Sample BYOD Policy

February 27, 2017

1 Expectation of Privacy

⟨Department Name⟩ will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for ⟨Department Name⟩ provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

```
'department' says 'technician' canMonitor(Device)
  if Device mustBeProvisioned.

'department' says 'technician' canMonitor(Device)
  if Device mustBeInvestigated.
```

2 Acceptable Use

2.1

The company defines acceptable business use as activities that directly or indirectly support the business of ⟨Department Name⟩.

2.2

The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

2.3

Devices may not be used at any time to:

```
'department' says Employee:E can-say
  E hasAcknowledged('acceptable-usage').

'department' says Employee:E mustAcknowledged('acceptable-usage').
```

- Store or transmit illicit materials

- Store or transmit proprietary information

- Harass others

- Engage in outside business activities

- Etc.

2.4

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

- Email

- Calendars

- Contacts

- Documents

- Etc.

```
'department' says Device:D canAccess('email').
'department' says Device:D canAccess('calendars').
'department' says Device:D canAccess('contacts').
'department' says Device:D canAccess('documents').
```

2.5

⟨Department Name⟩ has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

```
'department' says Device mustEnable('hands−free')
  if Device isInCar.

'department' says Device mustDisable('speaker')
  if Device isInCar.

'department' says Device mustDisable('sms')
  if Device isInCar.

'department' says Device mustDisable('email')
  if Device isInCar.
```

3 Devices and Support

3.1

The following devices are supported:

- iPhone (3GS, 4, 4S, 5, etc...)

- iPad (⟨list acceptable models⟩)

- Android (⟨list acceptable models⟩)

```
'department' says IPhone3GS:Device isSupported.
'department' says IPhone4:Device isSupported.
```

- Blackberry (⟨list acceptable models⟩)

- Windows (⟨list acceptable models⟩)

- Etc...

3.2

Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

3.3

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

4 Security

4.1

In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.

4.2

The companys strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password cant be one of 15 previous passwords.

4.3

The device must lock itself with a password or PIN if its idle for five minutes.

```
'department' says Employee:E can-say
  E hasAcknowledged('internet-unreliable').

'department' says Employee:E mustAcknowledged('internet-unreliable').
```

```
'department' says Device mustInstall(App)
  if Device mustBeProvisioned,
     App isStandardInstall.

'department' says 'it-department' can-say
  App:A isStandardInstall.
```

```
'department' says Device:D mustEnable('password').
'department' says Device canConnectToNetwork
  if Device mustEnable('password').
```

```
'department' says String:Password isAcceptable
  if Password isCreated(Date)
  where geq(length(Password), '6') = true,
        largeAlphabet(Password) = true,
        leq(minus(today(), Date), '90') = true,
        novel(Password) = true.

'department' says Employee:U can-say
  Password:P isCreated(Date:D)
      where geq(D, delegatedAssertionDate()) = true.
```

The `delegatedAssertionDate` would probably have to be an obligation constraint, and would require some dark magic to implement.

```
'department' says Device:D mustLock
  where geq(idleTime(), '300') = true.
```

```
'department' says Device cannotConnectToNetwork
  if Device isRooted.
```

4.4

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

4.5

Smartphones and tablets that are not on the companys list of supported devices are not allowed to connect to the network.

```
'department' says Device cannotConnectToNetwork
  if Device isNotSupported.
```

4.6

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

```
'department' says Device cannotConnectToNetwork
  if Device isNotProvisioned.
```

4.7

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

```
'department' says Device canReadData(X)
  if Device isOwnedBy(User),
     User canReadData(X).

'department' says 'it-department' can-say
  Employee:U canReadData(Data:D).
```

4.8

The employee's device may be remotely wiped if:

- The device is lost or stolen.

- The employee terminates his or her employment.

- IT detects a data or policy breach, a virus or similar threat to the security of the companys data and technology infrastructure.

```
'department' says Device mustWipe
  if Device isLost.

'department' says Device mustWipe
  if Device isOwnedBy(User),
     User isNotEmployed.

'department' says 'it-department' can-say
  Device:D mustWipe.
```

5 Risks/Liabilities/Disclaimers

5.1

While IT will take every precaution to prevent the employees personal data from being lost in the event it must remote wipe a device, but it is the employees responsibility to take additional precautions, such as backing up email, contacts, etc.

```
'department' says 'it-department' can-say
  Device:D mustWipe.
```

5.2

The company reserves the right to disconnect devices or disable services without notification.

```
'department' says 'company' can-say Device:D isDisconnected.
'department' says 'company' can-say Device:D mustDisable(Feature:X).
```

5.3

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.

```
'department' says Employee mustInform('company', 'device-lost')
  if Device isOwnedBy(Employee),
     Device isLost.
'department' says Employee mustInform(Carrier, 'device-lost')
  if Device isOwnedBy(Employee),
     Device hasCarrier(Carrier),
     Device isLost.

'department' says Employee can-say
  Device isLost
  if Device isOwnedBy(Employee).
```

5.4

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the companys acceptable use policy as outlined above.

```
'department' says Employee:E can-say
  E hasAcknowledged('ethical-policy').

'department' says Employee:E mustAcknowledged('ethical-policy').
```

5.5

The employee is personally liable for all costs associated with his or her device.

```
'department' says Employee:E can-say
  E hasAcknowledged('financial- liabiliy -policy').

'department' says Employee:E mustAcknowledged('financial-liabiliy-policy').
```

5.6

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.

```
'department' says Employee:E can-say
  E hasAcknowledged('liabiliy-policy')

'department' says Employee:E mustAcknowledged('liabiliy-policy')
```

5.7

⟨Department Name⟩ reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

6 User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of ⟨Department Name⟩ services. I understand that business use may result in

```
'department' says Employee:U mustAcknowledge('this-policy')
  if Device isOwnedBy(U).
```

increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided.