



Australian Government

**Department of Defence
Intelligence & Security**

Policy and Guidance for the Use of BlackBerry by the Australian Government

Defence Signals Directorate

Release Date: 31 March 2006

Table of Contents

Overview	3
BLACKBERRY POLICY	4
Overview	4
BlackBerry and Classified ICT Systems	5
Network Architecture Policy	6
BlackBerry Enterprise Server Configuration	7
BlackBerry Handhelds	9
Usage Policy and Procedures	11
ACSI 33 Keywords	12
TECHNICAL GUIDANCE	13
Overview	13
Network Architecture	14
BES Installation	15
Bluetooth Peripherals	18
S/MIME	20
BES IT POLICY SETTINGS	21
Overview	21
Settings	22

Overview

Introduction This document provides ICT security policy and technical guidance on the use of BlackBerry by the Australian Government. The information is derived from the Defence Signals Directorate's (DSD's) research into the BlackBerry Enterprise Server (BES) and the associated BlackBerry handhelds.

Sections The 'BlackBerry Policy' section covers all ICT security policy statements agencies are required to comply with when implementing BlackBerry.

It refers to the sections on 'Technical Guidance' and 'BES IT Policy Settings' as necessary, as well as more generic ICT security policy requirements defined in the *Australian Government ICT Security Manual (ACSI 33)*.

AGIMO documents The Australian Government Information Management Office (AGIMO), in conjunction with DSD, has developed additional guidance to support Australian Government agencies in implementing and managing the use of BlackBerry devices, and enabling officers to understand their responsibilities.

A Finance Instruction, "*Instructions on the Allocation and use of BlackBerry in the Australian Government*", has also been released to assist agency heads in interpreting the *Financial Management Act (FMA)* with respect to the use of BlackBerry.

These documents are available from the AGIMO website.

URL: <http://www.agimo.gov.au>

Contents This publication contains the following sections:

Section	See Page
BlackBerry Policy	4
Technical Guidance	13
BES IT Policy Settings	21

BlackBerry Policy

Overview

Summary

BlackBerry versions 3.6 to 4.x may be used for the transmission and storage of UNCLASSIFIED, X-IN-CONFIDENCE and RESTRICTED information in accordance with the policy contained in this document.

Note: The references to X-IN-CONFIDENCE throughout the policy do not include CABINET-IN-CONFIDENCE.

Keywords

The use of the keywords “MUST”, “MUST NOT”, “SHOULD”, “SHOULD NOT” and “RECOMMENDS” within this policy is consistent with the *Australian Government Information and Communications Technology Security Manual (ACSI 33)*.

See: ‘ACSI 33 Keywords’ on page 12 for a summary of the keywords.

Disclaimer

The issuing of this policy by the Defence Signals Directorate in no way implies any form of endorsement for the product or services described within.

BlackBerry has not completed a DSD-recognised formal evaluation; DSD has instead used a risk-managed approach to develop this policy.

Contents

This section contains the following topics:

Topic	See Page
BlackBerry and Classified ICT Systems	5
Network Architecture Policy	6
BlackBerry Enterprise Server Configuration	7
BlackBerry Handhelds	9
Usage Policy and Procedures	11
ACSI 33 Keywords	12

BlackBerry and Classified ICT Systems

Transmission and storage of classified information

Agencies may use BlackBerry versions 3.6 to 4.x for the transmission and storage of X-IN-CONFIDENCE and RESTRICTED information.

Agencies **MUST NOT** use BlackBerry for the transmission or storage of CABINET-IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET information.

Use with ICT systems processing classified information

Agencies **may** use BlackBerry with ICT systems that process information classified as:

- UNCLASSIFIED,
- X-IN-CONFIDENCE, or
- RESTRICTED.

Agencies **SHOULD NOT** use BlackBerry with ICT systems that process information classified as:

- CABINET-IN-CONFIDENCE,
- PROTECTED, or
- HIGHLY PROTECTED.

Agencies **MUST NOT** use BlackBerry with ICT systems that process information classified as

- CONFIDENTIAL,
- SECRET, or
- TOP SECRET.

Note: The phrase “use BlackBerry with ICT systems” means that some connectivity between the ICT system and BlackBerry exists. It does **not** mean that information of that classification is transmitted over the connection.

Controlling data transfer

Agencies **MUST** ensure that information is transferred between BlackBerry handhelds and the agency’s systems in accordance with *ACSI 33* (March 2005 or later).

Controls may need to be developed to cover situations where information such as contact details or meeting appointments may be classified above RESTRICTED or IN-CONFIDENCE, either individually or in aggregate.

See: ‘Electronic Mail Security’, ‘Electronic Mail – Protective Marking Policy’ and ‘Data Transfer’ in *ACSI 33*.

Network Architecture Policy

BlackBerry router

Agencies **SHOULD** install the BlackBerry router in a neutral subnetwork between the trusted corporate LAN and the Internet.

See: RIM document “*Placing the BlackBerry Router in the DMZ*”.

Additional firewall

The installation of an additional firewall between the BES and the internal mail servers allows the BES to be isolated from the rest of the network if it is compromised.

DSD **RECOMMENDS** agencies install an internal firewall between the BES and their internal mail servers.

Separation of services

Where RIM have provided the functionality to do so, agencies **SHOULD** separate services by installing them on different servers.

Note: This is currently possible for the Attachment Service.

Diagram

A diagram showing a typical configuration for a BlackBerry installation designed to mitigate known risks is included later in this document.

See: ‘Network diagram’ on page 14.

BES management

Agencies **SHOULD** manage the BES via a physical console. This removes the need for SNMP traffic to be permitted to the BES.

BlackBerry Enterprise Server Configuration

Using the BES	<p>Agencies using BlackBerry MUST use the “Enterprise” service.</p> <p>Note: This entails the use of a “BlackBerry Enterprise Server” (BES).</p>
BES IT policies	<p>Agencies SHOULD configure all IT policies within BES to at least meet that contained in this document.</p> <p>See: ‘BES IT Policy Settings’ on page 21.</p> <p>Note: If an IT policy is deleted from within the BES then all of the users associated with the deleted policy will be moved to the default policy.</p>
Determining permitted functionality	<p>User requirements for access to BlackBerry functions needs to be balanced against the risks associated with each of the functions under consideration.</p> <p>Agencies MUST base decisions on which functions to permit based on an assessment of the relevant risks and business benefits of allowing access.</p> <p>Information included elsewhere in this document may assist in identifying and assessing some of the relevant risks.</p> <p>See: ‘Technical Guidance’ on page 13.</p>
Host-based firewall	<p>DSD RECOMMENDS agencies install a host-based firewall on the BES, configured to limit traffic to the minimum necessary to allow the BES to perform its authorised tasks.</p>
Peer-to-peer messaging	<p>Peer-to-peer (also known as PIN-to-PIN) messaging allows users to send unencrypted messages directly to other handhelds.</p> <p>Agencies MUST NOT use peer-to-peer communications to transmit classified information.</p>
Using the Redirector	<p>Agencies MUST NOT use the “BlackBerry Desktop Redirector”.</p>
Using the MDS	<p>The “Mobile Data Service” (MDS) allows the BES software to act as a proxy between the agency’s Internet connection and the BlackBerry handhelds.</p> <p>DSD RECOMMENDS that agencies configure the MDS to use the agency’s proxy server.</p>

Continued on next page

BlackBerry Enterprise Server Configuration, Continued

Patching

Agencies **SHOULD** apply the relevant patches as specified in this document. Any agency deviating from this requirement **MUST** support the decision with a risk assessment that shows how the known vulnerabilities of the BES software are mitigated.

See: 'Technical Guidance' on page 13.

Generic policy on the patching and hardening of servers is given in *ACSI 33*.

See: 'Software Fundamentals' in *ACSI 33*.

Reviews

Agencies **SHOULD** perform a technical review designed to reveal any previously undetected compromises or other failures of security at least annually.

BlackBerry Handhelds

Choice of handhelds

This BlackBerry policy applies to any Java-enabled BlackBerry handheld model capable of running Version 3.6 or later, supplied and managed by the agency either directly or through a contractual arrangement.

See: 'Product Selection' in *ACSI 33* for policy on how to choose a product.

Agencies **MUST NOT** permit privately owned or managed BlackBerry handhelds to connect to classified agency systems.

Default settings

When initially installed, the BES provides a default IT policy. To avoid inadvertently activating insufficiently secure handhelds, these settings need to be reconfigured.

Agencies **MUST** reconfigure the BlackBerry default IT policy settings to reflect agency IT policies prior to providing handhelds to users for activation.

Storage and handling

Agencies **MUST** ensure that BlackBerry handhelds running version 3.6 of the handheld software are stored and handled in accordance with the classification of the information on them.

BlackBerry handhelds running version 4.x of the software may be stored and handled as for UNCLASSIFIED media even though they may contain X-IN-CONFIDENCE and/or RESTRICTED information.

Emanations security

Agencies **MUST** disable the wireless functionality of BlackBerry handhelds when in areas processing CONFIDENTIAL or SECRET information, by:

- a. turning off the RF Wireless function,
- b. turning off the BlackBerry handset, or
- c. removing the battery.

See: 'Portable Computers and Personal Electronic Devices' in *ACSI 33* for policy on PEDs within TOP SECRET areas.

Mobile phone functionality

BlackBerry handhelds can also function as a mobile phone.

See: 'Telephones and Telephone Systems' in *ACSI 33* for policy on the use of mobile phones.

Continued on next page

BlackBerry Handhelds, Continued

Bluetooth

Policy in *ACSI 33* limiting the use of wireless technologies such as Bluetooth applies only to the communication of classified information. Agencies therefore may choose to enable Bluetooth peripherals for UNCLASSIFIED voice communications without deviating from the defined policy.

DSD **RECOMMENDS** that any agencies enabling Bluetooth do so in accordance with the process defined in the Technical Guidance section of this document.

See: 'Bluetooth Peripherals' on page 18.

Agencies choosing to allow this **MUST** ensure that users are clearly instructed that only UNCLASSIFIED conversations may be held when using a Bluetooth-enabled peripheral device.

Agencies **MUST NOT** enable the Bluetooth serial port connection on any Blackberry handheld permitted to hold classified information.

Generic security requirements for PEDs

BlackBerry handhelds are a class of Personal Electronic Device (PED) and therefore the policy in *ACSI 33* that applies to PEDs also applies to the handhelds.

See: 'Portable Computers and Personal Electronic Devices' in *ACSI 33*.

Usage Policy and Procedures

Requirement for usage policy Agencies using BlackBerry **MUST**:

- a. have a policy and associated procedures for the use of the service, and
- b. ensure that staff acknowledge the policy and associated procedures before they are allowed to use the service.

Training The potential to compromise information on the BlackBerry is high unless strict user policy is adhered to.

As well as ensuring that staff acknowledge agency policy and procedures, as required above, agencies **SHOULD** train their staff in the use of the service, including the security requirements, before they are permitted to use it.

Passwords Agencies **MUST** ensure that users implement a password to control access to the BlackBerry handheld that either:

- a. is a minimum of 12 characters, with no complexity requirements, or
- b. meets the password selection policy in *ACSI 33*.

See: 'Password selection policy' in *ACSI 33*.

Lost or stolen handhelds It is possible to send a "Lock Handheld" or "Kill Handheld" signal to the BlackBerry handheld. A Lock signal causes the handheld to lock up until it is unlocked. A Kill signal causes the handheld to delete all data stored on it.

Agencies **SHOULD** have a policy and associated procedures for the use of these capabilities should a handheld be lost or stolen.

ACSI 33 Keywords

Introduction The following information has been extracted from the *Australian Government Information and Communications Technology Security Manual (ACSI 33)*.

Keywords for requirements The table below defines the keywords used within this policy to indicate the level of requirements. All keywords are presented in bold, uppercase format.

Keyword	Interpretation
MUST	The item is mandatory. See: ‘Waivers against “MUSTs” and “MUST NOTs”’ below.
MUST NOT	Non-use of the item is mandatory. See: ‘Waivers against “MUSTs” and “MUST NOTs”’ below.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. See: ‘Deviations from “SHOULDs” and “SHOULD NOTs”’ below.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course. See: ‘Deviations from “SHOULDs” and “SHOULD NOTs”’ below.
RECOMMENDS	The specified body’s recommendation or suggestion. Note: Agencies deviating from a RECOMMENDS are encouraged to document the reason(s) for doing so.

Waivers against “MUSTs” and “MUST NOTs” Agencies deviating from a “**MUST**” or “**MUST NOT**”, **MUST** provide a waiver in accordance with the requirements of the *Protective Security Manual*.

Deviations from “SHOULDs” and “SHOULD NOTs” 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.

DSD **RECOMMENDS** that ITSAs retain a copy of all deviations.

Technical Guidance

Overview

Introduction The information in this section is provided to give some technical guidance to agencies installing a BlackBerry solution consistent with Australian Government ICT security requirements as stated in the previous section.

Other software platforms This guidance is derived from the results of the DSD review in which the BES was installed upon a Microsoft (MS) Windows 2000 Server, configured to function with Microsoft Exchange Server version 5.5.

Certain aspects of the following guidance are therefore limited to these software versions. Where this occurs, agencies implementing BlackBerry solutions on other platforms are encouraged to apply comparable strategies to address the identified issues.

Currency Some of the information in this section, particularly with respect to current patches and URL locations, may become outdated. Although all such information is accurate at the time of publishing, agencies are advised to confirm that they have the latest information available when installing their BlackBerry systems.

Contents This chapter contains the following topics:

Topic	See Page
Network Architecture	14
BES Installation	15
Bluetooth Peripherals	18
S/MIME	20

Network Architecture

General principles

Distributing services will help to mitigate the effects of any future exploits and to improve availability, as will hardening the system by keeping permitted services and open ports to the minimum required.

Configuring the external firewall

The only traffic that should be passing through the firewall located between the Internet and the BlackBerry router is an agency-initiated connection to RIM's network operations centre.

Action: Configure the external firewall to permit only a single, outbound-initiated but bi-directional connection on port 3101 between the router and RIM.

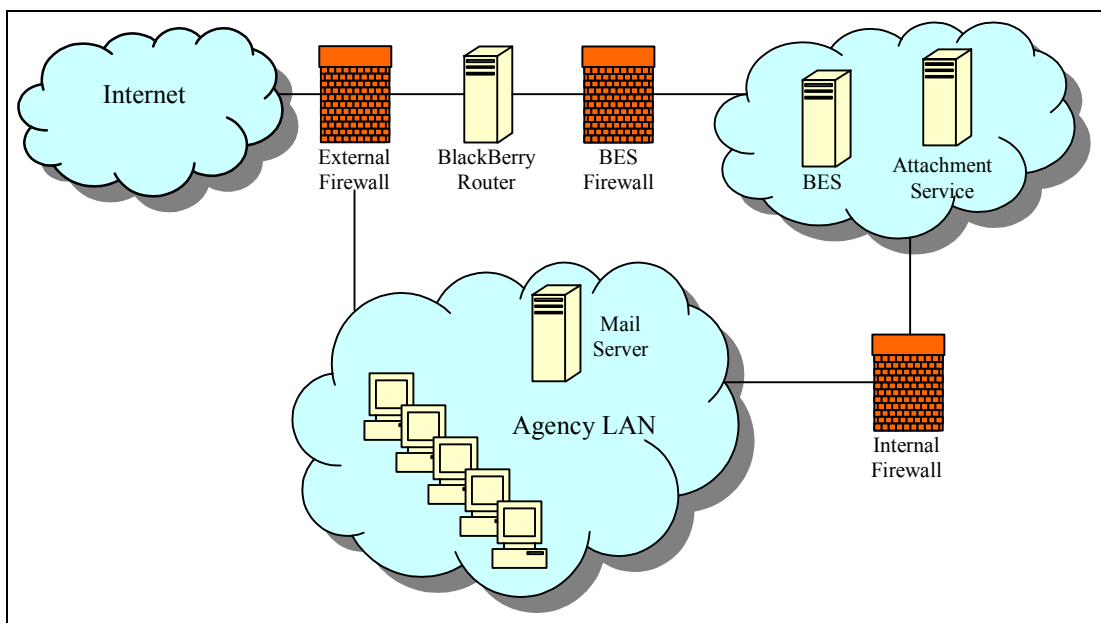
Attachment Service

The separation of the Attachment Service, which is known to have vulnerabilities, allows agencies to reduce the consequences of a successful attack against the Service by immediately isolating it from the network.

Action: Install the BlackBerry Attachment Server on a separate server to the BES.

Network diagram

The diagram below shows a typical configuration for a BlackBerry installation designed to mitigate known risks.



BES Installation

Patching the host operating system

Although the RIM installation guides do not provide advice on the level of vendor security patching that should be applied to either the BES's underlying operating system or the Microsoft Exchange server, best practice indicates that production servers be installed with the most current vendor cumulative patches and security hot fixes.

Information relating to patching levels is available from Microsoft's Technet.

Action: Apply relevant patches:

- Microsoft Windows 2000 Server – SP4,
 - Microsoft Windows 2003 Server – SP1, and
 - Any hot fixes released since these service packs.
-

Default Windows share

The default configuration for the BES, using a Microsoft Windows operating system, provides a Windows share of C:\ which is not required for BES functionality.

Action: Remove the C:\ share.

BES file share

Installing BES automatically creates a common network directory share for holding BlackBerry handheld software configuration files. These files are used to configure handhelds with the agency's IT policy; unauthorised modification to the files could reduce the security of handhelds.

Action: Set the handheld configuration files for Read Only access.

Additional hardening

A complete hardening guide and assessment is beyond the scope of this review as there are a number of server configurations that could be utilised. However, to ensure that the BES is protected against known vulnerabilities, agencies should ensure at minimum the vendor best security practice guidelines are followed. These guides will assist administrators in identifying the required patching levels and help to determine the necessary functions, services and file shares.

Action: Harden the Microsoft Windows 2000 Server supporting the BES platform in accordance with the vendor security guides, prior to installing any BlackBerry system.

Guides such as Microsoft's Baseline Security Analyser (MSBSA) and Windows 2000 Server Baseline Security Checklist were available at the time of draft from:

URL: www.microsoft.com/technet/security/tools/mbsahome.mspx

URL: www.microsoft.com/technet/archive/security/chklist/w2ksvrcl.mspx

Continued on next page

BES Installation, Continued

SQL Server 2000

The BES relies on configuration information being held in a Microsoft-compliant relational database. The option is available to install either a full version of Microsoft's SQL Server 2000, or Microsoft's SQL Server 2000 Desktop Engine (MSDE) during BES installation.

The full version of SQL Server 2000 is needed if administrators require management snap-ins for the local SQL database, as the functionality is not available with MSDE. Administrators will find SQL Server 2000 is useful if debugging is required during the installation process.

Action: If SQL Server 2000 is installed to the BES, apply the most current Microsoft cumulative patches and hot fixes. At time of draft this was SP4, available from:

URL:<http://support.microsoft.com/downloads/details.aspx?familyid=8E2DFC8D-C20E-4446-99A9-B7F0213F8BC5&displaylanng=en>

Browser

The BES requires Internet Explorer (IE) to be installed to allow viewing and navigation of locally stored RIM help files. However, the BES has no functional requirement for this IE installation to be aware of any external gateway allowing it to establish connections to the Internet, and to do so would greatly increase the risk to the system.

Note: The BES configuration manager, not the IE installation, is the service that allows the BES to conduct Internet requests made from BlackBerry handhelds.

Action: Ensure that all relevant IE Service Packs and associated post hot fixes have been applied to IE. IE 5.5 is currently at SP2 and IE 6.0 is at SP1

Action: Ensure that the server is not able to make connections to the Internet via the organisation's default gateway.

Action: Install a personal firewall to the BES with rules that allow the BES applications to communicate whilst explicitly denying IE.

Continued on next page

BES Installation, Continued

Exchange environment

The BES can be used with the following Exchange servers in the Microsoft Windows environment.

Action: Apply Microsoft cumulative Service Packs and post hot fixes for the version of Microsoft Exchange used prior to connection to the BES. At time of draft the current service packs for Microsoft Exchange were:

- a. MS Exchange 5.5 - Service Pack SP4, and security fixes MS05-029, MS05-012, MS04-026, MS03-047, MS03-046, MS01-047 and MS01-041,
- b. MS Exchange Server 2000 - SP3 and post SP3 update rollup and hot fixes, and
- c. MS Exchange Server 2003 - SP2.

Note: Microsoft has announced that Microsoft Exchange 5.5 will no longer be supported after 31 December 2005, so an upgrade strategy for moving to a supported application will be required.

Additional information

RIM provides a comprehensive guide on preparing and installing the system to operate in a functioning environment.

Action: Review the guide designed for the version of software that you intend to install, available from:

URL: <http://www.blackberry.com/knowledgecenterpublic>

RIM also provides a current series of hot fixes to address application efficiency and to mitigate against BES security issues. Australian service providers may provide local websites with this information and/or provide an update alert feature. A generic entry to this information is also available at:

URL: <https://www.blackberry.com/Downloads/entry.do?>

Action: Periodically check for and apply SPs and hot fixes to the BES Server as they become available.

Bluetooth Peripherals

Available peripherals

BlackBerry handhelds may incorporate Bluetooth functionality allowing pairing with the following peripherals:

- headset, and
- hands-free car set.

These peripherals are designed to allow hands-free voice communications only.

If agencies require a less risky hands-free option, the use of an earpiece and jack is recommended.

Recommended process

The risks of using Bluetooth within the context of BlackBerry handheld voice communications can be partially mitigated by using the process detailed below.

Step	Action
1	Ensure that BES Version 4 Service Pack 3 is installed at minimum. This will provide the Bluetooth IT Policy group with the option to disallow Bluetooth Discovery mode on the handheld.
2	Create a separate Bluetooth IT Policy Group on the BES for users that will be using Bluetooth. This policy should reflect all other agency IT policy settings with the exception of: <ul style="list-style-type: none"> • Bluetooth Policy Group: Disable Bluetooth = FALSE, • Bluetooth Policy Group: Disable Headset profile = FALSE, • Bluetooth Policy Group: Disable Pairing = TRUE, and • Bluetooth Policy Group: Disable Discovery Mode = TRUE.
3	Create a separate IT Policy for users that will not be using the Bluetooth peripherals: <ul style="list-style-type: none"> • Bluetooth Policy Group: Disable Bluetooth = TRUE.
4	Create a Bluetooth configuration IT Policy that represents the agency IT policy with the exception that: <ul style="list-style-type: none"> • Bluetooth Policy Group: Disable Bluetooth = FALSE, • Bluetooth Policy Group: Disable Headset profile = FALSE, • Bluetooth Policy Group: Disable Pairing = FALSE, and • Bluetooth Policy Group: Disable Discovery Mode = FALSE.
5	Within the confines of a controlled environment, set the handheld Bluetooth setting to Discoverable mode under the Bluetooth options menu. This will allow the device to be paired with a BlackBerry headset.

Continued on next page

Bluetooth Peripherals, Continued

Recommended process (continued)

Step	Action
6	Follow the RIM guide for pairing to the BlackBerry headset and ensure that: <ul style="list-style-type: none">• encryption with the paired device is used,• the device is set to non-discoverable mode, and• the handheld's Bluetooth device name is set.
7	Apply the Bluetooth IT Policy Group to the Handheld which disallows pairing to other devices.
8	Create a set of standard operating procedures for Bluetooth enabled users that is designed to educate them on the exploitability of Bluetooth and the manner in which they are to operate this function. Content may include: <ul style="list-style-type: none">• attempts to pair additional devices to the handheld are forbidden,• if prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators, and• the functionality is to be used only when a hands-free environment is required, and the functionality should be turned off whenever this is not the case.

S/MIME

Using S/MIME The introduction of Secure MIME (S/MIME) would ensure that end-to-end encryption using a DSD approved cryptographic protocol is applied to emails between all users, including the BlackBerry handheld. The use of S/MIME on an enterprise email system would therefore mitigate some of the risks introduced by a BlackBerry system.

BlackBerry networks are able to handle S/MIME and its introduction would decrease the attractiveness of all sources of email content information, including the BES.

Considerations If S/MIME is used, the network owner has to allow the traversal of encrypted information through their firewall to the mail server. Methods of dealing with the agency's email filtering and anti-virus protection requirements at the workstation, rather than just the gateway environment, would then need to be implemented.

Action: Consider the introduction of S/MIME to the enterprise wide mail network.

BES IT Policy Settings

Overview

Introduction	<p>The BlackBerry solution provides users with a broad range of options—approximately 175 IT policy settings—aimed at delivering end user functionality and flexibility.</p> <p>To ensure that security is also addressed by these settings, DSD has reviewed the available settings and determined appropriate values, consistent with <i>ACSI 33</i>, where relevant.</p>
Requirement for compliance	<p>Some of these settings MUST be implemented, in accordance with policy statements elsewhere within this document and <i>ACSI 33</i>.</p> <p>Other settings defined here but not referred to elsewhere SHOULD be followed.</p>
Other settings	<p>This section does not contain the full list of settings. Those setting not included here were not considered by DSD to have a direct impact on security and therefore are left up to the discretion of each agency.</p>
Versions	<p>The settings listed here are derived from a review of Version 4.0. If using Version 3.6, non-existent settings may be disregarded.</p>

Settings

**Non-grouped
Device-only**

The following settings are non-grouped device-only items:

Name	Value	Notes
Allow Peer-to-Peer messages	False	
Allow SMS	[Agency decision]	Messages sent via SMS cannot be logged by the BES. Only UNCLASSIFIED messages may be sent.
Default browser config UID	Null	This will ensure that the default RIM browser is used.
Enable long term timeout	True	
Enable WAP configuration	False	Maintain accountability by forcing all Internet browsing to go through the BES.
Maximum password age	90 days	
Maximum security timeout	5 min	
Minimum password length	[see Notes]	Set to 7 or greater if pattern checks = 3. Set to 12 or greater if pattern checks = 0.
Password pattern checks	[see Notes]	Set to 3 if password length is less than 12. Set to 0 if password length is 12 or greater.
Password required	True	
User can change timeout	False	
User can disable passwords	False	

**Non-grouped
Desktop-only**

The following settings are non-grouped desktop-only items:

Name	Value	Notes
Auto backup enabled	True	
Auto backup include all	True	
Auto signature	[Agency decision]	Ensure that no information identifying version numbers or that the email originated from a BlackBerry handheld is included.
Do not save sent messages	False	Ensure that a copy of all sent emails is saved.
Email conflict desktop wins	True	
Force load count	0	

Continued on next page

Settings, Continued

Non-grouped Desktop-only (continued)

Name	Value	Notes
Show application loader	False	
Show web link	False	

Common Policy Group The following group of settings controls some BlackBerry policies that apply to multiple groups:

Name	Value	Notes
BlackBerry Server Version	Null	Providing the version number may allow attackers to determine vulnerabilities more easily.
Disable MMS	True	The Multimedia Message Service does not go via the BES.
IT policy notification	True	Advising users when policy settings have changed will allow them to better judge whether a handheld is not behaving as expected.
Lock owner info	3	Lock down the fields with as little identifying information as necessary.
Set owner info	[see Notes]	Include sufficient information to enable a lost handheld to be returned, with no further identifying information. Example: If found, please return to BlackBerry PO Box XXX etc.
Set owner name	[see Notes]	Include as little identifying information as necessary: Example: Government Device [Asset number if necessary]

Password Policy Group

The following group of settings controls the use of passwords:

Name	Value	Notes
Maximum password history	8	No re-use within two years, based on a 90 day cycle.
Periodic challenge time	60 min	
Set maximum password attempts	5	
Set password timeout	5 min	
Suppress password echo	True	

Continued on next page

Settings, Continued

Security Policy Group The following group of settings controls various aspects of security:

Name	Value	Notes
Allow external connections	False	Prevent the handheld from opening connections to the Internet
Allow internal connections	False	
Allow smart card password caching	False	RIM recommendation.
Allow split pipe connections	False	Such connections can pass through the firewall without creating an audit trail.
Allow third party applications to use serial port	False	No third party applications are approved.
Application download control	[see Notes]	Limit the permitted downloads to certified applications only.
Certificate status cache timeout	1 day	
Certificate status maximum expiry time	4 hours	
Disable 3DES transport crypto	False	Ensure that encryption of packets between the BES and the handheld is enabled.
Disable email normal send	[see Notes]	If agencies have not implemented S/MIME, then set to False .
Disable forwarding between services	True	
Disable invalid certificate use	True	
Disable IP modem	True	Disable the modem capability where present.
Disable key store backup	True	
Disable key store low security	True	
Disable peer-to-peer normal send	True	
Disable persisted plaintext	True	Ensure that data stored in non-volatile memory is encrypted.
Disable radio when cradled	1	Do not allow the handheld to transmit RF when connected to workstations.
Disable revoked certificate use	True	
Disable stale status use	True	

Continued on next page

Settings, Continued

Security Policy Group (continued)

Name	Value	Notes
Disable third-party applications download	True	
Disable untrusted certificate use	True	
Disable unverified certificate use	True	
Disable unverified CRLs	True	
Disable weak certificate use	True	
FIPS level	2	
Forced lock when holstered	True	
Minimal encryption keystore security level	2	“2” = “high security”
Minimal signing keystore security level	2	“2” = “high security”

TLS Application Policy Group

The following group of settings controls the use of Transport Layer Security (TLS):

Name	Value	Notes
TLS device side	False	
TLS disable invalid connection	0	Disabled
TLS disable untrusted connection	0	Disabled
TLS disable weak ciphers	0	Disabled
TLS minimum strong DH key length	1024 bits	
TLS minimum strong DSA key length	1024 bits	
TLS minimum strong ECC key length	163 bits	
TLS minimum strong RSA key length	1024 bits	

WTLS Application Policy Group

The following group of settings controls the use of Wireless Transport Layer Security (WTLS):

Note: WTLS mode allows users to bypass the agency’s gateway infrastructure.

Name	Value	Notes
WTLS disable invalid connection	0	Disabled
WTLS disable untrusted connection	0	Disabled
WTLS disable weak ciphers	0	Disabled
WTLS minimum strong DH key length	1024 bits	
WTLS minimum strong ECC key length	163 bits	
WTLS minimum strong RSA key length	1024 bits	

Continued on next page

Settings, Continued

Browser Policy Group The following group of settings controls the use of the browser:

Name	Value	Notes
Disable execution of Java script in the handheld browser	True	

Bluetooth Policy Group The following group of settings controls the use of Bluetooth:

Name	Value	Notes
Disable pairing	True	If an agency has decided to implement Bluetooth, then this setting must be changed to “True” immediately after the approved peripherals have been paired, to prevent any additional, non-approved devices to be added later.
Disable serial port profile	True	

Desktop Policy Group The following group of settings controls the Desktop Policy:

Name	Value	Notes
Desktop password cache timeout	10 min	
Desktop allow desktop add-ins	False	Desktop software to be managed by the agency in accordance with the risk assessment.
Desktop allow device switch	False	Use to prevent users from switching to other devices.

Service Exclusivity Policy Group The following group of settings controls the service exclusivity:

Name	Value	Notes
Allow other email services	False	Force all email to go through the BES.
Allow other browser services	False	Force all web browsing to go through the BES
Allow public Yahoo! Messenger service	False	

Continued on next page

Settings, Continued

**S/MIME
Application**

The use of S/MIME is not mandated. However, if it is used, it must be configured in accordance with *ACSI 33* requirements .

See: ‘DSD Approved Cryptographic Protocols (DACPs)’ in *ACSI 33*.

The following group of settings defines how to configure S/MIME in accordance with *ACSI 33*:

Name	Value	Notes
S/MIME allowed content ciphers	0,5	Allows DACAs: AES (256) and 3DES.
S/MIME blind copy address	[Agency decision]	If used, seek legal advice on appropriate warnings to users.
S/MIME minimum strong DH key length	1024	
S/MIME minimum strong DSA key length	1024	
S/MIME minimum strong ECC key length	163	
S/MIME minimum strong RSA key length	1024	
