Mobile Security

How to Use Smartphones and Tablets securely in a Corporate Environment

General information

Sequence number:	001
Version:	1.0
State:	Final
Project:	Mobile Security
Author:	Werner Ansorge;Cédric Mauny
Date:	2014-04
Distribution:	CLUSIL members
Approval date:	2014-03-24
Approved by:	CLUSIL Management Board

Working Group

Name	Organisation
Werner ANSORGE	PayPal
Melanie CHEVALIER	ABN Amro
Adriana CULTRONE	Fortuna Banque
Myriam DJEROUNI	Cetrel
Philippe HOUGARDY (guest speaker)	Telindus Luxembourg
Guy ISLER	Centre Commun de la Sécurité Sociale
Serge MARELLI	CTIE
Cédric MAUNY	Telindus Luxembourg
Benjamin OBERMEIER	Ernst & Young
Cyril PIERRE-BEAUSSE	Avocat à la Cour / cpb.lu
Michael SIM	Governance, risk and compliance specialist consultant
Selim STITI	Deloitte
Raphael TABAN	ING
Tim van HONSTE	Symantec

Validation

Name	Role	Responsibility	Date	Signature
CLUSIL Management Board	Owner of the document	Validation before publication Approval for publication	2014-03-24	<CLUSIL>

Executive Summary

CLUSIL WG ISM (Working Group Information Security Management) addressed the topic of Mobile Device Security during a set of four sessions in 2012 where several speakers discussed security and counter-measures for mobile devices. Based on fruitful exchanges during these sessions it was decided to create a dedicated working group to develop supporting documentation addressing mobile device security and appertaining issues.

The target markets for this document are companies, organisations and other professionals wishing to ensure a secure mobile device environment whilst going about their business.

The goal of the document is to support persons responsible for an organisation's Information Systems (IS), such as Chief Information Officer (CIO) or Chief Information Security Officer (CISO), on how to address the request for usage of mobile devices in a corporate environment.

The focus of this document is limited to mobile devices only (such as smartphones and tablets). Laptops, netbooks, standard mobile phones or mobile device intentionally hacked or jail-broken are out of scope and therefore not considered.

Today, every company has to deal with employee requests who wish to use up-to-date, and privately-owned mobile devices for professional purposes. It is no longer possible to ignore the merge between professional and private life. This is emphasized by recent international studies that demonstrate that staff are now willing to use their own communication device for professional purposes with the possibility to use their social networks during their working day. Candidates often request this when negotiating their employment contract. It is no longer possible to ignore this. Therefore companies should consider this new trend and ensure incorporating appropriate controls, such as new policies, guidelines, and procedures as well as appertaining security solutions affecting such mobile devices. Company officials should be aware that mobile devices can be a medium for data leakage (i.e. disclosure of confidential information) and that this can lead to security breaches, affecting the company up to and including corporate legal as well as reputational risks.

To address this problem and help minimising said risks, this document will cover concepts for company owned devices (COD), Company-Owned-Personally-Enabled devices (COPE) and Bring-Your-Own-Device (BYOD). The objective being to support company officers choose the right concept and develop an appropriate strategy in line with company requirements.

In general it could be said that the most secure approach for a company is to prohibit all type of mobile devices. Unfortunately, in addition to endangering business, this may encourage staff to circumvent security policies, with the negative side effect that the company no longer controls data in the possession of the end-user.

A better solution is to accompany the change by implementing policies and procedures and appropriate security solutions regarding company devices. Decide on a strategy of either closed or enabled device for personal use. For instance, selecting only one brand (and line) for company-owned mobile devices and use appropriate management software would help to keep control over their mobile device environment. Additionally, it is recommended the organisation ensures appropriate staff awareness training in order that company end-users, at all levels within the organisation, understand and adopt correct behaviour to make the distinction between private and corporate information and adopt measures to protect data accordingly.

BYOD could be an alternative solution, but should only be an option and tolerated if the company's security processes are of a sufficient maturity level with regards to data confidentiality and if the risks can be addressed adequately from both the organisational and the technical viewpoints.

Table of Contents

Acronyms

BYOD	Bring-Your-Own-Device
CLUSIL	CLUb de la Sécurité de l'Information - Luxembourg
COD	Company-Owned-Device
COPED	Company-Owned-Personally-Enabled-Device
EMM	Enterprise Mobility Management
ISM	Information Security Management
MAM	Mobile Application Management
MDM	Mobile Device Management
MS	Mobile Security
OTA	Over-The-Air
PII	Personally Identifiable Information
VPN	Virtual Private Network
WG	Working Group

1. Introduction

1.1. Context

In 2012, CLUSIL WG ISM (Working Group Information Security Management) organised a set of working sessions on *Mobile Security*. As we consider this is an important topic, we decided to create a sub working group to elaborate a document regarding corporate security appertaining devices supporting this technology.

The Sub Working Group Mobile Security (Sub WG MS) met on a monthly basis between July 2012 and December 2013 to elaborate a document providing advice on how to meet the challenge and minimize risks related to mobile devices in a corporate environment.

This document is addressed to persons responsible for corporate Information Systems (IS), such as Chief Information Officer (CIO), Chief Information Security Officer (CISO) and all those interested in IS security (including security consultants) using mobile devices (i.e. end-users).

1.2. Objective

Nowadays mobile devices are increasingly part of our private and professional life and therefore more and more companies are challenged to integrate mobile devices into their corporate IS environment.

This objective can be realised in different ways, providing employees with approved corporate devices. Said devices being either not enabled for private use (COD) or enabled for private use (COPE = Corporate Owned Private Enabled), or allowing employees to bring their own device to be used in a corporate environment and enabled to perform their daily working tasks (BYOD = Bring Your Own Device) with their own devices. Each approach has its own risks and therefore it is important to raise awareness regarding related risks linked to this new mobile world and try to best protect against these risks.

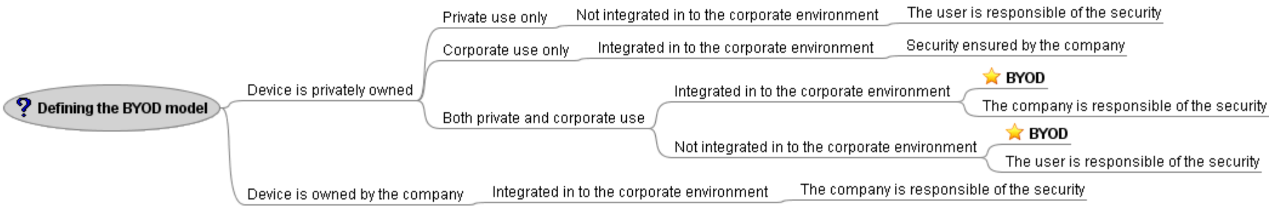

Defining the BYOD model
Device is privately owned
Private use only
Not integrated in to the corporate environment
The user is responsible of the security
Corporate use only
Integrated in to the corporate environment
Security ensured by the company
Both private and corporate use
Integrated in to the corporate environment
BYOD
The company is responsible of the security
Not integrated in to the corporate environment
BYOD
The user is responsible of the security
Device is owned by the company
Integrated in to the corporate environment
The company is responsible of the security

Figure 1: BYOD model

The main objective of this document is to give an overview about the current risk and threat landscape and advise on how to improve security levels from inception of such as project.

Agreeing on the adoption of a BYOD model requires due care and diligence to ensure that using mobile devices will be done in such a way that data leakage is minimised through the implementation of well informed security practices.

Note that most of the recommendations put forward in this document can be applied to both mobile devices as well as computers.

1.3. Scope and Exclusions

This document focuses only on mobile devices such as smartphones and tablets and does not focus on specific mobile device operating systems.

This document does not address laptops, netbooks, standard mobile phones or mobile devices intentionally hacked, rooted or jail broken.

2. Mobile Security Overview

The following chapters provide a general understanding of mobile security and why it is so difficult to address problems surrounding the subject matter.

2.1. Challenges

Ensuring mobile device security is, and will always be, a challenge for companies. Through the new upcoming consumerization effect it becomes even more challenging than ever before.

Today employees, independently of hierarchy, wish more than ever to use state of the art technology for professional working purposes. Should the company not provide it then they will seek possibilities to use their private, state of the art, mobile devices, and even using their own device for business purposes.

Thus companies should reassess their current posture and, perhaps, implement concepts to address, amongst others:

- Managing different brands and operating systems
- Dealing with employees expectations
- Securing corporate data on said devices all the while ensuring their usability
- Getting senior management buy-in and support in deciding what device types are allowed and what concept should be implemented (i.e. COD vs. BYOD)
- Educating employees to adopt prudent behaviour when dealing with mobile devices
- Addressing mobile device technology in such a way so as to ensure the company remains an attractive working environment in which employees may thrive.

A company able to integrate a mobile device strategy will not only minimize data leakage risks but will also satisfy employees.

2.2. History and current Trends

When looking at the history of mobile device, the release of RIM’s Blackberry 5810 in 2002 was a major evolutionary step towards the device we use today.

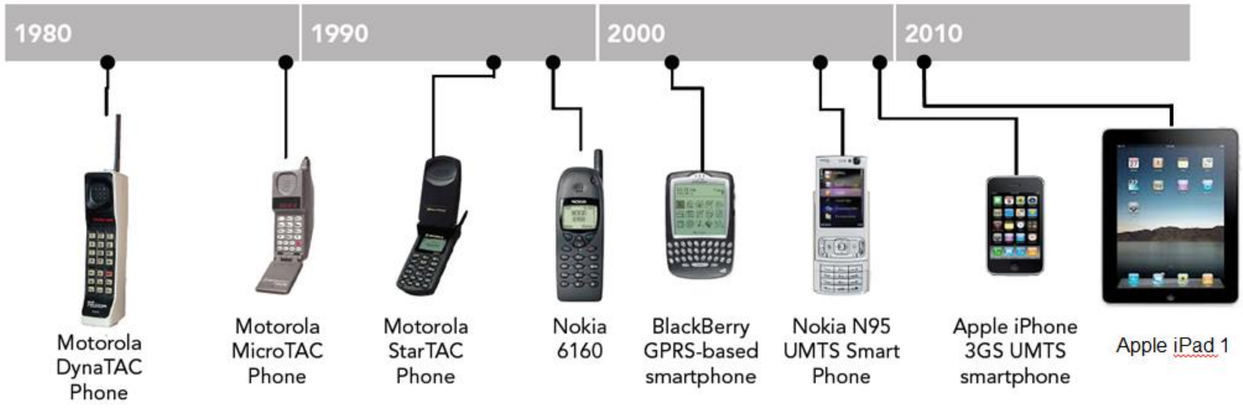
As the first device combining remote data access functionalities (email and calendar) with a phone ensured its place in history as the foundation of the mobile workforce.

Besides Blackberry, companies such as Palm Inc. (Palm Treo 180) and Hewlett Packard (HP Jornada 982) took up this trend by extending their personal digital assistant (PDA) device in 2002 with telephone functionality.

Even as the functionality of the devices increased, the features were still limited to mainly business related tasks such as remote access to email and calendar. As one of the major reasons it can be stated that until the year 2007 the 2G (GSM) network was the common telecommunication technology that only allowed for small size data transfer. Due to this the adoption was limited to companies providing this type of smartphone to their employees.

At the beginning, features and usability were limited due to bandwidth limitation of GSM and EDGE. Devices were mainly used by companies for email and calendar access of their workforce. Later, with the increase of so-called 3G networks, devices became more functional and at the same time private use increased.

The image below illustrates historical steps in the evolution of mobile devices.



All trademarks are the property of their respective owners.

Figure 2: Mobile evolution

2.3. Security Risks and Threats

With advances in mobile devices technology, the increase in risk to corporate data confidentiality through end-user data leakage also increases.

The probability that certain threats may materialise significantly are very real. For example it is easy to lose or have your smartphone, tablet or laptop stolen; this is not the case for a desktop.

Carelessly handling corporate data through unsecured cloud services or networks facilitates data leakage and disclosure of corporate confidential information, intentionally or not. The reasons are complex but it is mainly because mobile device users are not aware, nor do they understand, how to handle their devices securely. Added to which, companies have difficulties managing the multiplicity of mobile devices available on the market.

In general, the threat landscape has stayed more or less the same, but the scenarios have changed and users and companies alike are not yet ready to react accordingly to said changes. Therefore it is very important to implement an appropriate strategy with appropriate measures to minimise the risks as much as possible.

The following examples should provide an understanding of current risks and threats. Measures to minimise these risks and address the threats are discussed in chapter 4, “Recommendations for Mobile Security”.

Malware Threats

The mobile device threat landscape is increasingly similar to malware threats affecting standard computer systems. Increasingly malware targets the operating system itself and exploits security vulnerabilities of compromised app sandbox. The avowed aim being to gain unauthorised access to resources such as address books, geo-location data, photo/video database or browsing history and other personal data.

We should also mention that a mobile device could be the way into a standard computer system or network or when connecting for synchronisation purposes. In such a way an infected file (e.g. PDF) is copied to an exploitable system and could infect it when opened. As stated above, another threat could come from a compromised mobile device connected to a private or corporate network, i.e.. by using the mobile device the malware starts searching the network it is connected to for vulnerabilities to then exploit them, if at all possible.

The following attack examples all have the same goals, i.e. to exploit system and app vulnerabilities to access and download confidential data.

Virus Attack

Virus attacks are currently rare. But hacking capabilities are evolving and it is only a question of time for mobile device operating systems to be exploited directly more often.

Trojan Horses Attack

Threats through Trojan horses are already well known and were developed to access confidential information. They come via infected apps on the mobile device. App providers have addressed this issue by implementing check routines to verify if an app is clean of such Trojan horse functionalities but as these routines are, in general, automated processes it can happen that despite these checks an App gets approved.

Similar to Trojan Horses functionalities, apps can have hidden functionalities, implemented by app-developers to improve their service though not intentionally accepted or desired by the user. So, without formal user acceptance, confidential data can be collected by the app provider, which could be misused.

Besides these hidden threats, users might also be forced to accept access to confidential data in order for that app to run as desired. For instance, some photo apps require authorisation to access time and location data; some text message communication apps request access to the address book and request to upload it entirely to the app provider’s servers. In such cases users finally knowingly accept the disclosure and loss of control of confidential information and private information.

Drive-by-Attack

In September 2012 it was proven that browser apps can be exploited in a way to execute malicious code on a visited web site to give access to browsing history, photo/video data base and address book (NARAINE 2012).

Note: Please keep in mind that current Drive-by-Attacks will neither be able to install themselves to a mobile device nor modify the browser app. By closing the app the malicious code will disappear and the browser app used returns to its initial state.

Operating System Attack

Also in September 2012 a proof-of-concept (PoC) showed the possibility to manipulate the mobile phone’s operating system in such a way that either the SIM card is locked or the mobile phone wiped. It was only necessary to execute a code on the mobile phone for this attack to work. This type of attack can be performed in different ways, either by sending a text message, by visiting a web site (drive-by attack) or by scanning (e.g. a Quick Response Code / QRCode). Currently this exploit is only limited to a certain brand of operating system, but it already shows the weaknesses and hacking potential with a high risk factor.

Network Threats

Network threats require a different approach to protection than malware threats as in this case no app vulnerability gets exploited.

Wi-Fi Sniffing Attack

Attackers take advantage of end-users careless behaviour when connecting to unsecure network connections such as Wi-Fi access points in hotels, bars or public area hotspots. In such a way users might inadvertently connect to an attacker's access point with the same SSID as the official access point and become a victim of a man-in-the-middle attack. All their traffic can then be sniffed by the attacker. This could also include encrypted communications, as the attacker simulates an encrypted connection for the user where only the communication between the attacker and the destination web site is encrypted but not the communication between the user and the attacker.

GSM Network Sniffing Attack

The encryption GSM networks standard A5/1 was developed in 1987.

Although serious weaknesses were detected and numerous attack patterns have been published, this standard is still in use in Europe. It is not necessary to spend a fortune to purchase hardware and software freely available on the market to sniff and decrypt cell-phone (GSM) communications. This also includes the reception and decryption of text messages as the same encryption algorithm is used as for the communication itself.

Other Threats - Loss or Theft

Any state statistics demonstrate theft of mobile device, in particular smartphones, is one of the major threats.

Theft is generally motivated by the value of the mobile device itself (the hardware). Theft of mobile devices, except for targeted attacks, does not per se aim to obtain confidential and private information; but when a mobile device is stolen, all confidential and private information stored on it may be accessible to a hacker. Having said that, the loss itself may cause serious damage, especially if no backup is available for retrieving the information.

3. Law and Regulations

Laws and regulations, which we identified as important to companies are:

- Protection of personal data of customers – responsibilities of companies
- Protection of personal data of employees
- Protection of industrial and intellectual property

One should always consider the risk on personal data stored and managed by mobile devices and requirements from the Law in this regard.

The present information is subject to change consequent to the new EU Community Regulation prepared by the Commission and currently under review by the European Parliament.

3.1. EU wide

In this case as in many other, Luxembourgish law has to comply with EU legislation. So do our neighbouring countries. This theoretically reduces the risk of too much discrepancy between the present Luxembourgish law mentioned above and local laws, for instance in Germany or in France.

The main text that we consider here is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1].

Article 4 says that:

> *"Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*
>
> *(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law[2];"*

This is especially important in Luxembourg due to the nature of the country, the importance of cross border operations conducted from Luxembourg and the high number of border workers who might otherwise be subject to conflicting rules.

An employee accessing company data from across the border might be subject to different rules. However, it could be argued that the actual processing of the company and customer data is still located in the premises of the company (in Luxembourg) it is only the viewing of the result that is done in a different location. Although EU data protection authorities might not always retain this analysis, this would not create a problem insofar as access is made from another EU country.

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[2] Chaque Etat membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre; si un même responsable du traitement est établi sur le territoire de plusieurs Etats membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable.

3.2. Local (LU)

The relevant law is the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, as amended[3]". It regulates what companies must do e.g. declare any database they create to collect, hold and process private data to the CNPD. This goes further as any electronic processing should be declared and aspects such as type of processing, legitimacy, quality of the data etc. should also be considered

This is not a case where one actually *wants* to process (store, monitor..) personal information of the employees; however we're in the situation where the company *must* (and, for that matter, decides to) implement means to protect its own data and the data of its customers and employees. However, whether one wants or is somehow forced to this *surveillance*, it must be authorised by the CNPD.

Article 22 § 1 in particular states that

> "*The controller must implement all appropriate technical and organisational measures to ensure the protection of the data he processes against accidental or unlawful destruction or accidental loss, falsification, unauthorised dissemination or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. These measures will be contained in an annual report to be submitted by the controller to the CNPD*[4]."

So, companies actually (may) have a legal obligation to put in place all necessary measures to protect the data that employees may access from a mobile device. Such protection would encompass use of antimalware, firewalls as well as a VPN to protect communication over an unknown, uncontrolled network ("*in particular where the processing involves the transmission of data over a network*").

One should also read article 10 (which regulates monitoring activities applied to third parties, i.e. other than employees) and article 11 (which deals with employee monitoring).

Article 11 refers to article L.261-1 of the Luxembourg Labour Code, which specifies that employees *must be made aware* of surveillance, but also that their consent *never render surveillance legitimate*.. This means that the company should tell their employees that monitoring and protection takes place, but employees do not have to agree to this. Companies should always explain that the monitoring is not meant to spy on their employees (the CNPD would impose severe restrictions on such activities) but it is part of the company's responsibilities with regards to the protection of company information and personal identifiable information both of the employees themselves as well as those of the company's customers.

Art. L.261-1 of the Luxembourg Labour Code specifies that surveillance data may be used and processed amongst other for the purpose of

- protecting the assets of the company

[3] Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, telle que modifiée.

[4] Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement à la Commission nationale.

It is important to bear in mind that employees' consent "does not render processing carried out by the employer lawful[5]". In other words, consent by the employee (to monitoring) will not provide legal permission for "any form and extent of monitoring" (to the employee's personal data).

Articles 18 - 20 specify details with respect to sharing information with foreign countries. It may be relevant in situations where the company has offices (and data processing centres) abroad, which may be subject to different laws.

Art. 21 – 25 lists the obligations of companies and their employees to ensure the security of the data. This is where article 22, which we mentioned before, comes into play.

In particular, art. 23 has to be considered very carefully as, before describing a set of nine security objectives to reach, it describes criteria for defining the set of applicable security measures

- Risk on data subjects' privacy.
- State-of-the-art.
- Related cost.

The nine criteria listed are:

- *(a) prevent any unauthorised person from accessing the facilities used for data processing (monitoring of entry to facilities)*
- *(b) prevent data media from being read, copied, amended or moved by any authorised persons (monitoring of media);*
- *(c) prevent the unauthorised introduction of any data into the information system, as well as any unauthorised knowledge, amendment or deletion of the recorded data (monitoring of memory);*
- *(d) prevent data processing systems from being used by unauthorised person using data transmission facilities (monitoring of usage);*
- *(e) guarantee that authorised persons when using an automated data processing system may access only data that are within their competence (monitoring of access);*
- *(f) guarantee the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (monitoring of transmission);*
- *(g) guarantee that the identity of the persons having had access to the information system and the data introduced into the system can be checked and recorded ex post facto at any time and by any person (monitoring of introduction);*
- *(h) prevent data from being read, copied, amended or deleted in an unauthorised manner when data are disclosed and data media transported (monitoring of transport);*
- *(i) safeguard data by creating backup copies (monitoring of availability).*[6]

[5] Le consentement de la personne concernée ne rend pas légitime le traitement mis en oeuvre par l'employeur

[6] (a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations);

(b) empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports);

(c) empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire);

(d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);

(e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);

3.2.1. Private data vs. company owned data

Since we are talking about using company devices or private devices for mixed private/professional usage, we will specify what data is private and what data is considered company owned.

Personal e-mail received at a personal e-mail address, personal documents, music files, private photos and such will be considered to be the employees' private data.

E-mail with a professional contents or received for a professional purpose, on a company e-mail address or on some other address will be considered company data. It should be noted that using a personal e-mail address for professional use when a company e-mail address exists and is available should be prohibited.

3.2.2. Recommended action

A legal document should be written where the employee acknowledges that he has been made aware of his/her responsibilities with respect to the data he/she has access to and that he/she is aware that some kind of monitoring and data protection is necessary and may be enforced and that he agrees with this.

The document should indicate that usage of the device is subjected to the acceptance of the rules listed in the document. The employee is not forced to sign the document but he/she will not be allowed to use a (company owned or private) mobile device for professional use if he/she does not agree to the rules. Again, consent will not be a condition of the surveillance, only the CNPD's prior authorization is required.

In the case of a *company owened device*, the document should indicate that the device's main usage if professional and that private use is allowed (or prohibited, depending on the company policy).

In the case of a *personal device* that is occasionally (or frequently) used for professional usage (BYOD), the document shall describe the company policy accompanying such use. However, according to recent information, such a document may not be sufficient and might not be recognized by legal authorities. In fact it might be considered as "signed under duress (force)" and as such, invalid. The reader is strongly encouraged to ask for professional legal advice.

In this respect, one should bear in mind that Art. L.261-1 of the Luxembourg Labour Code states that employees' consent "does not render processing carried out by the employer lawful", and that the CNPD's prior authorization is required by law. This authorization always includes restrictions and conditions to monitoring activities, including where monitoring is applied to professional or company owned data.

The document shall further indicate that security measures are, or will be installed on the device and what those security measures are: encryption, antimalware, firewall, VPN, anti-theft software. If such is the case, the document should also indicate that the protection measures

(f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission);

(g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction);

(h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);

(i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité).

include the possibility of remote destruction (wipe) of part or all data on the device – in case the device is lost or stolen, or in case the employee should leave the company and be allowed to keep the device.

4. Recommendations for Mobile Security

Managing, mobile and remote equipment is not a simple matter.

Nowadays road-warriors (workers who travel a lot on behalf of the company) and other users need to be able to work from remote locations, or need to be able to use internal data, read (and sometimes write) documents and read and write e-mails, etc. This data is in general of a confidential and sensitive nature, such as private customers' data, company or customers' trade secrets and more.

There are two possibilities to access information:

- Either data can be stored on the mobile device or
- Users will access information & data from remote locations via remote access means.

Storing confidential information on any kind of mobile device carries with it a high risk because these device are small and, as previously stated, are easily misplaced, lost or stolen. Encrypting the whole device is not always possible, nor can such encryption always be trusted.

The following chapters provide advice to companies and private persons how to use and secure mobile devices in a better way.

4.1. Best Practices for End Users

The reader will find Best Practice advice to implement security settings for mobile devices. Independently of use, everyone should implement these settings.

Take care for your device

Mobile devices are more often lost than stolen. And sometimes those who find the device are honest and would like to return the device to its owner.

To this end, in case you lost your device, make sure that you, the owner, can be identified easily, so that an honest finder can return the device to you.

Advice:

A mobile device should be secured by means of a password. It is recommended to stick either a label with your name and email address on the device, or modify the background picture of the lock screen that it shows this information when the device is switching on.

Locking the device

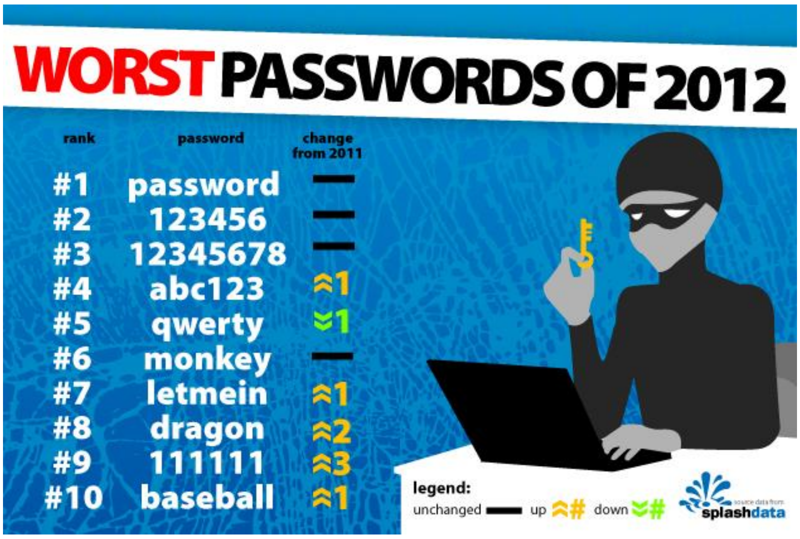
The password is often the only way to protect your privacy and data. Therefore it is important to enable the device's lock-screen function with a password.

It is recommended to enable "strong password" usage. The usage of the standard 4 digit code is not recommended as it can be brute-forced easily.

Advice:

1. Enforce a strong password policy. Rules for secure passwords should be even stronger for mobile devices than for information system or websites that are inside the (protected) corporate network.
2. Never lend the mobile device to another person
3. Never disclose the screen-lock password; including to family members.
4. Enable lock device with password when pressing the power key

5. Enable automatic lock device after several minutes' inactivity. It is strongly recommended to set it to maximum of 5 minutes
6. Do not forget to lock also your SIM card with the 4 digit passcode



WORST PASSWORDS OF 2012

rank	password	change from 2011
#1	password	—
#2	123456	—
#3	12345678	—
#4	abc123	↑1
#5	qwerty	↓1
#6	monkey	—
#7	letmein	↑1
#8	dragon	↑2
#9	111111	↑3
#10	baseball	↑1

legend: unchanged — up ↑# down ↓#

source data from splashdata

Figure 3 Bad passwords[7]

A strong password is a password which is hard to guess. Avoid words found in a dictionary and avoid personal information such as your wife's first name, car registration number, date of birth or name of the dog. Password length superior as 10 characters, with digits, an uppercase character and why not a special character (@, !, …).

Note:

Activating password protection provides an additional layer of protection to the mobile device, as this function also enables, on some mobile devices, the protection of the hardware encryption keys.

Please take in to account that only apps that make use of the hardware encryption will encrypt the information and only this information will remain encrypted as long as the password is not disclosed. This is also the case if a mobile device is jail broken or hacked.

Selecting Apps

Apps have to be selected carefully as they are the easiest way for hackers to compromise a mobile device and retrieve confidential information.

Two main principles need to be respected:

1. Use only reliable source for apps to avoid the risk of installing a malicious app.
2. Choose only apps that communicate through an encrypted network communication flow, i.e. including the login procedure.
   Try to select apps which do not request access to the address book, photo library and GPS data.

Note:

Be aware that providers of reliable sources also have difficulties ensuring that all provided apps are free of malicious code. They are limited in testing apps from A-to-Z for reliability.

[7] Source: ScaryLogins (http://www.splashdata.com/press/PR121023.htm)

Therefore, as an end-user, be always attentive and monitor the mobile device's behavior. A higher than usual telephone bill or short battery lifetime could be a sign, that the mobile device is compromised and that unauthorized services are running in the background.

Do not jail break or root your device

The process of jail breaking, or rooting, a mobile device will allow circumventing the in-built security and protection model of the operating system. Doing so enables installing apps from other and unknown resources than those allowed by the original providers. Apps installed from unknown and unsecure sources can be infected with malware and Trojan horses and are dangerous functionalities threatening any private and corporate environment.

Storage of sensitive data

Mobile devices are often used to store all kind of information, such as user credentials, passwords, credit card information, etc. to make life easier.

It is recommended to use an app which encrypts its content and which is password protected. If the mobile device gets lost, it is difficult to retrieve the stored information.

In general it is advised to use always a dedicated app that:

- Can be locked by a strong password
- Encrypts its content using the latest encryption standard and
- Was successfully tested by known organisations against any hacking attempts.

When using a cloud-based synchronisation service, it is recommended to take care that the app encrypts the data before sending. Additionally it is recommended to use a cloud service provider who ensures encryption of all data stored in its cloud.

Advice:

- Chose a dedicated app with high in-built security and encryption level and which takes advantage of the mobile device hardware encryption.
- Chose different password for each app and do not use the same as for the locking screen.
- Never disclose any passwords; including to family members.

Note:

Some mobile devices offer the possibility to add an external memory card to extend the memory capacity of the device. As such, memory cards can be easily removed, misplaced, lost or stolen, it is highly recommended not to store any confidential data on such memory cards.

Safe usage of Wi-Fi Hotspots

Data transmitted over a Wi-Fi network is not usually encrypted. This means that, if using an app not encrypting communication from the beginning, any information, be they passwords, e-mails or whatever are transmitted in a clear and readable format from the device to the endpoint. Said data can, thus, be intercepted by other computers connected to the same Wi-Fi network.

Consider the following:

- Use only encrypted Wi-Fi networks (WPA, WPA2 …).
- Hotspots, free access networks (e.g. in hotels, airports…) that do not support encryption, should be avoided.
- When using unknown Wi-Fi networks (e.g. in hotels, airports…) for private use, users should always connect to a secure version of the visited sites (HTTPS) and verify the validity of certificates.

- ***Connection to the corporate network or to any corporate node (e.g. e-mail, webmail) over unknown networks (e.g. in hotels, airports…) should only be allowed through a VPN.***
- Mobile device should be configured in a way that they do not connect automatically to any available network. Each connexion should always be (manually) initiated by the user.
- The ad-hoc mode of the device should be disabled to avoid any intruder connecting to the device.
- Disable Wi-Fi when it is not being used. Note that this will also save battery lifetime.

Safe usage of personal Wi-Fi Access Point at SOHO (small office / home office)

Wi-Fi access points should also be secured:

- Nobody can sniff the data traffic
- Unauthorised devices are not able to connect to it

Consider the following minimum guidelines for home access-point setup:

- When creating a SOHO Wi-Fi network, hide the SSID, that only those who know the name can connect to it
- Enable encryption (e.g. WPA2-PKS) and
  - Use a secure password fulfilling the standard requirements (i.e. at least 16 characters, including numbers and special characters; see also “Locking the device”)
  - Never disclose any passwords; including to family members.
  - Store the password in a safe place and don’t forget to keep a backup
- Limit the devices allowed in your network with their MAC address; i.e. only device part of the MAC address list are able to connect.

Safe Bluetooth usage

Bluetooth is a technology for devices that are in close proximity to one another (limited to max 10 metres). The connection between two devices is done via a pairing method, with a generated or manual pin code to give in.

Consider the following points for system setup and usage:

- Change the device’s name. Do not keep the original device name (“My iPhone 5” for instance). Knowing a device brand and model makes it easier for a remote hacker to identify vulnerabilities.
- Disable the “*discoverable*” mode, which allows everyone around to “see” the device and possibly get access to it. Only enable the discovery mode temporarily when pairing with a new device.
- Verify new connections (pairing) to ensure that pairing is established with the correct device.
- And disable Bluetooth when it is not being used. Do not hesitate to ‘forget a device’ (delete pairing) if you are sure you’ll never connect again with it.
  Note that this will also save battery lifetime.

Usage of a Firewall

Depending on the mobile device brand it is possible to install a firewall. This should be done to prevent unauthorized remote access.

The goal of the firewall should be to filter incoming traffic and block any unwanted remote connection. It could also protect device from Trojan horses that might initiate an internet connection to extract confidential data or to take control of your device.

Usage of Antivirus & Antispyware software

Depending on the mobile device brand, it is possible to install antivirus and antispyware software. If possible any device, whether company owned or privately-owned, should be protected by such software. Although the available software is not yet as powerful as computers versions, they might help protect against or detect accidental installation of malware.

Usage of remote detection and remote access

All remote connection possibilities (excluding remote-wipe functionality) on the device should be disabled to avoid that the device could be easily detected.

Such functionality can be made available by the operating system, or also by some installed apps, which broadcasts their service availability. In general apps are broadcasting over the Wi-Fi network and not the mobile network. Therefore, if possible, deactivating Wi-Fi and Bluetooth will help hide the mobile device from “curious” people.

Enable Remote-Wipe

This feature enables to remotely erase some or all data stored on the device should the device be stolen or lost.

Advice:

- Remote-Wipe feature should be enabled whenever technically and legally possible
- In addition activate the function to wipe the mobile device after 10 failed log-in attempts

Perform regular updates

Be careful and distinguish between operating system updates and application updates. Both are important, but operating system updates are more important.

- ○ *Regular update of the operating system of the mobile device*

  Automatic update must be activated, because every operating system have security breaches.

  The latest version of the mobile device’s operating system is dedicated not only to add new functionalities, but also to make the mobile device more secure.

- ○ *Regular update of the applications installed on the mobile device*

  Automatic update should be considered with attention.

  The latest versions of applications installed on the mobile device should not be considered as the safest as developers don’t necessarily provide application updates to improve security (for instance, updates can be issued to improve user experience). In particular, application updates may grant the application with different / additional access rights than those granted at the time of the initial installation of the application. Granting additional access rights may constitute a factor of risk and may, in particular, negatively impact the privacy of the owner of the mobile device.

Perform regular backups

Backup your personal data on a regular basis in order to keep it should you be forced to perform a remote wipe (through repeated entry of an incorrect password / pin).

4.2. Best Corporate practice

Besides the above-mentioned Best Practice, which we recommend always be implemented by default, organisations should consider much more when allowing mobile devices in the corporate environment.

The following advice should help introduce and manage mobile device in a corporate environment:

- Company-Owned-Device (COD)
- Company-Owned-Personal-Enabled-Device (COPED)
- Bring-Your-Own-Device (BYOD)

Note:

The advices for COD can be also considered as baseline approach for COPED and BYOD.

As mentioned in chapter 1.3 jail-broken and rooted mobile devices are excluded from the scope. But it could be a possibility for companies to consider jail breaking or rooting the mobile device operating system intentionally, if they have the internal competencies to harden operating systems and increase the security baseline.

4.2.1. Company-Owned-Device

Assess Threats and Risks

It is essential for the business to have a comprehensive overview regarding threats and risks imposed through using mobile device technology. This helps to define security requirements and select the right solution(s) to securely handle mobile device.

Assess Data Access by Population

Senior management and other company road-warriors need access to different data and different access rights (read, write, modify) than do employees who remain desk-bound.

Therefore it is important to assess and classify data according to sensitivity and restrict access rights according to specific user types. Justified exceptions should be tolerated, though these should be weighed according to merit and specific business needs (e.g.: business continuity key persons). Thus, think Role-based Access Controls.

Implement a Mobile Device Security Policy

A Mobile Device Security Policy is essential to protect corporate data, this not only applies to data hosted on the mobile device but also of all data accessible from the corporate infrastructure.

Independent of the chosen approach (COD, COPED, BYOD), the Mobile Device Security Policy should address mandatory rules regarding strong password settings, acceptable use of the device, device ownership, intellectual property ownership, user responsibilities as well as penalties for non-compliance. This list is not exhaustive and needs to be adapted according to company needs. The mobile security policy should be inline with Corporate Security policy, regularly monitored and reviewed.

Should employees want to use mobile devices to access corporate systems (networks, data), then they must sign off to acknowledge the Mobile Device Security Policy.

Employees unwilling to accept the Mobile Device Security Policy should be prohibited to receive a company owned device or access to the corporate network via their own mobile device.

Establish an Exit Strategy

A company needs to ensure that sensitive corporate information does not leave the company when an employee leaves said company. Therefore it is important to setup an Employee Exit Strategy.

- Regarding COD, the solution is to retrieve the device from the user upon his leaving the company.
- COPED is a little more complex as the company needs to be assured that the employee can keep the device including his private data though not the company data. The company also needs to ensure that the ex-employee’s private date is not stored on its backup systems stored on its corporate network

Device Selection and Purchase

The company’s mobile device pool needs to be as homogeneous as possible to ease its management.

Therefore it would be a wise to select one brand only and to remain with that brand as long as possible. Should a new model be released try to exchange the “old” device for the new one as soon as possible.

Focus your purchasing / leasing strategy only to reliable and well known vendors to ensure mobile devices are not tampered with prior to delivery. If possible carry out due care and diligence during the supplier selection process.

Test the device to ensure hardware, selected management solution and apps fulfil the security, reliability, availability requirements.

Set clear Purchasing Policies applicable to all corporate divisions. Such policies should be applicable not only to mobile device but any and all equipment and services.

Device and App Management

System administrators cannot expect to have the same access to mobile device clients as they would have to corporate desktops. Lack of access, combined with operating system heterogeneity, complicates routine tasks such as deployment, configuration settings, application installations and help-desk tasks. Each mobile device has unique management requirements and tasks often must be performed remotely, over-the-air (OTA).

There are two categories of software (or software solutions) which may help when considering using mobile devices in a corporate environment:

- Mobile Device Management software (MDM), and
- Enterprise Mobility Management software (EMM).

Mobile Device Management (MDM)

MDM software secures monitors, manages and supports mobile device deployed across mobile operators, service providers and enterprises.

MDM functionality typically includes OTA distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, mobile computers, mobile printers, mobile POS devices, etc.

MDM can be used with **COD**, **COPED** and **BYOD.**

Enterprise mobility management (EMM)

EMM systems generally provide middleware to automate management tasks and insulate administrators from the complexity of performing tasks on many different types of device. It also provides infrastructure to securely administer devices OTA and self-management portals, enabling users to download updates and applications by themselves are other common features.

Typically, solutions include a server component, which sends out the management commands to the mobile device, and a client component, which runs on the end-user's handset and receives and implements the management commands.

Independent of the chosen category (MDM or EMM) it is important to ensure that the OTA capabilities of the selected software fulfils the requirements.

Requirements could be:

- The ability to remotely configure a single mobile device, an entire fleet of mobile devices or any IT-defined set of mobile devices
- Send application and OS updates
- Remote policy enforcement
- Automatic backup
- Remotely lock and wipe a device, to ensure data stored on the device remains secured when lost or stolen, and
- Remote troubleshooting.

EMM is more suitable for **COD** and **COPED** management models.

Note:

Please keep in mind that for **BYOD,** performing a remote wipe or, indeed, for forensic analysis on a privately owned mobile device may not be legally possible.

Safely providing Company Information

Web applications or virtualisation could be an alternative to ensure company information security to MDM or EMM.

Note:

Be aware that, providing corporate information via web application or virtualisation does not prohibit against taking screenshots or copying data to the personal mobile device.

Web Application

By providing information via web applications, employees' access and update corporate information by means of a web browser on the mobile device. In this case both the data and the applications reside on the web server hosted in a controlled environment (think "highly secured data centre"). No data is copied and stored on the end user devices.

Each employee should be provided with a login id and password pair that can be revoked by the administrator at short notice. Additional security can be provided by using two or three-factor authentication (or two-step log-in). Session security is provided by the proven SSL VPN connection security and encryption technology.

Access permissions to different applications and data sets on the system can be granted or removed from users and user groups by the administrator. No installation is required on the end user's mobile device.

Virtualisation

Virtualisation is the simulation of the software and/or hardware upon which other software runs. The usual goal of virtualization is to offer a secure environment (sandbox) and to centralize administrative tasks while improving scalability and overall hardware-resource utilization

Virtual desktop infrastructure (VDI) is one form of desktop virtualization. It can be viewed as a more advanced form of hardware virtualization. Rather than interacting with a host computer directly via a keyboard, mouse, and monitor, the user interacts with the host computer using another desktop computer or a mobile device by means of a network connection

Mobile virtualization is a technology that enables multiple operating systems or virtual machines to run simultaneously on a mobile phone or connected wireless device.

Label Mobile Device

In case the mobile device gets lost should a third party find he/she should have the possibility to return the device easily to the company.

Recommendation:

Add the mobile device to company's asset management system, the ITIL CMDB process is a good example on how to go about this. Labelling each asset is one way to ensure asset traceability. The asset label should guide third parties finding the device to a SPOC[8] address in order to be able to return said lost/found asset. Those who designed the unique asset id labelling methodology should ensure that the label only displays the minimum information to effectively return the asset whilst still protecting the asset from data leakage..

Limit company data on the device

By definition, mobile device are portable and can easily be lost or stolen.

It is advised that no corporate data should ever be stored on a mobile device, to avoid disclosure of confidential data in case the device gets lost or stolen (including laptops). In case corporate information is needed during a professional travel, though not always feasible, the information should be stored on a corporate server and accessed remotely, e.g. via the above mentioned solutions (web application, virtualisation, company dedicated apps).

Data backup

Mobile device have to be included into the standard backup process like any other device.

The backup strategy for mobile devices should be added to the corporate backup policy.

Awareness Training

Employees must be made aware regarding data sensitivity matters, It is one of the most important part of IS security. Technology alone cannot fulfil all the conditions required by

[8] SPOC: single point of contact

information security. Nevertheless, the tools to ensure data protection must be made available by management, through adequate commitment and funding to ensure users can meet business security objectives.

One approach to data protection is to declare, by means of a policy, that all information not specifically identified as Public should, and must, be considered as for Internal Use Only and, as such, all supporting technologies will be configured to ensure data is protected accordingly. End users, road-warriors specifically, are required to ensure they protect corporate data by doing all that is in their power to align to the corporate information security strategy by respecting, among others, Acceptable Use, Password & Wi-Fi hotspot policies.

Data Classification is another way of ensuring sensitive data is adequately protected. Once a data classification process is rolled out within an organisation, corporate users need to be able to easily recognise data not meant for public consumption without prior management approval.

Road warriors must understand that their mobile device could represent a danger to the organisation in case of non-respect of security rules.

A standard awareness program should be defined describing the basics of information security (threats, vulnerability, availability…) and should contain a specific chapter regarding mobile security covering:

- Data sensitivity, remote access, device configuration and
- Risks for the company and for the user in case of misuse of mobile device.
- Specific mobile device technology risks and how to cope with them.
- Shoulder surfing by undesirable third parties
- The awareness program should be mandatory and repeated at least once a year.

Note: It is recommended to provide examples and advice that the employee can apply at home and to their own mobile device. This added value will hopefully have a long-term effect for a better security behaviour and culture.

4.2.2. Additional Requirements for COPED

Providing mobile devices to employees is a challenge. Enabling them also for personal use increases the challenge for mobile security significantly, but with the advantage, that companies still keep the device ownership and therefore are able to monitor and control its content and settings.

Additionally to advice contained in “4.2.1. Company-Owned-Device” companies should consider satisfying data protection and mobile security needs if employees are also allowed to use it for private use.

Note: Companies should state that they take no responsibility for any private application and data. The user will remain the data and application owner and needs to ensure all measures not to lose his data in case of incidents.

User guidelines

The user guideline should extend mobile security policy through rules regarding what users are allowed to do (Acceptable Use policy). If it is a separate document employees must sign it.

Data backup

For personally enabled mobile devices, it has to be considered that the data backup also includes the user’s private data. The data backup policy and user guidelines should mention this point and highlight that the company takes no responsibility for recovering private data.

It remains the company's prerogative to decide and setup a backup strategy for private data. Depending on this decision, an appropriate device management solution that fulfils the strategy requirements should be implemented. If possible, the solution should provide sufficient flexibility to distinguish between company and private data backup and restoration processes.

Device and App Management

Chapter of "4.2.1. Company-Owned-Device" provides advice as to what solutions are available to securely manage mobile device.

The final decision as to which solution is the best, depends on the company's mobile device strategy, taking into account the additional COPED related requirements. The main focus should be on functionalities to distinguish and manage:

- Corporate and private data,
- Backup and restoration, and
- Remote wipe.

4.2.3. Special Requirements for BYOD

We do not recommend implementing BOYD in a corporate environment, because no IS security measure is able to create an acceptable security level regarding company data when allowing personal device to access and process them. Not to mention all the difficulties of managing the IS security measures on all device brands and their different operating system versions.

Note: Senior management should never bring / use their own device for business purposes as they handle highly sensitive data. Try to convince senior management to only use COD using cost saving arguments such as device security and simplified trouble shooting by the company's service desk.

BYOD should only be considered as an alternative, but only if the security posture of the company shows an acceptable risk level with regards to sensitive data, after having assessed risks and after having lead a cost / benefit analysis.

If deciding for BYOD we consider it really important that the company implements the right management mobile device solution, one which fulfils the company's expectations regarding security and the expectations of the device owners that their personal device is not restricted in any way.

This should come in addition to setting up an appropriate organisational, legal and governance framework within the company addressing human resources, legal and compliance issues. Note that BYOD implies more governance than COD and COPED.

Following rules need to be followed when deciding for BYOD

- The company will not manage the device
- Give access only to company information via
  - Appropriate Mobile Application Management (MAM) tool
  - Web applications
- Deny jail broken or rooted device to access to company information via
  - Appropriate Mobile Application Management (MAM) tool
  - Web applications
- Implement a mobile device security policy
- Create guidelines for use of personal device in a corporate environment
- State penalties as defined in the corporate policy

- Give no access to the corporate network
- Do not allow synchronisation of corporate email, calendar and contacts
- Grant Internet access only through separate and dedicated network (e.g. guest account)
- Train employees
- Define an employee exit strategy

Deny Jail breaking / Rooting

The company should not provide or allow access to corporate information via MAM tool and / or Web applications on jail broken or rooted mobile devices.

The company should install a MAM tool that is able to detect if the device owner jailbreaks or roots his mobile device. If this tool detects such an action then all access to corporate data has to be denied and/or removed from the device immediately. To jailbreak or root a device is considered as a serious security breach and, although it is a private device, penalties should be clearly stated and agreed upon in advance.

Device management

The personal device is subject to privacy and therefore only the owner can manage it.

It is advised that the company has no intention to manage the personal devices.

How to manage company information on a personal device

If a company intends to provide access to company information via the personal mobile device, it is advised to use at a minimum Web applications or a Mobile Application Management (MAM) tool.

Such a MAM tool provides a type of Sandboxed Appstore (managed by the company) to provide secure access to company approved or developed applications and to company content. This technology is called Mobile Application Management (MAM). This allows the company to concentrate on the content that it wants to share with the BYOD users and the company can enforce sufficient security measures around this content such as strong passwords, two factor authentication, prohibiting sharing content from within the sandbox with the device or other applications, VPN connections, encryption and even DLP.

With this technology it doesn’t matter what device they bring into the company as long as it’s an iOS or Android (and even limited support for Blackberry and soon also Windows RT support).

Note: The chosen solution should be in line with the “Employee Exit Strategy”.

Mobile Device Security Policy

The same mobile device security policy as for that of a corporate device needs to be implemented, as the same strict security rules have to apply to private devices as for corporate mobile devices.

In addition, the corporate security policy should explicitly state that jail-broken and rooted device are prohibited and penalties can be imposed if such a device is detected.

The mobile device security policy should be inline with Corporate Security policy, regularly monitored and reviewed.

Network access

It is not advised to provide corporate network access to a personal mobile device, as a personal mobile device should be always classified as unsecure. Corporate network access should be prohibited by default for any such device population.

If a company wants to allow at least Wi-Fi Internet access, then this should happen through a dedicated “guest” account. This Wi-Fi network should be well separated from the corporate network but monitored as the provider of an Internet access (i.e. the company) stays responsible for any activity of the user.

Awareness training

The awareness training has to be modified to cover BYOD related risks and threats. I.e. the employee has to be informed regarding corporate data sensitivity and must understand that his mobile device could be a danger in case of a non-respect of the specific rules of the company’s BYOD mobile security policy.

Employee Exit Strategy

Companies should consider the consequences regarding corporate data when personnel leave the company. It is not as simple as having an employee return a company device and just disabling his access rights. And from a legal perspective it is also not possible to carry out mandatory device-wipe on privately owned device (see the chapter on laws and regulations).

Therefore especially for BOYD it is important to choose, early on in the design stage, an appropriate management strategy and software, so as to be able to remove corporate data from the personal mobile device, without impacting the owner’s private data.

5. Appendix

5.1. Appendix 1 – Checklist

The following checklist is not exhaustive, but should support the mobile device management in a corporate environment.

#	Subject	Applied (Yes/No)
Best Practices for End Users		
1	Enable screen lock with strong password	
2	Enable automatic device lock after 5 minutes of inactivity	
3	Use dedicated app(s) to encrypt and store sensitive information	
4	Store sensitive data only encrypted in a private cloud service	
5	Disable automatic connection to known networks	
6	Hide SSID of personal Wi-Fi access point	
7	Encrypt Wi-Fi communication of personal Wi-Fi access point with strong password	
8	Limit access to personal Wi-Fi access by using a MAC address filter list only for authorised devices	
9	Change default device name	
10	Disable Bluetooth "*discoverable*" mode	
11	Install a firewall if possible on the mobile device	
12	Install antivirus & antispyware software if possible on the mobile device	
13	Disable all remote detection & connection functionalities of • Operating system • Installed app(s)	
14	Enable remote-wipe	
15	Enable remote discovering of mobile device	
16	Enable wipe after 10 failed log-in attempts	
17	Perform updates of • Operating system • Installed app(s)	
18	Perform regular updates	

19	Label mobile device with owner's contact information	
Best practices for Companies		
20	Assess threats and risks	
21	Assess population for data access	
22	Create a mobile security policy	
23	Create an exit strategy	
24	Keep mobile device environment homogenous	
25	Keep an inventory of all used mobile devices	
26	Set rules for brand and device purchase	
27	Choose a management solution (EMM or MDM)	
28	Provide safely company information via • Web applications • Virtualisation	
29	Find solution to deny or limit storage of company data on mobile device	
30	Include mobile device to corporate's backup strategy	
31	Conduct awareness training	
Additional requirements for COPED		
32	Create User guidelines for mobile device	
33	Decide how the company will consider private data for backup and restoration	
34	Adapt backup strategy/policy according to the decision how company will handle private data	
Special Requirements for BYOD		
35	Deny jail-broken / rooted device if access to corporate information via a secure solution is requested	
36	Refuse any management of private mobile device	
37	Implement a MAM to keep control over corporate data	
38	Implement a dedicated mobile device security policy for BYOD	
39	Allow only Internet access via a guest account	
40	Deny all network access to corporate network	
41	Conduct a dedicated awareness training for BYOD	

42	Create a BYOD related exist strategy	
43	Deny synchronisation of email, contacts and calendar	

5.2. Appendix 2 – Working sessions on Mobile Security

CLUSIL WG ISM organised four working sessions on the topic of Mobile Security. A different guest speaker on a predefined subject presented each session so that CLUSIL participants might benefit from the speakers' experience.

Authors of this document want to thank each of these guest speakers. CLUSIL would also like to thank their members for attending said presentations.

Session of 2012, May 24th

Title: "Security Risks - Mobile Computing"

Abstract: The talk was about current security risks in the field of mobile computing. It covered current attacks and threat scenarios and furthermore indicated ways to protect against said threats. Some of these scenarios were presented live in order to demonstrate the impact of current attacks.

Speaker: Christoph WOLFERT, Senior Security Consultant from SCHUTZWERK GmbH, Germany.

Thursday 2012, June 28th

Title: The Mobile Security

Abstract:

- Short introduction
- Walled Garden vs Open Garden approach (Apple / RIM vs Android model)
- Attack Vectors & Identifying the Attack Surface
- Security issues in an enterprise environment
- Live MITM demo -- intercepting HTTPS communication from an iOS device
- Tips and Tricks for mobile security

This was a high level presentation, not going into deep technicalities. If someone was interested in a more technical discussion he was able to have it at the end of the presentation separately.

Speaker: Neal HINDOCHA from Terremark, a Verizon company.

Session of 2012, September 20th

Title: (It's a Mobile World - Don't Get Left Behind) BYOD, Security, Compliance. Understanding the challenges

Abstract: Mobile device are overwhelming companies whereas they are either corporate property or belong to the individual. Users need to access corporate and private resources 24/7. Thus the companies are facing new challenges to protect their data, offer great user experience to motivate their employees. Not only applications are at stake, but also Compliance, network security and of course data and software security and integrity. Understand the new challenges to address the BYOD strategy.

Speaker: Philippe HOUGARDY, Business Consultant from Telindus Luxembourg

5.3. Appendix 3 – References

- Guidelines for Managing the Security of Mobile Devices in the Enterprise
  - NIST SP 800-124, Revision 1
- ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management
- NARAINE, Ryan (September 19, 2012): Mobile Pwn2Own: iPhone 4S hacked by Dutch team.

  http://www.zdnet.com/mobile-pwn2own-iphone-4s-hacked-by-dutch-team-7000004498/

  [Accessed on November 15, 2012]
- Figure 3: Mobile evolution taken from Md7, LLC and modified

  http://www.md7.com/international/united-kingdom/

  [Accessed on January 29, 2013]

5.4. Appendix 4 – Mapping with ISO/IEC 27001:2013 Annex A

Mapping with the (new) ISO/IEC 27001:2013 - Annex A:

- A.6 Organization of information security > A.6.2 Mobile devices and teleworking > A.6.2.1 Mobile device policy
  - all

- A.6 Organization of information security > A.6.2 Mobile devices and teleworking > A.6.2.2 Teleworking
  - all

- A.7 Human resource security > A.7.2 During employment > A.7.2.2 Information security awareness, education and training
  - all

- A.8 Asset management > A.8.1 Responsibility for assets > 8.1.4 Return of assets
  - all

- A.8 Asset management > A.8.3 Media handling
  - all

- A.9 Access control > A.9.4 System and application access control > A.9.4.2 Secure log-on procedures
  - […] k) terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on mobile devices […]

- A.10 Cryptography > A.10.1 Cryptographic controls
  - […] c) the use of encryption for protection of information transported by mobile or removable media devices or across communication lines […]

- A.11 Physical and environmental security > A.11.2 Equipment > A.11.2.6 Security of equipment and assets off-premises
  - [...] Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location [...]

- A.11 Physical and environmental security > A.11.2 Equipment > A.11.2.8 Unattended user equipment
  - […] c) secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use […]

- A.13 Communications security > A.13.2 Information transfer > A.13.2.1 Information transfer policies and procedures
  - all