2 Security Policy for Handheld Devices

2.1 General policy requirements

Policy agreement.

IT department MUST ensure that all employees (regular employees, interns, externals) using devices falling into the category “handheld devices” as defined in section 1.7, have acknowledged this security policy and the associated procedures before they are allowed to use corporate services using handheld devices.

```
'company' says 'it−department' can-say∞ Employee:U canUse(Device:D).

'it−department' says Employee:User canUse(Handheld:Device)
  if U hasAcknowledged('policy').

'it−department' says Employee:User can-say
  User hasAcknowledged('policy').

'it−department' says Employee:U mustAcknowledged('policy').

'it−department' says 'regular' isEmployee.
'it−department' says 'intern' isEmployee.
'it−department' says 'external' isEmployee.

'it−department' says 'pocket−pc' isHandheld.
'it−department' says 'smartphone' isHandheld.
```

Use of private handheld in corporate environment. IT governance MUST define whether private handhelds are authorized to connect to corporate networks in the user acceptance policy, according to its risk assesment policy.

```
'company' says 'it−governance' can-say Device canConnectToNetwork('corporate−network')
  if Device hasMet('risk−assesment−policy').
```

Private handhelds are not authorized: In highly restricted facilities, private handheld devices MUST be prohibited. In that case, mobile devices MUST be collected prior to the user’s entrance into the facility.

Private handhelds are authorized in offices but are not allowed to connect to internal networks.

Private handhelds MUST NOT connect to corporate networks and access corporate information. This includes synchronization with a workstation connected to internal networks. Corporate networks MUST be protected accordingly using network access control mechanisms and MUST NOT grant access to any corporate information to unregistered devices.

```
'company' says Device mustProhibitCollectAt(Location)
  if Device isPrivatelyOwned,
     Location isSecurityLevel('restricted').
```

Private handhelds are authorized: Any non business-owned (that, is private) device must be able to connect to ⟨Company⟩ network MUST first be approved by technical personnel such as those from the ⟨Company⟩ IT department or desktop support.

If allowed, privately-owned handheld devices MUST comply with this security policy and MUST be inventoried along with corporate handhelds, but identified as private. This is in order to prevent theft of corporate data with unmanaged handhelds (i.e. owner of device is not identified).

```
'company' says Device canConnectToNetwork('company−network')
  if Device isApproved,
     Device isActivated,
     Device isPrivatelyOwned.

'company' says 'technical−personnel' can-say Device isApproved.

'company' says 'it−department' can-act-as 'technical−personnel'.
'company' says 'desktop−support' can-act-as 'technical−personnel'.
```

IT department roles and responsibilities. IT governance is responsible for the mobile handheld device policy at ⟨Company⟩ and shall conduct a risk

```
'company' says 'it−department' can-say Device:X hasMet('mobile−handheld−device−policy').
'company' says 'it−department' can-say Device:X hasMet('approved−device−policy').
'company' says 'it−department' can-say App:A isInstallable.
'company' says 'it−department' can-say App:A isNotInstallable.
```

analysis to document safeguards for each device type to be used on the network or on equipment owned by ⟨Company⟩.

The IT department maintains a list of approved mobile handheld devices and makes the list available on the intranet. The IT Department maintains lists of allowed and unauthorized applications and makes them available to users on the intranet.

2.2 Physical security

Physical security. In case of loss or theft of handheld, users MUST report AS SOON AS POSSIBLE (right after the loss has been noticed) the IT department or help desk, in order to take the appropriate measures.

Procedure for reporting lost device MUST exist and be clearly communicated to all users:

To report lost or stolen mobile computing and storage devices, call the Enterprise Help Desk at +41-xx-xxx-xx- xx. For further procedures on lost or stolen handheld wireless devices, please see the PDA Information and Procedures section.

```
'company' says User can-say
  Device isLost
  if Device isOwnedBy(User).

'company' says User mustInform('enterprise—help—desk', 'device—lost')
  if D isOwnedBy(User),
     D isLost.
```

Device safety. Usage of handheld devices in uncommon situations is depicted in the acceptable use policy 0, which states that: Conducting telephone calls or utilizing handhelds while driving can be a safety hazard. Drivers should use handhelds in hand only while parked or out of the vehicle.

If employees must use a handheld device while driving, ⟨Company⟩ requires the use of hands-free headset devices.

```
'company' says Device:D canCall(TelephoneNumber:X)
  where inCar(D) = true,
        usingHandsfree(D) = true.
```

This seems very similar to section 5 of the NHS device policy.

Password policy. Access to handheld devices MUST be password-protected.

```
'company' says Device:D hasMet('password—policy')
  where passwordEnabled(D) = true.
```

Ownership information. Owner information SHALL be written on the handheld. Owner should be either end-user (if users are responsible for their device) or generic owner information to avoid revealing the company name and thus exposing the device to more scrutiny. This is possible in two ways, according to hardware capabilities:

```
'company' says Device can-say Device isOwnedBy(X)
  if Device isOwnedBy(X).

'company' says Device:D can-say D isOwnedBy(Company).
```

- Either the information can be displayed on the lockout screen on the handheld

- Or the information MUST be written on a sticker on the back of the handheld

This would allow anyone finding a lost device to return it to its owner.

Availability of device & services—business continuity. As handheld devices consume lots of resources (processing, memory), battery management is crucial to ensure business continuity. Mobile users working out of companys offices MUST have the necessary accessories to charge their device, according to the situation they are in: car, train, at customer sites, etc.

Batteries are consumed faster during the following operations, and devices should be switched off if not used:

- Wireless LAN (searching for nearby network)
- Encryption/decryption of communications

```
'company' says Device:D mustDisable('wlan')
  where usingBattery() = true.

'company' says Device:D mustDisable('encryption')
  where usingBattery() = true.
```

Similar to 3.11–3.13 of NHS policy.

Use of camera. Digital camera embedded on handheld devices might be disabled in restricted environments, according to ⟨Company⟩ risk analysis. In sensitive facilities, information can be stolen using pictures and possibly sent using MMS or E-mail services.

In high-security facilities such as R&D labs or design manufacturers, camera MUST be disabled. Furthermore, MMS messages should be disabled as well, to prevent malicious users from sending proprietary pictures.

```
'company' says Device mustDisable('camera')
  if ' restricted -environment' isWhereIs(Device).

'company' says Device mustDisable('mms')
  if 'high-security-environment' isWhereIs(Device).

'company' says 'high-security-environment' can-act-as 'restricted-environment'.

'company' says Location:L isWhereIs(Device:D)
  where location(D, L) = true.
```

2.3 Operating system security

Firmware version, updates & patching. Devices firmware MUST be up-to-date in order to prevent vulnerabilities and make the device more stable. Firmware patching and updating processes are the responsibility of the IT department, MUST be documented and tested prior to deployment on a whole fleet of handsets

```
'company' says Device mustBeUpdated
  if Device isRunningVersion(Version)
  where lth(deviceVersion(Device), Version) = true.

'company' says 'it-department' can-say Device:D mustRun(Version:V).
```

OS hardening: removing unnecessary services. In order to enhance the security level of end devices, all unnecessary built-in services should be disabled, especially including:

- Internet file-sharing
- FTP client

```
'company' says 'device' mustDisable('file-sharing').
'company' says 'device' mustDisable('ftp-client').
```

How do we check for this? Should device query if ∃ service that should be disabled?

System hardening: removing unnecessary applications. If employees have no reason to use certain file types (especially MP3s and videos), removal of the corresponding applications from the devices is recommended.

This not only prevents a devices being used as an expensive MP3 player, but it also protects the organization from potential legal problems regarding these types of media (DRMs infringement). Furthermore, removing unnecessary applications prevents attackers from exploiting implementation flaws in those applications.

Unsigned applications policy. Users MUST NOT install any UNSIGNED application or applications theme on the handheld device, for any purpose; this in policy order to prevent malicious infection of the device.

Certificates management. Only IT department staff are authorized to manage (install and revoke) certificates on handhelds. The IT department MUST provide the necessary certificates to enable all required services to users. Only the IT department can install certificates in the root certificates store or in the intermediate certificates store (if available).

Antivirus policy. Mobile devices MUST have antivirus software installed to prevent viruses from being vectored into the corporationeither as e-mail attachments or through file transfers. Antivirus software MUST be configured in order to:

- Do automatic signature update when connected to desktop PC or wireless network
- Do automatic and regular scan of device

2.4 Personal Area Networks (PAN) security policy

Bluetooth version. No Bluetooth Device shall be deployed on ⟨Company⟩ equipment that does not meet Bluetooth v2.1 specifications without written authorization from the Information Security Manager.

Any Bluetooth equipment purchased prior to this policy MUST comply with all parts of this policy except the Bluetooth version specifications.

```
'company' says App isNotInstallable
  if App isAssociatedWith('mp3').

'company' says App isNotInstallable
  if App isAssociatedWith('mimetype−audio−mpeg').
```

I need to fix bug in parsing due to unacceptable characters in strings (i.e. '*' and '.')

```
'company' says App hasMet('unsigned−applications−policy')
  if App isSignedBy(X).
```

```
'company' says 'it−department' can-say Certificate:C isValid.
```

```
'company' says 'av−software' canConnectToServer(URL:X)
  where connectedToWifi() = true.

'company' says 'av−software' canScan(Device:D).
```

There is a delegation relationship to the AV software in terms of its fuctionality and the requirement to have it installed, but I'm unsure how to express it. Software traditionally doesn't speak in AppPAL.

```
'company' says Device:D canEnable('bluetooth')
  where geq(bluetoothVersion(), '2−1') = true.

'company' says 'information−security−manager' can-say Device canEnable('bluetooth').
```

```
'company' says Device1 can-say Device1 hasPairedWith(Device2, PIN:P)
  if Device1 canPair(Device2).

'company' says Device:D1 canPair(Device:D2)
  where location(D1, 'restricted') = false.
```

The second part (re: reporting duplicate pairing attempts) seems tricky to express in AppPAL. Feels like a meta-policy about the state of a device's assertion context.

PAN PINs and pairing. When pairing two communicating devices in a PAN, users should ensure that they are not in a public area. If the equipment asks for a PIN after it has been initially paired, users MUST refuse the pairing request and immediately report it to IT department or the help desk. Unless the device itself has malfunctioned and lost its PIN, this is a sign of a hack attempt.

Care must be taken to avoid being recorded when pairing Bluetooth adapters; Bluetooth 2.0 Class 1 devices have a range of 100 meters.

File transfer (beam in PAN). File transfers between devices in close range (PAN), taking place over Bluetooth or Infrared, MUST take place only between authenticated parties, which MUST agree on a pairing key as defined in section 4.2: PAN PINs and pairing.

Anonymous connections (i.e. without pairing) MUST NEVER take place.

```
'company' says Device1 canSendTo(Device2, Data:X)
  if Device1 hasPairedWith(Device2, PIN),
     Device2 hasPairedWith(Device1, PIN).

'company' says Device1 can-say Device1 hasPairedWith(Device2, PIN)
  if Device2 hasStartedPairing(Device1, PIN).
```

PAN security audits. Information security staff SHALL perform audits for Bluetooth and IrDA to ensure compliance with this policy. In the process of performing such audits, information security auditors SHALL NOT eavesdrop on any phone conversation.

```
'company' says 'is-staff' canMonitor(Device:D, Feature:X)
  where ! X = 'conversation'.
```

Similar to NHS policy 3.14.

Infrared IrDA. Infrared support MUST be disabled if Bluetooth connectivity is supported. Bluetooth MUST be preferred to IrDA when available.

```
'company' says Device mustDisable('irda')
  if 'bluetooth' isOwnedBy(Device).
```

2.5 Data security

Information classification. The information classification policy applies restrictively to handheld devices as it applies to laptops.

A handheld device SHALL NOT be used to enter or store passwords, safe/-door combinations, personal identification numbers, or classified, sensitive, or proprietary information. Corporate documents are classified according to their level of confidentiality e.g.:

- Public documents
- Internal documents
- Confidential documents
- Strictly confidential or secret documents

```
'company' says 'device' cannotStore(Doc) if Doc isSecurityLevel('secret').
'company' says 'device' cannotStore(Doc) if Doc isSecurityLevel('strict-confidential').
'company' says 'device' cannotStore(Doc) if Doc isSecurityLevel('confidential').
'company' says 'device' cannotStore(Doc) if Doc isSecurityLevel('internal').
```

- Secret and confidential documents MUST NEVER be stored on end devices.

Internal documents SHOULD NOT be stored on mobile devices unless strictly necessary. Public documents can be carried on mobile devices without risk. However, if not needed, public corporate files MUST be removed from the device.

Data security. Mobile handheld devices containing confidential, personal, sensitive, and generally all information belonging to ⟨Company⟩ SHALL employ encryption or equally strong measures to protect the corporate data stored on the device, as stated in corporate encryption standards.

If memory encryption is not available natively in the device, a third party application SHALL be purchased.

```
'company' says Encrypted:Device canStore(Confidential:Doc).
```

Persistent memory. Corporate data, i.e. any corporate file, even public, MUST not be stored in persistent (or device) memory, but rather in memory card (SD or MMC).

```
'company' says 'internal' canStore(File:Doc).
'company' says 'external' cannotStore(File:Doc).
```

We could do this with app permissions, by prohibiting the `WRITE_EXTERNAL` permission.

Encryption of removable storage card. Removable storage on smartphones (e.g. SD cards) MUST be encrypted in order to prevent data theft on storage card.

Usually, encryption of MMC is natively built in devices. Encryption of MMC MUST be turned on. Third-party encryption software might be used if native platform does not offer the option of data encryption on MMC.

```
'company' says Device:D canInstall(App)
  if App isEncrypting,
    App isInstallable.

'company' says Device canInstall(App)
  if App isInstallable,
    Device mustEnable('mmc−encryption').

'company' says Device:D can-say
  D mustEnable('mmc−encryption').
```

2.6 Corporate networks access security

Network access control. All devices, including handhelds that have to connect to internal networks MUST be identified by IT department for Network Access Control purposes, after they are declared in the corporate inventory.

Any attempt to access corporate networks with an unknown device will be considered as an attack against corporate assets.

```
'company' says 'it−department' can-say Device canConnectToNetwork('internal')
  if Device isActivated.

'company' says 'it−department' can-say Device:D isActivated.
```

File sharing. File-sharing services MUST be disabled, independently of the transport technology.

```
'company' says Device:D mustDisable('file−sharing').
'company' says Device:D canEnable('file−sharing')
  if ' file −sharing' mustEnable('authentication').
```

If enabled, authentication MUST be in place to force the identification of the communicating party: no anonymous access shall be possible. Guidelines or a policy depicting valid passwords are available in the password policy.

Wireless support. Independently of the company risk analysis, disable WLAN support in the following cases: Whenever connectivity is not required to prevent unnecessary battery consumption.

When connected to a desktop computer to prevent the spread of malware.

Access to WLAN MUST be restricted if mobile workers do not require access to public, open, or untrusted WLAN, according to ⟨Company⟩ risk analysis and its business model:

- Restrict the list of authorized access points to corporate access points only.
- Disable connection to open/public WLANs without encryption and authentication methods.
- Disable connecting to WEP-protected WLANs (considered insecure).

```
'company' says 'device' mustDisable('wifi').

'company' says Device:D canConnectToAP(AP:X)
  if X isOwnedBy('company').

'company' says Device:D canConnectToAP(AP:X)
  if X canAuthenticateWith('wpa').
```

2.7 Over-the-air provisioning security

Handheld configuration for OTA provisioning. Mobile devices MUST be configured to receive provisioning files only from a list of trusted PPGs. This white list of trusted PPGs MUST contain corporate PPG IP address only, and eventually other PPGs owned by the operator.

This white list MUST be provisioned by security staff, and regularly pushed to end devices for security policy enforcement.

```
'company' says PPG:PPG can-say File:F isProvisioningFile
  if PPG isApproved.
'company' says 'security-staff' can-say PPG:PPG isApproved.
```

OTA provisioning messages security. Provisioning messages (using OMA DM or WAP Push) MUST be encrypted. Necessary SSL certificates MUST be provided by corporate IT department. Note that SSL certificates on OMA Device Management Server must be signed by a Certification Authority or by the Operator.

```
'company' says 'it-department' can-say Device:D isUpdatedBy(Update:U).
'company' says 'operator' can-say Server:S isUpdatedBy(Update:U).
```

2.8 Internet Security

Use of Internet services. Users MUST agree to the email security/acceptable use policy and eventually to the eCommerce security policy.

```
'company' says User canUse(Device)
  if Device isOwnedBy(User),
     User hasAcknowledged('email-security'),
     User hasAcknowledged('acceptable-use'),
     User hasAcknowledged('ecommerce-security').

'company' says Employee:U mustAcknowledged('email-security').
'company' says Employee:U mustAcknowledged('acceptable-use').
'company' says Employee:U mustAcknowledged('ecommerce-security').
```

Seems to add to the `canUse` policy in 2.1.

E-mail attachments download. Users SHALL NOT download files attached to e-mails. Restriction of attachment downloading can be implemented on both the device (via provisioning) and the mobile email server (via configuration). Attachment download restrictions MUST be implemented, preferably in mobile e-mail servers in order to prevent users tweaking the device security features.

```
'company' says Device:D mustDisable('attachment−download').
```