYOD access policies, procedures and guidelines.

<table>
<thead>
<tr>
<th>Employee Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor</td>
<td>Date</td>
</tr>
</tbody>
</table>

© 2017 Copyright Janco Associates, Inc. -- ALL RIGHTS RESERVED -- www.e-janco.com
# Mobile Device Security and Compliance Checklist

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>ID Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title</td>
<td>Location</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Tablet</td>
</tr>
</tbody>
</table>

## Security Controls

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

- 256 bit AES encryption per file at rest, 30-day rotating encryption key
- 256 bit SSL encryption data transfer
- SSAE 15 Type II compliant, redundant data centers and DR policy
- 99.9% SLA Uptime Guarantee

## Remote Device Management

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

- Auto-timed screen logout on mobile devices
- Custom 4-digit pass code
- Immediate access restriction on device
- Auto login to end user accounts for remote wipe

## Access Management Controls

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

- Prohibit access to App/Web UI from admin console
- Prohibit access to content (folders and groups) from admin console
- Domain Identity Control: SSO available on mobile apps

## Compliance Disaster Recovery – Business Continuity

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

- Has the user of this device completed all of the acknowledgement and use forms
- Is this device and all of its data backed up
- Is this device included in the Disaster Recovery Business Continuity Plan
- Does this device meet the compliance requirements for the record management process
- Has the user of this device completed all necessary training

## Audit Trail

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

- All global files can be accessed directly from central admin console
- Usage statistics tracked for files, individual users and groups
- Downloads, uploads, previews
- Tracked by IP Address

---

**Employee Signature**

**Date**
What’s New

### 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