ICT Security Policy for the Use of BlackBerry by the Australian Government

Overview

Version

October 2005

Introduction

This document provides ICT security policy on the use of BlackBerry® by the Australian Government. DSD has based the policy on the results of its research.

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.

Contents

This document contains the following topics:

Policy

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 8 for a summary of keywords.

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 UNCLASSIFIED, X-IN-CONFIDENCE and RESTRICTED information.

Agencies **SHOULD NOT** use BlackBerry with ICT systems that process CABINET-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED information.

Agencies **MUST NOT** use BlackBerry with ICT systems that process CONFIDENTIAL, SECRET or TOP SECRET information.

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.

Continued on next page

Policy, Continued

Communications methods

Agencies using BlackBerry **MUST** use the "Enterprise" service.
Note: This entails the use of a "BlackBerry Enterprise Server" (BES).

Agencies **MUST NOT** use peer-to-peer ("PIN to PIN") communications to transmit classified information.

Agencies **MUST NOT** use the "BlackBerry Desktop Redirector".

The "Mobile Data Service" (MDS) allows the BES software to act as a proxy between the agency's Internet connection and the BlackBerry devices. DSD **RECOMMENDS** that agencies configure the MDS to use the agency's proxy server.

Agencies **SHOULD** disable the use of Wireless Transport Layer Security (WTLS) mode.
Note: WTLS mode allows users to bypass the agency's gateway infrastructure.

BlackBerry devices can also function as a mobile phone.
See: 'Telephones and Pagers' in ACSI 33 for policy on the use of mobile phones.

Content filtering

Agencies **MUST** ensure that content is transferred between the BlackBerry devices and the agency's systems in accordance with ACSI 33.
See: 'Electronic Mail Security', 'Electronic Mail – Protective Marking Policy' and 'Data Transfer' in ACSI 33.

BES IT Policies

Agencies **SHOULD** configure all IT policies within BES to at least meet that contained in this document.
See: 'BES IT Policy Settings' on page 5.

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.

Continued on next page

Policy, Continued

Usage policy and procedures

Agencies using BlackBerry **MUST** have a policy and associated procedures for the use of the service.

Agencies **MUST** ensure that staff acknowledge the policy and associated procedures before they are allowed to use the service.

DSD **RECOMMENDS** that agencies train their staff in the use of the service, including the security requirements, before they are permitted to use it.

Agencies **MUST** ensure that users implement a password that controls access to the BlackBerry device that meets the password selection policy in ACSI 33.
See: 'Password selection policy' in ACSI 33.

It is possible to send a "Lock Handheld" or "Kill Handheld" signal to the BlackBerry device. A Lock signal causes the device to lock up until it is unlocked. A Kill signal causes the device to delete all data stored on it. Agencies **SHOULD** have a policy and associated procedures for the use of these capabilities should a device be lost or stolen.

Storage and handling

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

BlackBerry handheld devices that are 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.

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.

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 undergone a DSD-recognised formal evaluation and therefore DSD has used a risk-managed approach to develop this policy.

BES IT Policy Settings

Introduction

This section contains the IT policy settings used by DSD during its research. They are consistent with ACSI 33, where relevant.

Note: This is not the full list of settings for BES version 3.6. Those not in these lists were not considered by DSD to have a direct impact on security and therefore are left up to the discretion of each agency.

Ungrouped Device-only Items

The following settings are ungrouped device-only items:

Name	Value
Password required	True
Allow PIN to PIN	False
Minimum password length	7
Users can disable passwords	False
Maximum security timeout	5 minutes
Maximum password age	90 days
User can change timeout	True
Password pattern checks	3
Enable long term timeout	True
Enable WAP configuration	False

Ungrouped Desktop-only Items

The following settings are ungrouped desktop-only items:

Name	Value
Show application loader	False
Force load count	0
Email conflict desktop wins	True
Auto backup enabled	True
Auto backup frequency	1 day
Auto backup include all	True
Allow other email services	False

Continued on next page

BES IT Policy Settings, Continued

Password Policy Group

The following group of settings control the use of passwords:

Name	Value
Set password timeout	3 minutes
Set maximum password attempts	3
Suppress password echo	True
Maximum password history	8

Compressed MIME (CMIME) Application Policy Group

The following group of settings control the use of Compressed MIME:

Name	Value
Disable revoked certificate use	True
Disable Peer to Peer normal send	True
Disable key store low security	True
Key store password maximum timeout	60 minutes
Disable third-party applications download	True
Forced lock when holstered	True
Allow third-party applications to use serial port	False
Allow internal connection	False
Allow external connections	False
Allow split pipe connections	False
Disable invalid certificate use	True
Disable weak certificate use	True

Continued on next page

BES IT Policy Settings, Continued

Transport Layer Security (TLS) Application Policy Group

The following group of settings control the use of Transport Layer Security:

Name	Value
TLS disable weak ciphers	0 (disabled)
TLS disable untrusted connection	0 (disabled)
TLS minimum strong RSA key length	1024 bits
TLS minimum strong DH key length	1024 bits
TLS minimum strong ECC key length	163 bits
TLS disable invalid connection	0 (disabled)
TLS restrict FIPS ciphers	False
TLS minimum strong DSA key length	1024 bits

Wireless TLS (WTLS) Application Policy Group

The following group of settings control the use of Wireless Transport Layer Security:

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

Desktop Policy Group

The following group of settings control the Desktop Policy:

Name	Value
Desktop password cache timeout	10 minutes
Desktop allow desktop add-ins	False
Desktop allow device switch	False

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 **RECOMMENDED**	The specified body's recommendation or suggestion. **Note:** Agencies deviating from a **RECOMMENDS** or **RECOMMENDED** 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.

Change Summary

July 2005

This block contains a summary of the changes that have been made between the March 2005 and the July 2005 versions of this policy.

Note: Minor changes to fix editorial and presentation issues have not been included.

Section	Change
(Various)	Clarified the intent of the policy by adding "and storage" to policy statements referring to "transmission".
Summary	Reduced the scope of the approval from "version 3.6 and later" to "versions 3.6 to 4.x".
Use with ICT systems processing classified information	Added a note to reduce potential confusion regarding the interpretation of these policy statements.
Communications methods	• Removed "BlackBerry Web Client" from the second paragraph. • The two remaining items in the second paragraph of this Block were split into two separate statements.
Storage and handling	Added this new block on the storage and handling of the handheld devices.

October 2005

This block contains a summary of the changes that have been made between the July 2005 and the October 2005 versions of this policy.

Section	Change
Ungrouped Device-only Items	Amended the value for the "Maximum security timeout" setting to "5 minutes".