Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Policy for the use of handheld devices in corporate environments

Copyright SANS Institute
Author Retains Full Rights

AD

Security Policy Template

Use of Handheld Devices in a Corporate Environment

GSAE Gold Certification

Author: Nicolas R.C. Guérin, nicolas.rc.guerin@gmail.com

Adviser: Rick Wanner

Accepted: 29 May 2008

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1. Introduction 3
1.1 Purpose 3
1.2 Scope of application and obligations 3
1.3 Roles & responsibilities 4
1.4 Target readership 6
1.5 How to use this security policy template 7
1.6 Terms and abbreviations 9
1.7 Definitions 10
1.8 References 12

2. Security Policy for Handheld Devices 14
2.1 General policy requirements 14
2.2 Physical security 26
2.3 Operating System security 30
2.4 Personal Area Networks (PAN) security policy 37
2.5 Data security 42
2.6 Corporate networks access security 47
2.7 Over-the-air provisioning security 53
2.8 Internet Security 56

Index of Tables

Table 1: Roles & Responsibilities 5
Table 2: Acronyms 9
Table 3: ISO27001 Standard policies 12

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

The use of handheld devices is increasing in corporate environments, providing mobile services and constant connectivity to mobile workers. Due to the fact that handheld devices are recent and not yet properly managed, they present new threats to corporate assets. Handheld devices combine security challenges posed by laptops, removable storage (e.g. USB keys), and cameras.

1.1 Purpose

This security policy establishes rules for the proper use of handheld devices in corporate environments in order to protect the confidentiality of sensitive data, the integrity of data and applications, and the availability of services at <COMPANY NAME>, protecting both handheld devices and their users, as well as corporate assets (confidentiality and integrity) and continuity of the business (availability).

1.2 Scope of application and obligations

This policy applies to all employees, consultants, vendors, contractors, students, and others using business or private mobile handheld devices on any premises occupied by <COMPANY NAME>.

Adherence to these requirements and the security policies derived from them and

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

implementation of provisions is binding across the whole of <COMPANY NAME>, its subsidiaries and majority holdings.

Willful or negligent infringement of the policies jeopardizes the interests of <COMPANY NAME> and will result in disciplinary, employment, and/or legal sanctions. In the case of the latter the relevant line managers and where applicable legal services shall bear responsibility.

These requirements and the security policies derived from them and implementation provisions also apply to all suppliers of <COMPANY NAME>. They shall be contractually bound to adhere to the security directives. If a contractual partner is not prepared to adhere to the provisions, he must be bound in writing to assume any resulting consequential damage (see also [1]).

1.3 Roles & responsibilities

1. All employees are responsible for adhering to the information security provisions. Specific tasks are documented in the definition of roles.

2. For each role a person must be defined by name and made known to the IT security department.

3. Individuals may assume several roles.

4. Definition of roles applies to all the security policies and implementation provisions

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

derived from this policy.

5. IT security ensures that the roles are documented consistently in corporate quality management.

The following table represents roles and responsibilities at the management level:

Table 1: Roles & Responsibilities

Name	Responsibilities
Business owner	Ensures the necessary resources are provided to IT department
IT governance	Maintains security policies: - Creation, adaptation to existing policies in place - Maintenance up-to-date - Guidelines and procedures to implement this policy exist and are communicated to the intended people - Policy and procedures are documented - Policies and procedures are well communicated Is responsible for policy enforcement:

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

	- Ensures that users are properly trained
IT department, IT staff, security administrator, devices manager	Are responsible of managing mobile handheld devices Manage the inventory Ensure that the necessary services are available to users Provide the necessary resources for the use of services Are responsible for policy enforcement: - Via the appropriate working controls - Make requests for changes/adaptations in this policy to IT governance
Users, Employees	- Must read, understand and agree to security policies - Must conform to security policies - Must inform IT staff of exceptions to security policies

1.4 Target readership

This corporate security policy for the use of handheld devices is intended for mid-size to large companies, which need to manage a large number of users using a Mobile Device Management (MDM) solution to monitor and control those devices.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

This policy template is aimed at IT governance (from table 1), which is in charge of adapting this template, according to the business risk analysis and the resources available to implement security controls, to present a final version of the policy that does not leave its interpretation to users.

The IT department is responsible of the application of this policy in a practical sense. It is in charge of mobile devices management and is responsible for providing the necessary complementary documentation and information for the best application of this policy.

Important notice:

This security policy remains as general as possible, depicting various options or scenarios that must be applied according to the business risk analysis. IT governance has the responsibility to enable a secure environment without impairing the functionality of relevant devices and services.

1.5 How to use this security policy template

The security policy template is a long document organized in 5 parts:

- Organizational security processes
- Physical security
- Operating system security

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- PAN security
- Data security
- Corporate network access security
- OTA provisioning security
- Internet security

Copyright: This document is a policy template, free of copyrights. It must be adapted to your specific organization and according to your business risk analysis and the available resources (time, budget, staffs). You are authorized to modify, adapt, or change this policy template as required.

Persons responsible for the security of handheld devices will need to adapt this document to fit the needs of their own organization. Basically, sentences using the verb "SHALL" are mandatory requirements applying to practices with high probability of putting the business at risk, whereas "SHOULD" means that the policy needs to be applied according to the business's specific situation.

Note that *this policy does not take into account specific country or industry regulations*. As a result, some parts of this policy might be adapted to fit country-specific needs. For example, in the healthcare industry compliance to HIPAA regulation is mandatory in the U.S.A., which has specific implications for privacy of data and encryption standards.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1.6 Terms and abbreviations

Table 2: Acronyms

DM	Device Management
DMZ	DeMilitarized Zone
HTTP	Hypertext Transfer Protocol
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IrDA	Infrared
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Code
MIME	Multipurpose Internet Mail Extensions
MMC	Multi Media Card
MMS	Multimedia Messaging Service
MS	Microsoft
MSISDN	Mobile Subscriber ISDN Number
OMA	Open Mobile Alliance
OS	Operating System
OTA	Over The Air
OTA-HTTP	(Push) OTA over HTTP
OTA-WSP	(Push) OTA over WSP
PAN	Personal Area Network
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PI	Push Initiator

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

PIN	Personal Identification Number
PPG	Push Proxy Gateway
QoS	Quality of Service
RFC	Request For Comments
SGML	Standard Generalized Markup Language
SI	Service Indication
SIA	Session Initiation Application
SIR	Session Initiation Request
SL	Service Loading
SMS	Short Message Service
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
WAP	Wireless Application Protocol
WBXML	WAP Binary XML
WINA	WAP Interim Naming Authority
WM	Windows Mobile
WSP	Wireless Session Protocol
WTA	Wireless Telephony Applications
WTLS	Wireless Transport Layer Security
XML	Extensible Mark-up Language

1.7 Definitions

The following definitions have been added for the reader so as to be precise about the terms. Note that these definitions have changed slightly due to recent changes to current

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

operating systems.

Handheld device: A communication device small enough to be carried in the hand or pocket and variously known as a personal digital assistant or personal communication device. Handheld devices considered in this document provide a broad range of services beyond simple telephony, and are closer to mobile computers than legacy mobile phones.

Examples of handheld devices: pocket PCs, smartphones, palmtops, the Blackberry.

Pocket PCs: Handheld devices having a touchscreen and a stylus, in addition to smartphone functionality. For Windows Mobile Pocket PCs, two distinct versions exist that present functions in addition to Windows Mobile Standard:

Pocket PC: Windows Mobile Classic

Pocket PC Phone Edition: Windows Mobile Professional

Smartphones: The principal difference with pocket PCs is that smartphones do not have a touchscreen. Sometimes this results in a slightly different implementation at the OS level. However, the word “smartphone” recently has become a universal term to designate all types of handheld devices (including both pocket PCs and smartphones). In this document, “smartphone” is synonymous with handheld devices.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

are to be interpreted as described in RFC 2119.

1.8 References

This security policy for the use of handheld devices complements a set of existing corporate security policies that are listed below. Those security policies might override this policy; in that case, pointers to the relevant policies are provided.

The following security policies SHOULD exist (or a different set of policies covering the same security areas) and remain available to all employees, and respective guidelines and implementation guides must be provided and remain available to IT staff. The policies are provided with references to corresponding sections of ISO/IEC 27002.

Table 3: ISO27001 Standard policies

ISO 27001:2005 Recommended Policies	ISO control
Information Security Policy	A.5
Access Control Policy	
Clear Desk and Clear Screen Policy	
Data Archive and Retention Policy	
Data Classification and Control Policy	A.7.2, A.11.6
Disposal of Information/Media/Equipment Policy	A.10.7
eCommerce Security Policy	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Email Security/Acceptable Use Policy	A.10.8.4, A.7.1.3
Information Security Risk Assessment Policy	A.12.6
IT Outsourcing Security Policy	
Laptop Security Policy	
Mobile Computing and Teleworking Policy	A.11.7
Overarching ISMS Policy	
Password policy	A.11.2.3, A.11.3.1, A.11.5
Penetration Testing Policy	
Personnel Security Policy	A.8
Physical Security Policy	A.9
Privacy Policy	
Software Copyright Policy	
Spam Policy	
System/Data Backup and Recovery Policy	A.10.5
System Usage Monitoring Policy	A.10.10
Third Party Access Policy	A.6.2, A.10.2, A.10.8
Virus / Malware Policy	A.10.4
User Acceptance Policy	
Corporate encryption standard	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2. Security Policy for Handheld Devices

2.1 General policy requirements

General policy requirements		A.5 Security Policy	
Policy		Description	ISO control
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.	A.5 [Security policy]
Applicable information security		Handheld devices and their users MUST comply with this security policy and all security policies in place at <COMPANY NAME>. The following are policies that are applicable to handheld devices from the table in section	A.5 [Security policy]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

policies		1.8: Information Security Policy 0 Access Control Policy 0 Clear Desk and Clear Screen Policy 0 Data Archive and Retention Policy 0 Data Classification and Control Policy 0 Disposal of Information/Media/Equipment Policy 0 eCommerce Security Policy 0 Email Security/Acceptable Use Policy 0 Information Security Risk Assessment Policy 0 Laptop Security Policy 0 Mobile Computing and Teleworking Policy 0 Overarching ISMS Policy 0 Password Policy 0 Penetration Testing Policy 0 Personnel Security Policy 0	A.15.2.1 [Compliance with security policies and standards]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		Physical Security Policy 0 Privacy Policy 0 Software Copyright Policy 0 Spam Policy 0 System/Data Backup and Recovery Policy 0 System Usage Monitoring Policy 0 Third-Party Access Policy 0 Virus / Malware Policy 0 User Acceptance Policy 0 Corporate encryption standard 0	
Exceptions to handheld security policy		Requests for an exception to this policy MUST be submitted to the IT department via the policy exception request form (e.g. EXEC E2.205).	
Policy enforcement		Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.	A.8.2.3 [Disciplinary process]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Users: roles & responsibilities		In a general sense, users are required to use their common sense in order to act in the best interest of <COMPANY NAME>, its assets and its services. In case of doubt, users MUST contact the IT department to clarify a given situation (See section1.13). Users of handheld devices MUST diligently protect such devices from loss and disclosure of private information belonging to or maintained by <COMPANY NAME>. Before connecting a mobile handheld to the network at <COMPANY NAME>, users MUST ensure it is on the list of approved devices issued by the IT department. The enterprise help desk/IT department MUST be notified immediately upon suspicion of a security incident, especially when a mobile device may have been lost or stolen. The cost of any item beyond the standard authorized equipment is the responsibility of the employee.	A.8.1.1 [Roles and responsibilities] A.11.3 [User responsibilities]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

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 0, according to its risk assessment policy 0. *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 [A.11.4], and MUST NOT grant access to any corporate information to unregistered devices.	A.7.1.3 [Acceptable use of assets] A.11.3.2 [Unattended user equipment]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		Private handhelds are authorized: Any non business-owned (that is, private) device able to connect to <COMPANY NAME> network MUST first be approved by technical personnel such as those from the <COMPANY NAME> 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).	
IT department roles & responsibilities		IT governance is responsible for the mobile handheld device policy at <COMPANY NAME> and shall conduct a risk analysis to document safeguards for each device type to be used on the network or on equipment owned by <COMPANY NAME>. This policy should be reviewed on an annual basis by <COMPANY NAME> IT governance, taking into account	8.1.1 [Roles and responsibilities]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		changes according to new services available, new capabilities of devices, changes in corporate backend servers, and new threats to mobile devices. IT governance is responsible for developing procedures for implementing this policy. 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.	
User awareness training		Users MUST be trained in order to ensure the proper use of devices and corporate resources. A focus on corporate applications and basic security features is mandatory. The following list is not exhaustive, but contains most crucial points that MUST be treated during an initial	A.8.2.2 [Information security awareness, education and training]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		training: - Review of policies - Procedure implementation - Password protection - How to deal with social engineering attacks - Proper protection of devices - Locking the device - Preventing the use of systems by unauthorized users - Protecting devices from loss or theft - Ensuring the information on a handheld device is absolutely necessary - Ensuring the information on a handheld device is also stored on the company network where it is regularly backed up - How to encrypt sensitive information	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- User awareness of changes in technologies (devices and services) and security policies should be regularly tested.	
Inventory of mobile devices		An inventory of handhelds in use associating owner name and identity for network access control (NAC) is mandatory. This inventory MUST take into account at least but not be limited to the following list of identifiers: - Device name - Owner's ID - Device serial number - Device IMEI - Device's MAC address - Owner's ID (user) - User's MSISDN - Device capabilities (Bluetooth, IrDA, Camera, etc.)	A.7.1 [Responsibility for assets] A.11.4.3 [Equipment identification in networks]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- Supplementary accessories provided	
Authorized services and applications		Only approved third party applications can be installed on handhelds. The approved list can be obtained by contacting the IT department, or should be available on the intranet. If a desired application is not on the list, a request can be submitted to the IT department. If the program meets internal testing requirements (stability or security), it will be added and at that point it can be installed. Common authorized services: - Phone (call) services - Messaging (SMS, MMS, IM) - Internet access through corporate networks: - Mobile Office applications - Word processing application - Spreadsheet application	A.7.1.3 [Acceptable use of assets] A.11.4.1 [Policy on use of network services] A.12.4.1 [Control of operational software]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- Presentation application	
Forbidden services		IT department MUST provide a list of unauthorized applications and communicate it to users. The list of unauthorized applications MUST remain available to users via the intranet. The following services might be disabled according to <COMPANY NAME> risk analysis in order to prevent information disclosure or data leakage: - Peer-to-peer services (e.g. Skype, BitTorrent) - MMS messages - Instant messaging - Camera - Third-party applications - Any type of tunneling application that does not allow filtering the content of communications, except the approved VPN solution.	A.7.1.3 [Acceptable use of assets] A.11.4.1 [Policy on use of network services] A.12.4.1 [Control of operational software]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Unauthorized actions		Users MUST NOT modify security configurations without request to and approval from the IT department. Failure to comply with this rule will engage disciplinary procedures. Unauthorized actions: - Installing and/or using unauthorized applications or services (especially UNSIGNED applications) - Removing root certificates from certificate stores - Conducting any careless actions leading to an interruption of service (device out of service) - Disabling security features implementing this security policy	A.7.1.3 [Acceptable use of assets] A.11.4.1 [Policy on use of network services]
Uncovered issues		All issues that are not covered by this security policy MUST be brought to the attention of the IT department of <COMPANY NAME>, which will treat them on a case-by-case basis.	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2.2 Physical security

Physical security		A.9 Physical and environmental security	
Policy		Description	ISO control
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. Note: It is *highly recommended* that a dedicated phone number be allocated for reporting loss or theft of a device. Allocation of this number depends on the number	A.7.1 [Responsibility for assets] A.13 [Information security incident management]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		of devices and users to manage.	
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 NAME> requires the use of hands-free headset devices.	A.7.1.3 [Acceptable use of assets]
Password policy		Access to handheld devices MUST be password-protected. The password policy 0 of <COMPANY NAME> applies in	A.11.2 [User access management]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		the same way to handhelds.	A.11.5 [Operating system access control]
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: 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.	A.7.1 [Responsibility for assets]
Remote		A corporate mobile device management solution SHALL	A.13 [Information

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

blocking & remote wiping		feature remote device wiping (or possibly only blocking) mechanism for all devices accessing corporate internal networks. This feature helps the organization protect itself in case of lost devices. Remote wiping feature ensures the company that data on the handheld cannot be retrieved by an outsider. Note that if removable storage (SD or MMC card) in device is not encrypted, the information contained in the storage card remains accessible for an attacker using it in another device.	security incident management]
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 company's offices MUST have the necessary accessories to charge their device, according to the situation they are in: car, train, at customer sites, etc.	A.7.1 [Responsibility for assets] A.14.1.2 [Business continuity and risk assessment]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		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	
Use of camera		Digital camera embedded on handheld devices *might* be disabled in restricted environments, according to <COMPANY NAME> 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.	A.7.1.3 [Acceptable use of assets]

2.3 Operating System security

Operating system security			
Policy		Description	ISO control

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Firmware version, updates & patching		Device's 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 [A.12.5.1 Change control procedures]. Furthermore, handheld devices content MUST be backed up prior to update. Distribution (provisioning) methods available for deploying firmware updates or patches: - Pull configuration from an internal web page - Push configuration over-the-air - Synchronized when connected to host computer through sync software	A.12.5.2 [Technical review of applications after operating system changes] A.12.6 [Technical vulnerability management]
OS version, updates & patching		Operating System MUST be kept up-to-date with the most recent patches in order to prevent vulnerabilities and make the device more stable.	A.12.5.2 [Technical review of applications

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		Patching and updating processes MUST be documented and MUST be tested before deployment on a whole fleet of devices. Furthermore, handheld devices' content MUST be backed up prior to update. Distribution (provisioning) methods available for deploying updates, patches, or configuration files: - Pull configuration from an internal web page - Push configuration over-the-air - Synchronized when connected to host computer through sync software	after operating system changes] A.12.6 [Technical vulnerability management]
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	A.12.4 [Security of system files] A.12.5.3 [Restrictions on changes to software packages]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

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 device's 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.	A.15.1.2 [Intellectual property rights (IPR)]
Defining the security model		A security model has to be defined according to business requirements in terms of needed applications and services. Security OFF mode SHALL NOT be used (unsecure). Third-party signed applications should be authorized on an application-by-application basis, tested prior to	A.12.4 [Security of system files]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		approval. Locked mode is the recommended security mode. The IT department can choose either third-party signed or locked security model, depending on the applications or services required by the business. If no third-party application is needed, security locked mode SHALL be in use.	
Unsigned applications policy		Users MUST NOT install any UNSIGNED application or theme on the handheld device, for any purpose; this in order to prevent malicious infection of the device.	A.12.4 [Security of system files] A.12.5.3 [Restrictions on changes to software packages]
Third-party party signed applications		Corporate IT department MUST create an inventory of authorized applications to run on handhelds. Especially, Security administrators should in particular study	A.12.4 [Security of system files]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

policy		whether any third-party applications are needed. If not, third-party party applications (signed with a valid certificate) should not be authorized on the mobile device. Necessary third-party applications SHALL be tested prior to authorization and publication on the list of authorized applications. The list of authorized applications MUST be published on corporate intranet.	A.12.5.3 [Restrictions on changes to software packages]
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). Users SHALL NOT revoke certificates in the root certificate store. If users are allowed to install third-party	A.12.4 [Security of system files] A.12.5.3 [Restrictions on changes to software packages]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		applications, users' certificates MUST be placed only in the user certificates store or intermediate certificates store.	
Antivirus policy		Mobile devices MUST have antivirus software installed to prevent viruses from being vectored into the corporation—either 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	10.4 [Protection against malicious and mobile code]
Firewall		*THIS FEATURE DOES NOT EXIST ON ALL EXISTING PLATFORMS YET*. If available, handheld devices MUST use their own application-level firewall to ensure their integrity. Possibly, the firewall might report security information to corporate mobile device management system.	10.4 [Protection against malicious and mobile code]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		The personal firewall acts as the first logical line of defense against penetration attacks. Main functions performed by a personal firewall are: 1. Monitoring incoming traffic and blocking suspicious code 2. Monitoring outgoing messages that infect other company resources 3. Preventing unauthorized use of logical ports by hiding them from malicious code or human penetration attempts	

2.4 Personal Area Networks (PAN) security policy

Personal Area Networks (PAN) security policy			
Policy		Description	ISO control
Bluetooth version		No Bluetooth Device shall be deployed on <COMPANY NAME> 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	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		MUST comply with all parts of this policy except the Bluetooth version specifications.	
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.	A.11.3.1 [Password use]
Bluetooth device security settings		All Bluetooth devices SHALL employ "security mode 3," which encrypts traffic in both directions between a Bluetooth Device and its paired equipment. Switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed. <u>Note</u> that enabling encryption of Bluetooth connections	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		restricts the number of compatible devices to exchange data with.	
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.	A.7.1.3 [Acceptable use of assets]
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.	
Unauthorized use of Bluetooth/IrDA		The following actions are unauthorized uses of <COMPANY NAME>-owned Bluetooth/IrDA devices: - Eavesdropping	A.7.1.3 [Acceptable use of assets]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- Device ID spoofing - DoS attacks - Any attack against other Bluetooth/IrDA enabled devices - Using < COMPANY NAME>-owned Bluetooth/IrDA equipment on non-< COMPANY NAME>-owned Bluetooth enabled devices - Unauthorized modification of Bluetooth/IrDA devices for any purpose	
Bluetooth/IrDA user responsibilities		It is the Bluetooth/IrDA user's responsibility to comply with this policy. Bluetooth/IrDA users MUST access <COMPANY NAME> information systems using only approved Bluetooth/IrDA device hardware, software, solutions, and connections. Bluetooth/IrDA device hardware, software, solutions, and connections that do not meet the standards of this policy	A.7.1.3 [Acceptable use of assets]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		SHALL NOT be authorized for deployment. Bluetooth/IrDA users MUST act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth/IrDA equipment. Bluetooth/IrDA users are required to report any misuse, loss, or theft of Bluetooth/IrDA devices or systems immediately to information security.	
Infrared IrDA		Infrared support MUST be disabled if Bluetooth connectivity is supported. Bluetooth MUST be preferred to IrDA when available. If IrDA support has to be enabled, pairing with other devices MUST use long pairing keys as defined in section 4.2: PAN PINs and pairing. Security policy for Bluetooth also applies to IrDA the same way: - PAN PINs and pairing (section 4.2) - PAN security audits (section 4.5)	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- Unauthorized use of Bluetooth/IrDA (section 4.6) - Bluetooth/IrDA user responsibilities (section 4.7)	

2.5 Data security

Data security			A.7 Asset Management
Policy		Description	ISO control
Information classification		The information classification policy 0applies 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	A.7.2 [Information classification]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- Strictly confidential or secret documents - Secret and confidential documents MUST NEVER be stored on end devices. Internal documents SHOULD NOT be stored on mobile devices unless strictly necessary (cf. Information classification and control policy 0). 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 NAME> SHALL employ encryption or equally strong measures to protect the corporate data stored on the device, as stated in corporate encryption standards 0. If memory encryption is not available natively in the device, a third party application SHALL be purchased.	A.10.7 [Media handling]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		Note: As of the date of this paper, U.S. government use requiring encryption algorithms must meet National Institute of Standards and Technology FIPS PUB 140-2.	
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). See section 5.4.	A.10.7 [Media handling]
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.	A.10.7 [Media handling]
Data backups		Data on handheld devices MUST be backed up regularly according to corporate backup policies 0, which should	10.5 [Backup]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		specify the frequency of backups. The following points are particular to handheld devices: Location to perform backup: *At the Office:* Handheld device MUST be backed up each time it is connected to its usual host desktop workstation (i.e. owned by the same user) via USB. Note that this operation is generally automatically configured. *Out of corporate offices:* Users SHOULD only synchronize the data available in email clients: emails (without attachments), contacts address book, calendar, tasks and notes. Backup frequency: Each time the smartphone is connected to its host desktop workstation Frequency MUST be defined in a backup policy 0	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		The following data, at least, MUST be backed up: - Corporate information - Address book - Agenda - Tasks/notes - Device configuration settings Note: this part of the policy might override the backup policy 0if this latter already takes into account handheld devices.	
Private data on corporate devices – general considerations		According to <COMPANY NAME> risk analysis: Users are not allowed storage of private data on their handheld devices; in this case: Users MUST NOT store any private data on corporate devices. The device's user has full responsibility for managing its data. Especially in cases of device theft, <COMPANY NAME> cannot be held responsible in any manner for the (malicious) use of private information.	A.12.4.2 [Protection of system test data]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		Users are allowed storage of private data on their handheld device: If users want to store private data on corporate devices at their own risk, the best practices recommend using a dedicated wallet application that encrypts confidential data using a password, following corporate standards for encryption 0. Note: the passphrase in use for the wallet MUST be different from the password in use to block the device.	

2.6 Corporate networks access security

Corporate networks access security			A.11 Access Control
Policy		Description	ISO control
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	A.11.4.3 [Equipment identification in networks] A.11.4.6 [Network

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		unknown device will be considered as an attack against corporate assets.	connection control]
File sharing		File-sharing services MUST be disabled, independently of the transport technology. 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 0. Note: File sharing allows users to create a shared folder on their phone in order to make it accessible through the network, like the *folder sharing* capability on Windows desktop computers.	A.12.4 [Security of system files] A.7.1.3 [Acceptable use of assets]
Remote access to corporate resources		Compliance of all staff (employees, consultants, vendors, contractors, and students) using PDAs with the remote access, Teleworking 0, disposal of information / media / equipment 0, and other applicable policies, procedures, and standards is mandatory.	A.7.1.3 [Acceptable use of assets] A.11.4.1 [Policy on use of

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

			network services]
			A.11.4.2 [User authentication for external connections]
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 NAME> risk analysis and its business model: - Restrict the list of authorized access points to	A.11.4.5 [Segregation in networks]
			A.10.6 [Network security management]
			A.11.7.1 [Mobile computing and communicati

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		corporate access points only. - Disable connection to open/public WLANs without encryption and authentication methods. - Disable connecting to WEP-protected WLANs (considered insecure). If mobile workers do require connectivity through public, open, or untrusted WLAN, then users MUST use WLANs using, if available and in this order: WPA(2) encryption, WEP 256 bits (or 128 bits), or finally open networks if nothing else is available. Users connected to data networks in an open environment MUST use a VPN connection to corporate networks to avoid direct attacks against the handheld and data communications.	ons]
Internal access to corporate networks		Access using synchronization software: Synchronization of data with corporate desktop computer or internal network must be protected. The sync operation uses a third-party application to synchronize mobile devices with desktop computer's email	A.11 [Access control]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		application. Consequently, handheld devices' access permissions in corporate networks MUST NOT overstep the permissions granted to the desktop workstation belonging to the same user. Furthermore, handhelds' permissions may be further restricted according to the information classification policy 0. Using a desktop computer's credentials to access resources in the intranet allows a handheld device to access corporate networks (and possibly the Internet, if users are allowed to) while being protected by the computer's security controls (antivirus, firewall, etc.). Direct access to corporate networks through WLAN: If handheld devices have direct access to corporate networks, they MUST be identified and remain under control of IT Staff in charge of handheld devices (using, e.g., NAC technologies).	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Desktop PC security		Desktop workstation used to synchronize a handheld device MUST be protected according to security policies for securing corporate workstations. Among other security controls stated by corporate security policies, desktop workstations should make use of, at least: - An up-to-date antivirus solution - An application-level firewall	A.12.4 [Security of system files]
Synchronization		Synchronization between desktop PC using Sync software and the mobile device MUST be secured using a pairing key following corporate standards or password policy 0.	A.12.4 [Security of system files]
VPN access & configuration		Security for remote access to corporate networks MUST be enforced following corporate policy for mobile computing and teleworking 0. Users connecting wirelessly to corporate network MUST use VPN software, either as a built-in or third-party	A.11.7 [Mobile computing and teleworking]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		application. Using VPN SHALL be mandatory for the security of communications between mobile devices and corporate networks. Without the VPN solution approved by <COMPANY NAME>, access to corporate networks shall not be granted to handheld devices. Most recent handheld devices contain built-in VPN support, although older devices might require the installation of a third-party VPN client.	

2.7 Over-the-air provisioning security

Over-the-air provisioning security			
Policy		Description	ISO control
Mobile device management		Depending on the company size, a central management capability in the organization MUST be in place. Since handheld devices are not completely under the control of the organization and are by nature mobile, the	A.10.10 [Monitoring] A.11.4

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		organization MUST have a mechanism to monitor the devices and enforce the security policy from a central location.	[Network access control]
OTA provisioning method		OMA Device Management (continuous provisioning) MUST be preferred to OMA client provisioning (one-way WAP push), in order to constantly enforce security policies (permanent connection) and allow real-time monitoring of devices. Note that OMA DM (continuous provisioning) is required in order to allow remote device management and real-time monitoring.	A.11 [Access control]
OTA provisioning architecture		Servers and gateways in corporate networks MUST be protected against external and internal threats. Mechanisms to secure servers are described in Access Control security policies for corporate networks. The security measures MUST secure the following functions and nodes: Corporate mobile gateway (PPG) should be placed in	A.11 [Access control]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		DMZ PPG must authenticate and authorize any push initiator: - Trusted Provisioning Server (TPS) - Mobile e-mail server - Mobile Device Management Server - Any corporate node using the PPG to remotely communicate with mobile devices	
OTA communications security		Mobile devices able to use corporate data services out of corporate offices MUST use VPN encryption in order to secure communications, as depicted in mobile computing and teleworking policy 0. VPN solutions can either be present natively in the OS or be purchased as third-party software. Necessary SSL certificates should be provided by corporate IT department. Refer to corporate policy for remote access and VPN.	A.11 [Access control]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

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.	A.11 [Access control]
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.	A.11 [Access control]

2.8 Internet Security

Internet Security			
Policy		Description	ISO control
Use of Internet		Users MUST agree to the email security/acceptable	A.10.8 [Exchange

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

services		use policy 0and eventually to the eCommerce security policy.	of information] A.10.9 [Electronic commerce services]
General e-mail security requirements		Corporate e-mail policy applies to handhelds the same way it applies to any e-mail client. Handheld devices might be subject to further restrictions according to company's risk analysis. Additional restrictions are as follow. For the specific use of e-mail from handheld devices, these security mechanisms MUST be taken into account, and applied following the corporate e-mail policy 0: - S/MIME encryption - Choice of algorithm - Algorithm negotiation - Signing messages	A.10.8 [Exchange of information] A.10.9 [Electronic commerce services]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		- Using personal certificate - Using applications certificate - Allow only signed messages in inbox - HTML messages (allow or deny)	
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.	A.10.8 [Exchange of information]

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**