2013

Orb Data

Simon Barnes

[BRING YOUR OWN DEVICE POLICY]

This document specifies a sample BYOD policy for use with the Orb Data SaaS MDM service

Contents

1 ACCEPTABLE USE

Company [COMPANY NAME] grants its employees the privilege of purchasing and using Smartphones and tablets of their choosing at work for their convenience. Company [COMPANY NAME] reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of Company [COMPANY NAME]'s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

[COMPANY NAME] employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

1.1 General Rules

- The company defines acceptable business use as activities that directly or indirectly support the business of Company [COMPANY NAME].
- The company defines acceptable personal use on company time as reasonable and limited personal communication
- The employee will not download/transfer business data that is considered sensitive or confidential to the personal device
- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
- Company [COMPANY NAME] has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

2 DEVICES AND SUPPORT

Smartphones, tablets and laptops that are not on the company's list of supported devices **are/are not** allowed to connect to the network.

or [erase as appropriate]

Smartphones, tablets and laptops belonging to employees that are for personal use only **are/are not** allowed to connect to the network.

2.1 Smartphone Support

The following Smartphones are supported:

- Apple iOS (5.x, 6.x) iPhone
- Android (ARM) versions 2.2, 2.3x, 3.x 4.x
- Blackberry 4 - 7[1]
- Nokia Symbian
- Microsoft Windows Mobile 5.x, 6.0-6.1
- Windows Phone 8[3]

Devices that are not included in this list are not to be connected to the Company [COMPANY NAME]'s network without explicit permission.

2.2 Tablet/Laptop Support

The following Tablets/Laptops are supported:

- Apple iOS,
- Google Android
- Windows 8 professional[2]
- Windows RT[3]
- Blackberry 10[3]
- Windows XP[2]
- Windows 7[2]
- Mac OS X 10.3 – 10.8[2]

Devices that are not included in this list are not to be connected to the Company [COMPANY NAME]'s network without explicit permission

2.3 Connectivity

Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

[1] Managed through the Blackberry Management Extender, MDM license and access to Blackberry Server required.

[2] These devices are running native agents and will require an IEM lifecycle management license.

[3] Managed through the Exchange Extender, MDM license and access to Exchange Server required.

2.4 Mobile Device Management

Before BYOD devices are connected to the Company [COMPANY NAME]'s network the device must have an **IBM Endpoint Manager for Mobile Device Management** application (or agent) installed and configured.

To do this the device must be presented to IT for configuration or use supplied self-service processes to install and configure the agent.

2.5 Support

Support **will/will not** be offered for the devices that form part of this scheme.

The company [COMPANY NAME] will provide a forum for BYOD device issues. This will not be manned or run by the IT department but questions may be answered by IT department employees as time permits.

2.6 Loss or Damage of a Device

If the device is lost or damaged the employee is responsible for the purchase of a replacement device. A lower specification device will be available from the company [COMPANY NAME] whilst the replacement is purchased but will be lent for no longer than **2** weeks.

3 REIMBURSEMENT

3.1 Device Purchase

The company [COMPANY NAME] will/will not reimburse the employee for a percentage of the cost of the device)

or [erase as appropriate]

The company [COMPANY NAME] will contribute £xx.xx amount of money toward the cost of the device.

3.2 Tax Liabilities

[Delete section if employer is buying the device for the employee and will retain ownership.]

The tax liabilities accruing from the purchase of the device are the responsibility of the employee. The money given is considered to be salary and attracts tax and national insurance (both employee and employer). Thus an employee given £1000 who is a 40% tax payer will in reality only get £600 (less NI) and the employer will pay more in NI for making the grant.

In addition the device bought will be liable to VAT and will not be reclaimable by the company [COMPANY NAME].

3.3 Mobile Plan

The company will ***[erase as appropriate]:***

- Pay the employee an allowance
- Cover the cost of the entire phone/data plan,
- Pay half of the phone/data plan, etc.

The company will/will not reimburse the employee for the following charges:

- Roaming
- Plan over use charges

4 SECURITY

4.1 Mobile Device Security

The company security policy will be applied to all mobile devices.

This will enforce the following policy:

4.1.1 Passwords/PIN codes

[Change settings in red as appropriate. Current setting are based on Center for Internet Security (CIS) standard]

- Devices must be password protected using the features of the device
- The device must lock itself with a password or PIN if it is idle for **2** minutes.
- The device will be disabled after **6** failed login attempts
- Passwords must have the following settings:
    - An alphanumeric value
    - A minimum password length of **5** characters
    - Passwords will be rotated every **90** days
    - The new password can't be one of **24** previous passwords

4.1.2 Rooted or Jail broken Phones

Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

4.1.3 Applications

Employees are not allowed to download, install and use any app that does not appear on the company's list of approved apps.

The current list of approved apps are:

[add/remove apps as appropriate]

- Twitter
- Starbucks
- Dropbox
- LinkedIn
- Google Maps
- WhatsApp
- Trello
- Salesforce
- IBM Mobile Client

4.1.4 Cameras

Devices' camera and/or video capabilities **are/are not** allowed.

4.1.5 Websites

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.

The following web-sites are allowed:

[add/remove URLs as appropriate]

- www.ibm.com
- www.orb-data.com

4.1.6 Corporate Data

Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

Employees may use their mobile device to access the following company-owned resources:

- Email
- Calendars
- Contacts
- Documents

4.1.7 Remote Wipe of the Device

The employee's device may be remotely wiped if

1. The device is lost
2. The employee terminates his or her employment
3. IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure

While the company [COMPANY NAME] will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

4.1.8 USB Connection to Work PC

Only BYODs that provide FIPS 140-2 device-level encryption[4] may be connected to the company [COMPANY NAME] PCs for document transfer purposes.

4.2 Laptop Security

The company security policy will be applied to all laptop devices.

This will enforce the following policy:

4.2.1 Passwords

[Change settings in red and delete items as appropriate]

- Devices must be password protected
- The device must auto lock after **15** minutes of inactivity
- No accounts with blank passwords should exist on the system.
- Passwords should be a minimum of **8** characters.
- Maximum password age is **90** days
- System is set with a password protected screen saver
- Password is required on resume from sleep and hibernate.
- Guest account must be disabled

[4] (currently only Blackberry devices are certified as 140-2 compliant)

4.2.2 Software

The following company software must be installed and will be checked to ensure it is active and up to date on devices enrolled in the BYOD scheme.

[Change settings in red and delete items as appropriate]

- Anti-virus / malware
- Data loss prevention
- Firewall
- Encryption
- VPN Client
- Backup software

4.2.3 Encryption

All drives on the device must be encrypted.

4.2.4 Security Patches

All devices enrolled in the scheme will be automatically patched with the latest vendor supplied OS Security patches.

4.2.5 Application Security Patches

All devices enrolled in the scheme will be automatically patched with the latest application specific security patches.

4.2.6 Websites

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.

The following web-sites are allowed:

- www.ibm.com
- www.orb-data.com

4.2.7 Corporate Data

Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

Employees may use their laptops to access the following company-owned resources:

- Email
- Calendars
- Contacts
- Documents

5 RISKS/LIABILITIES/DISCLAIMERS

5.1 Risks and Liabilities

The employee bears the following risks and liabilities:

[Delete as appropriate]

i. The company reserves the right to disconnect devices or disable services without notification.
ii. Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
iii. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
iv. The employee is personally liable for all costs associated with his or her device.
v. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
vi. Company [COMPANY NAME] reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

5.2 BYOD Asset Register

All employee owned devices that are enrolled in this scheme will regularly update details on the BYOD asset register. This information collected will differ depending on the type of device. These details are required to allow devices to be identified, secured and configured.

i. **Hardware Information** - The details collected will differ depending on the device type, but will at a minimum contain the following:
   - Manufacturer
   - Model
   - Serial Number
   - Operating System
   - Operating System Patch Level
   - Device Ownership

ii. **Installed Software Information** - The detail collected will differ depending on the device type, but at a minimum will contain the following:
   - Application name
   - Application version

iii. **Access to Asset Register** - The following departments will have access to the details stored on the asset register
   - IT Support
   - IT Security

iv. **Employee Data Requests** - An employee has the right to request a copy of the data that is being held on their personal device that is registered with the BYOD scheme. A written request must be made to **emal@address.com**, data will be provided within 28 days.
v. **Removal of data from asset register** - When a devices is removed from the BYOD scheme the data stored on the Company Asset Register will be removed within 28 days.

5.3 Disclaimers

i. While the company [COMPANY NAME] will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

6 USER ACKNOWLEDGMENT AND AGREEMENT

It is the company [COMPANY NAME] right to restrict or rescind computing privileges, or take other administrative or legal action due to failure to comply with the above referenced Policy and Rules of Behaviour. Violation of these rules may be grounds for disciplinary action up to and including removal.

I acknowledge, understand and will comply with the above referenced security policy and rules of behaviour, as applicable to my BYOD usage of the company [COMPANY NAME] services. Should I later decide to discontinue my participation in the BYOD Program, I will allow the company [COMPANY NAME] to remove and disable any company provided third-party software and services from my personal device,

Employee Name: ____

BYOD Device(s: ____

IMEI Number: ____

Phone Number (if appropriate): ____

Employee Signature: ______________________________ Date: __________

Effective Date: [DATE]

Responsible Office: [OFFICE NAME]

----------------------------End of Document----------------------------