Introduction

Section 44 of the Financial Management and Accountability Act 1997 (FMA Act) requires the Chief Executive of each department and agency to promote the efficient, effective and ethical use of resources for which they are responsible. The Chief Executive is also responsible for the day-to-day management of their agency’s protective security arrangements (Protective Security Manual Part A Section 1.3).

Using information and communication technology (ICT) to enhance government service delivery and administrative processes is an objective of the Australian Government’s e-government policy. Personal Electronic Devices (PEDs) can help people in government manage information more efficiently, especially when they are outside their normal office environment (eg. when travelling interstate or otherwise off-site).

The efficient and effective use of PEDs requires informed planning and careful management, paying particular attention to whole-of-government security considerations.

The Defence Signals Directorate (DSD) has developed ICT security policy on the use of PEDs in the Australian Government. This policy is described in the “Australian Government Information and Communications Technology Security Manual” (ACSI 33) Part 3 Chapter 4.

This Better Practice Guidance for CIOs – Security Considerations for the Use of Personal Electronic Devices has been developed to assist Chief Information Officers in considering the approval, requirements and appropriate use of PEDs in their ICT environment in accordance with government security policy and consistent with a risk managed approach. It is complementary to Better Practice Guidance No. 23 – Use of BlackBerry Devices.

Comments about the guidance and suggestions for additional checkpoints may be directed to:

Security and Communications
Australian Government Information Management Office
Department of Finance and Administration
Phone: (02) 6215 1548

Email: better.practice@finance.gov.au

Related documents

Chief Executive Guidance - Security Considerations for the Use of Personal Electronic Devices (PEDs)
Better Practice Guidance No. 23 - Use of BlackBerry Devices
Better Practice Guidance No. 24 - User Requirements for BlackBerry Devices
Acknowledgments

This guidance was developed with the assistance of the Defence Signals Directorate (DSD).

Disclaimer

The issuing of this guidance by AGIMO in no way implies any form of endorsement for the product or services described within.
What are Personal Electronic Devices?

The “Australian Government Information and Communications Technology Security Manual” (ACSI 33) describes Personal Electronic Devices (PEDs) as “portable devices that can process, store and/or transmit data electronically” (ACSI 33 Part 3 Chapter 4, "Portable Computers and Personal Electronic Devices").

Examples of PEDs by this definition include (but is not limited to):

- Mobile telephones and ‘smartphones’
- BlackBerry® devices
- Personal Data Assistants (PDAs)
- Digital cameras/video
- MP3 players such as Apple iPod®
- Thumb drives and storage keys
- Smart cards
- Data cards and data card readers (e.g. CF, XD, SD, Sony Memory Stick®)
- USB wireless devices such as CDMA broadband modems, Bluetooth and 802.11 keys
- Portable games consoles such as the Sony Play Station Personal (PSP®)

PEDs generally lack comprehensive in-built security features including, for example, identification, authentication, access control and auditing.

Portable (laptop) computers are generally outside the scope of the PED definition as they have a more complex security capability and may be managed in a similar way to other computer workstation technology (described in ACSI 33).

PEDs have become commonplace in our society and are increasingly being adopted into workplace environments as standard business tools. Mobile telephones, PDAs and thumb drives are commonplace around most workplaces and MP3 players are being used by staff as ‘virtual offices’ and for the storage and transfer of information.

The rapid uptake of these devices has spurred further development and convergence of the functionality that PEDs offer. For example:

- Most mobile telephones have the ability to synchronise contact and appointment data with personal computers and also the ability to connect (via infrared or Bluetooth technologies) to other mobile telephones to transmit information

- ‘Smartphones’ combine the capability of PDAs, digital cameras, MP3 players and file storage with mobile telephone technology into a single, easily portable unit. The more recent advances in ‘smartphone’ technology also include inbuilt wireless 802.11 networking capability (with corresponding software for internet browsing and virtual private network (VPN) connectivity), and global positioning satellite (GPS) systems, and

- MP3 players, such as the Apple iPod®, have capable calendaring functionality and can synchronise with desktop software. These devices can also be used as portable storage devices.

It is therefore opportune that agencies consider the benefits and assess the risks of deploying and connecting these devices in their business systems.
Essentially, PEDs can be categorised on a continuum according to their intrinsic capability:

**Passive PEDs** are devices that do not have any intrinsic complex processing or intercommunications capability on their own. These devices are used to provide a specialised functionality to other devices/systems.

Examples of passive PEDs include:
- Digital cameras and video recorders
- Thumb drives and storage keys
- Data card readers and data cards
- USB wireless, CDMA and 3G modems

**Active PEDs** are devices that have their own programming logic and are able to perform some processing and communications tasks independent from other devices.

Examples of active PEDs include:
- Mobile telephones and ‘smartphones’
- BlackBerry® Devices
- PDAs
- MP3 players
- Some portable games consoles

Consumer devices, such as portable games consoles, have been included in this guidance as the facilities offered by these devices generally migrate over time into business devices and vice versa.
When PEDs may, should not and must not be used

ACSI 33 Part 3 Chapter 4 (“Portable Computers and Personal Electronic Devices”) provides specific policy for the use of PEDs in Australian Government agencies.

In essence, the policy states that:

a. Agencies must protect portable computers and PEDs storing classified information to at least the same level as hardcopy material of the same classification, in accordance with the PSM requirements for access, storage and handling. Requirements may be reduced by the use of encryption products.

b. DSD recommends that agencies encrypt data on all portable computers and PEDs.

c. Portable computers and PEDs containing classified information should be:
   i. operated in physically protected areas classed as intruder resistant or better
   ii. kept under continual, direct supervision when in use, and
   iii. stored in physically protected areas appropriate for that classification when not in use.

d. If intending to use portable computers or PEDs to process classified information, agencies should ensure that all data collection and communications functions of the devices not identified as business requirements are removed or disabled as effectively as possible within the limitations of the particular device.

e. Agencies should put a protective marking on all portable computers and PEDs.

f. Agencies should put a label warning against unauthorised use on all portable computers and PEDs.

g. An additional label should be affixed asking the finders of a lost portable computer or PED to hand the equipment in to any Australian police station or, if overseas, an Australian Embassy, Consulate or High Commission.

h. Agencies should develop an emergency destruction plan for any portable computer or PED used in high risk situations.

Additionally, Part 3 Chapter 11 (“Data Transfers”) details specific requirements for the direct connection of devices such as PEDs to classified agency resources. These connections are referred to as “Temporary Connections” and require that Agencies:

i. must not insert media of any classification into a system of a lower classification.

j. intending to allow portable computers or PEDs to be temporarily connected to a system of a different classification must ensure that a firewall of the appropriate assurance is used to protect the more highly classified side of the connection, and

k. should not allow unaccredited portable computers and PEDs to connect to agency ICT systems or store official information.

Numerous other sections in ACSI 33 describe policy for the use and management of devices with the capability that PEDs provide. Appendix A lists the sections that are of particular relevance to the function of PEDs and compliance with these applicable sections is mandatory in addition to the specific policy for the use of PEDs in Australian Government.
agencies. Where a device provides more than one capability, compliance is required with sections applicable to ALL capabilities provided by the PED.

To obtain the best outcome for ICT security when implementing new systems ACSI 33 advocates designing agency policy and controls based on a risk assessment for the new system and with reference to any overarching obligations. In some instances an agency may determine that compliance with a particular requirement may increase rather than decrease the risk profile of a new technology. Part 1, Chapter 1 of ACSI 33 details a methodology for deviation from the ACSI 33 requirements:

Agencies deviating from a “must” or “must not”, must provide a waiver in accordance with the requirements of the PSM.

Agencies deviating from a “should” or “should not”, must document:
   a. the reasons for the deviation,
   b. an assessment of the residual risk resulting from the deviation,
   c. a date by which to review the decision,
   d. the ITSA’s involvement in the decision, and
   e. management’s approval.

The definition in this guidance document of “must”, “should” and “should not” is consistent with that of ACSI 33.

The Defence Signals Directorate (DSD) Policy and Guidance for the Use of BlackBerry by the Australian Government describes the specific requirements for the use of BlackBerry in agencies.

The general difference between BlackBerry type devices and other PEDs is that the BlackBerry style of device is delivered as a packaged ‘system’, i.e. each of the individual security component requirements described in this guidance have generally been built into the capabilities of the system.
## GUIDANCE SUMMARY

### CHIEF EXECUTIVE APPROVAL
- Seek Chief Executive approval for the implementation of PEDs.
- Identify policy and standards relevant to the approval, deployment and use of PEDs.

### BEFORE IMPLEMENTING PEDs
- Conduct a risk assessment to determine the vulnerabilities that may be exposed with the introduction of the device.
- Establish a system of controls to manage the use of the device.
- Develop agency policies and procedures, including any restrictions, for the use of PEDs that align with Australian Government policies and standards and that adhere to Defence Signals Directorate (DSD) information security requirements.

### MANAGE USE
- Disseminate the Agency’s policy on the use of PEDs to all staff.
- Provide staff with training on the use of PEDs and security requirements.
- Ensure that staff acknowledge in writing their agreement to adhere to specific agency and Australian Government policies and associated procedures.
- Report damaged, lost or stolen PEDs.

### REVIEW AND AUDIT
- Audit compliance with policies and standards for the use of PEDs.
CHECKPOINTS

CHIEF EXECUTIVE APPROVAL

- Seek Chief Executive approval for the implementation of PEDs.

Section 44 of the *Financial Management and Accountability Act 1997* (FMA Act) requires the Chief Executive of each department and agency to promote the efficient, effective and ethical use of resources for which they are responsible.

The Chief Executive is also responsible for the day-to-day management of their agency’s protective security arrangements (Protective Security Manual Part A, Section 1.3), including the approval and use of PEDs.

Seek formal approval from the Chief Executive for the procurement and use of PEDs.

- Identify policy and standards relevant to the approval, deployment and use of PEDs.

Relevant policies and standards for the use of PEDs include:


- The Australian Government Information and Communications Technology Security Manual (ACSI 33). Describes the policies and guidance required to achieve an assured information technology security environment.

  Appendix A provides references to specific sections in ACSI 33 that relate to PEDs.

Related policies for BlackBerry provide specific requirements for compliance for BlackBerry devices:


- Instructions on the Allocation and Use of BlackBerry in the Australian Government – AGIMO
BEFORE INTRODUCING PEDs INTO AN AGENCY’S ICT ENVIRONMENT

- Conduct a risk assessment to determine the vulnerabilities that may be exposed with the introduction of the device.

An assessment of the environment into which the PED will be introduced is essential in maintaining control over that environment. A risk assessment is used to determine the impact of a new technology on the managed ICT environment and enables a thorough evaluation of the controls required to maintain the integrity of the ICT systems and information stored and processed in that environment.

The following points should be addressed in the risk assessment:

- Intended functionality of the PED (e.g. passive or active device and capabilities)
- Physical environment in which the PED will operate
- Classification of the information with which the PED will be in contact
- Extent to which the device can be controlled within, and outside the agency’s ICT environment
- Extent to which the device may be used for purposes other than the intended functionality
- Modifications required to work practices to cater for the device
- The portable and attractive nature of the device
- Controls around the connectivity of the device to the agency’s managed ICT environment
- Re-useability and disposal
- Audit-ability – the ability to ensure compliance with policy and procedures

ACSI 33 Part 2 Chapter 4 describes an accepted approach for ICT risk assessment in Government agencies.

- Establish a system of controls to manage the use of the device.

A rigid controls environment will help to ensure that the PED is implemented into the agency environment in a safe and reliable way. The accepted approach used by Australian Government agencies is the development of a System Security Plan (SSP) (ACSI 33 Part 2 Chapter 5) for the PED and its associated software and utilities.

In developing the SSP, the agency should consider:

- Connection of the device to agency ICT infrastructure (direct PC (e.g. USB) cable connection, Bluetooth, IrDA, 3G or other mobile carrier service, Wireless LAN, LAN/WAN, external via VPN)
- Access controls for devices that can connect directly to information resources
- Security requirements for information to be transmitted to and from the device
- Antivirus, anti-Trojan and anti-spyware solutions with sufficient capability to manage any introduction of malware (applications designed to cause disruption or harm to corporate information systems) into the network from a PED
- Use of the device outside of the controlled agency ICT environment
- Hardware and software configuration and lockdown of capability on intelligent PEDs (e.g. ‘smartphones’)

Security Standard Operating Procedures (SOPs) should be reviewed and updated to ensure they encapsulate the requirements of the new device as specified in the SSP for that device or device type.

ACSI 33 Part 3 Chapter 4 (“Classifying, Labelling and Registering Hardware”) provides a number of requirements for the classification, labelling and registration of hardware media containing or in contact with classified information. Agencies should assess the requirements for labelling of PEDs that may be used in public places to determine the suitability of such markings on these devices. If an agency’s risk assessment indicates that these markings may heighten the risk of theft (given the portable and attractive nature of these devices) then the agency must, with the ITSA’s involvement, document the reasons for the deviation and show that the agency has addressed the residual risk resulting from the deviation. The decision to deviate from this requirement must be approved by management and the decision should be reviewed at a nominated time in accordance with ACSI 33 Part 1 Chapter 1 (paragraphs 1.0.20-1.0.21).

The AGIMO “Implementation Guide for Email Protective Markings for Australian Government Agencies” describes how to filter and control the flow of security classified and protectively marked email inbound and outbound from an agency, including to PEDs.

- Develop agency policies and procedures, including any restrictions, for the use of PEDs that align with Australian Government policies and standards and that adhere to Defence Signals Directorate (DSD) information security requirements.

Effective policies and procedures help to ensure that an agency considers relevant issues and operates in accordance with whole-of-government guidelines. Documenting and making these available to staff will help to ensure that users are aware of the organisation’s expectations of them when using PEDs.

PEDs provide a variety of functions which may be utilised by agencies, from portable storage to remote communications solutions e.g.

- Many PEDs incorporate several complementary capabilities into a single device (e.g. ‘smartphones’ have communications, storage and some data processing capability).
- There are many different devices on the market, each offering similar functions but with differing capabilities for control. Consumer preferences for technology leaders seem to vary with each generation of devices.
- PED technologies are an emerging and growing market and are subject to rapid change and various implementation approaches.
- No one technology is appropriate for all business needs.

Policy and procedures should, therefore, be written around the type of device and its capabilities, rather than relating to specific devices and technologies.

Agencies will need to consider the varying business requirements of its user base and may consider providing multiple device types. This should be offset/considered against the total cost of ownership of providing and supporting multiple or single device configurations.

Agency policy should address:

- Minimum security capability required of the device type to meet the requirements of ACSI 33 and other agency security policy
- Acquisition and control of PEDs that may be connected to the agency’s ICT environment; and
- Acceptable use of the PED in the conduct of business for the Agency and for which the PED is intended. This should make specific reference to the classification of information that the PED may come in contact with.
Procedures should be formalised to manage the:

- acquisition of appropriately capable PEDs for use in the Agency
- disposal of PEDs in line with ACSI 33 requirements for disposal of hardware, media sanitisation and destruction
- handling of loss or theft of devices that may store official, personal or security-classified information

The AGIMO Better Practice Guidance No. 24 – *User Requirements for BlackBerry Devices* provides information specific to the user requirements for BlackBerry and is generally applicable to the broader category of PEDs.
MANAGE USE

☐ Disseminate the Agency’s policy on the use of PEDs to all staff.

The policy for the connection (by whatever means e.g. direct cable, IrDA, Bluetooth, 802.11 wireless or 3G) of PEDs to the Agency ICT environment should be disseminated to all staff and should form part of the induction pack for new staff and contractors.

The rapid adoption of PED technologies in the consumer market has resulted in these devices being commoditised. Many people now carry personally owned PEDs, such as thumb drives, MP3 players and PDAs. The connection of these PEDs to Agency ICT systems poses risks to agencies as these devices are not subject to the same controls as Australian Government-owned equipment. Agencies should assess the risks of having these personally owned devices connecting to their ICT systems and should make an explicit statement in their policy about the use of such devices.

ITSAs should be trained to identify and appropriately address unauthorised connections of PEDs to the Agency’s ICT environment.

☐ Provide staff with training on the use of PEDs and security requirements.

In many areas of administration, failure to follow policies and procedures is not generally a result of deliberate actions, but a lack of awareness of requirements. Training in the appropriate use of devices can assist staff to implement policies and procedures. The existence of training can also help to distinguish deliberate misuse from incompetent usage.

As a part of this training, agencies should also inform staff that these devices are likely to be attractive targets for thieves, and that the implications of the information contained in them being accessed by others could be detrimental to the Australian Government.

Training should be provided to officers before they are issued with PEDs. The training should cover (but not exclusively):

- Acceptable use of the PED within and outside the controlled agency environment
- Responsibilities of the officer in the event of loss or theft of the device
- Procedures for repair, disposal and/or redeployment of the device
- Protective markings and use of the device to store or access classified information
- Inherent risks of PEDs (e.g. identity theft, data spillage) and the user’s responsibilities to protect information in their possession.

Training should be provided to officers about security classifying and protectively marking emails and attachments. The Protective Security Manual provides policy to assist agencies to determine the appropriate classification of an email and attachment.

☐ Ensure that staff acknowledge in writing their agreement to adhere to specific agency and Australian Government policies and associated procedures.

Staff using an agency-issued device are responsible for its appropriate use. Staff must be aware of and agree to act in accordance with the organisation’s policy and procedures. The ramifications of failing to apply those policies and procedures must also be clear to staff.
Report damaged, lost or stolen PED devices.

Users of agency-supplied PEDs should be advised to report lost or damaged devices to a relevant support authority within the agency, either the client services support team or the security authority (in the case of a lost device containing security classified information). Repair or disposal of faulty PEDs should only be undertaken by an appropriate agency support authority as described in ACSI33 Part 3 Chapter 4 (“Repairing and Maintaining Hardware” and “Disposing of Hardware”).

Agency support authorities should have sufficient processes to ascertain an appropriate course of action for the device to remedy the situation and minimise any security exposure.

Loss of a device containing security classified information constitutes a Physical Security Incident and should be handled in accordance with ACSI33 Part 3 Chapter 1 (“Physical Security Incident”).

REVIEW AND AUDIT

Audit compliance with policies and standards for the use of PEDs.

Setting out policy without monitoring compliance is bad practice. There should be appropriate internal – and from time to time external – checks of compliance with policies governing the use of PEDs.

There should also be regular reviews of internal policies, to test their currency and adequacy.

Other Resources

For further information about security requirements, see the following:

Protective Security Manual

Australian Government Information and Communications Technology Security Manual (ACSI 33)

Policy and Guidance for the Use of BlackBerry by Australian Government

Implementation Guide for Email Protective Markings for Australian Government Agencies
www.agimo.gov.au

Email Protective Marking Standard for the Australian Government
www.agimo.gov.au

Australian Government Information Management Office, Better Practice Guidance and Checklists:
Appendix A – ACSI 33 security policy applicable to PEDs

The following sections detail the reference paragraphs in the Australian Government Information and Communications Technology Security Manual (ACSI 33) applicable to PEDs. The paragraph numbers are consistent with the version of ACSI 33 released on 29 September 2006.

General
These policy sections apply to the implementation of any system or device within an Australian Government environment and compliance is mandatory for the implementation of any PED. Applicable paragraphs are:

2.2.6 Risk Management Plan for ICT Systems
2.2.7 System Security Plans
2.2.8 SOPs
2.2.9 [SIC]
2.8.22 – 2.8.31 Managing Security Incidents
3.1.5 – 3.1.9 Fundamentals [of Physical Security]
3.2.5 – 3.2.12 User Training and Awareness
3.3.7 – 3.3.13 Product Selection
3.3.14 – 3.3.17 Acquiring Products
3.3.18 – 3.3.21 Installing and Using Products
3.3.22 – 3.3.24 Secure Disposal
3.4.21 – 3.4.25 Repairing and Maintaining Hardware

Part 3 Chapter 7 – Active Security, with particular reference to:
3.7.29 – 3.7.32 Vulnerability Analysis

Part 3 Chapter 11 – Data Transfer with particular reference to:
3.11.12 – 3.11.22 Temporary Connections

Devices with storage capability
The following policy sections address the requirements for compliance of any device containing storage media that may be used to store security-classified data:

3.1.43 – 3.1.46 [Physical security of] Removable Media

Part 3 Chapter 4 – Hardware Security with particular reference to:
3.4.7 – 3.4.20 Classifying, Labelling and Registering Hardware [ref to media]
3.4.26 – 3.4.30 Disposing of Hardware
3.4.31 – 3.4.43 Media Sanitisation
3.4.44 – 3.4.52 Media Destruction
3.9.12 – 3.9.15 DSD Approved Cryptographic Algorithms (DACAs)
3.9.16 – 3.9.20 DSD Approved Cryptographic Protocols (DACPs)
Devices with data transmission and/or receiving capability

The following policy sections address the requirements for compliance of any device that may connect to security-classified systems or other lesser-classified devices:

Part 3 Chapter 6 – Logical Access Control
3.8.39 – 3.8.48 Wireless Communications
3.8.68 – 3.8.86 IP Telephony
3.8.57 Cordless and Mobile Telephones
3.8.67 Paging Services
3.9.25 – 3.9.29 Secure Shell (SSH)
3.10.12 – 3.10.17 Internetwork Connections
3.10.42 – 3.10.44 Remote Access

Devices with inbuilt processing capability

The following policy section addresses the requirements for compliance of any device with independent processing capability using in-built or purpose-built software:

Part 3 Chapter 5 - Software Security
Appendix B – PED Scenario

This section describes a typical PDA and its capabilities. It is intended as a ‘reference device’ to identify specific security control requirements that must be considered when looking to deploy PEDs into an Agency’s ICT environment.

Device capabilities
The reference device has the following functionality/capabilities:
- Mobile telephone on the 3G mobile network (SMS and MMS capable)
- Windows® Mobile 2005 PDA with synchronisation capability for calendar, tasks, contacts, email, files and databases
- Digital camera
- Voice recording
- Speaker phone operation
- 802.11b wireless network card
- Bluetooth
- IrDA
- Mini USB direct cable PC connection using USB 1.1
- SDIO expansion slot
- 512Mb SD card
- SDIO document scanner attachment and software (purchased separately)
- SDIO GPS attachment and software (purchased separately)
- Fingerprint biometric access control

Context
The chosen device is required to:
- enable mobile telephone capability
- provide GPS and navigation assistance
- connect to the internet
- access work-related messaging facilities (e.g. email, calendar, contacts), and
- interact with purpose-built data collection systems that inter-operate in real-time or offline modes with agency data systems.

It is intended that the device will be used inside (direct USB cable connected to an agency computer or wireless connection direct to ICT services if available) and outside (via 802.11b or 3G connection and VPN) the controlled agency ICT environment. The ICT network is classified to Protected level and the data systems are X-in-Confidence.

Security Control Considerations
The connection of any device to the agency computer network must be managed, consider:
- Logical security and access control at the connection point – direct PC connection, LAN/WAN, external
- Security Policy enforcement on the device
- Antivirus and anti-Trojan solutions on the device and at the connection points
- Anti-spyware software at the connection point
- Ability for the device to act as a router between the controlled agency environment and the internet
- Ability to disable unnecessary functions to prevent data theft or eavesdropping (e.g. camera, voice recording, speakerphone function)
As the device will be used outside the physical controls environment of the agency office, consider:

- Connection to the agency network (wireless LAN and 3G) is unprotected
- VPN or other tunnelling solutions and encryption of data while in transit
- Authentication of the device to the corporate network
- Access restrictions to network resources, sensitive information and administrative functions
- Access requirements to data systems for two-way communication
- Access to email: will email be pushed from the server as it arrives or pulled from the device in a scheduled synchronisation process?
- Should the device be allowed to access internet resources without connecting to the VPN?
- Labelling of the device to facilitate recovery in the event that the device is lost
- Limiting connection capability to the device by disabling unnecessary features (e.g. IrDA and Bluetooth)

How will the agency manage upgrades and technology enhancements as they become available?
Consider:

- Variety of similar devices – market preference for devices changes from generation to generation
- SDIO devices add functionality to the device. Some newer devices are aggregating capabilities (e.g. storage and GPS receiver in one unit)
- Updating of existing devices with service packs/patches/software updates etc.
- Investigation of new devices before acceptance on the approved device list – new devices will most probably have new functionality which may impact on security
- Installation of new software on the device: who can do this and how is it controlled?

The data on the device is sensitive and contains personal information that may breach the Privacy Act 1988 and/or other Acts if spilled or contribute to identity fraud or physical endangerment.
Consider:

- Encryption of the data on the device (using DSD-accredited encryption system as appropriate)
- Access policy on the device and the ability to enforce rigorous password principles on the device and the systems containing sensitive information
- Ability to remotely manipulate the device: can it be shut down or the data erased if it is reported to be out of the control of the agency
- What is the likelihood of the data on the device having a serious negative impact on the Agency or the Australian Government if spilled? Is there sufficient control to mitigate this risk or at least reduce it to an acceptable level?
- Sanitisation mechanisms before redeployment or disposal

Before a new device can be deployed in a controlled environment, guidelines for acceptable use and handling of the device should be developed and disseminated to officers responsible for the new capability.
Consider:

- Instructions for use of the device (including a clear statement on what constitutes misuse of the device)
- Policy and procedures for handling repairs, maintenance and disposal of the device
- Occupational Health and Safety issues and any modifications to work practices
- Monitoring of compliance with defined policy and procedures
- Asset management and assignment procedures
Appendix C – Glossary of Terms

3G
short for third-generation technology. It is usually used in the context of mobile telephones. The services associated with 3G provide the ability to transfer both voice data (a telephone call) and non-voice data (such as downloading information, exchanging email, instant messaging, video).

802.11 Wireless
(IEEE 802.11) denotes a set of Wireless LAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802). The term 802.11x is also used to denote this set of standards and is not to be mistaken for any one of its elements. There is no single 802.11x standard.

Bluetooth
an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers and digital cameras via a secure, low-cost, globally available short range radio frequency.

CDMA
Code Division Multiple Access is a form of multiplexing that encodes data with a special code associated with each channel and uses the constructive interference properties of the special codes to perform the multiplexing. Commonly refers to digital cellular telephony systems that make use of this multiple access scheme.

ICT
Information and Communication Technology – referring to the system of hardware and software used for the communication, processing and storing of information.

IrDA
Infrared Data Association – defines physical specifications communications protocol standards for the short range exchange of data over infrared light, for uses such as personal area networks (PANs). For the devices to communicate via IrDA they must have a direct line of sight.

LAN/WAN
Local Area Network (a computer network covering a small local area)/ Wide Area Network (a computer network covering a wide geographical area).

Malware
software designed to infiltrate or damage a computer system, without the user’s consent.

MP3
MPEG-1 Audio Layer 3 is a popular digital audio encoding and compression format.

PDA
Personal Digital Assistant, a handheld device supporting calendaring, address book, task list, memo pad, clock, and calculator functionality. Newer PDAs also have colour screens and audio capabilities, enabling them to be used as mobile phones, web browsers or media players. Many PDAs can access the Internet, intranets or extranets via wireless or mobile networks.
Security-classified any security classification above Unclassified

Spyware a broad category of malicious software designed to intercept or take partial control of a computer’s operation without the informed consent of the user. Usually exploits infected computers for commercial gain by delivering unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.

USB *Universal Serial Bus* – provides a serial bus standard for connecting devices, usually to computers.

VPN *Virtual Private Network*, a private communications network usually used within a company, or by several different companies or organisations, to communicate over a public network.

Wireless See 802.11 Wireless.