BETTER PRACTICE GUIDANCE

24. User Requirements for BlackBerry® Devices

Introduction

Section 44 of the Financial Management and Accountability (FMA) Act 1997 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. BlackBerry 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).

Like other technologies, the efficient and effective use of BlackBerry requires informed planning and careful management, paying particular attention to security considerations.

A key role of the Australian Government Information Management Office (AGIMO) is to identify and promote ‘Better Practice’ in the use of ICT in government. This Better Practice Guidance sets out the User Requirements for the effective use of BlackBerry and is complementary to Better Practice Guidance No. 23 - Use of BlackBerry Devices. This guidance may be used as the basis for an agency’s BlackBerry policy and is applicable to staff, contractors and consultants, whether on or off-site, using or connecting to an agency’s network facilities. It complements, but cannot be used as a substitute for policy available from DSD.

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

Emerging Technologies Team
Australian Government Information Management Office
Department of Finance and Administration
Phone: (02) 6215 1546

Email: better.practice@finance.gov.au

Acknowledgments

This guidance was developed with the assistance of the Defence Signals Directorate (DSD).
What is BlackBerry?

BlackBerry is the proprietary name for a series of personal digital assistant (PDA) hardware devices and associated network server services developed and supplied by the Research in Motion (RIM) organisation, with the supply of corresponding network services from the major Australian telecommunications carriers.

BlackBerry devices provide converged mobile telephone and digital assistant technologies into a single piece of hardware. BlackBerry integrates with existing user networks for wireless access to electronic mail (email) and other corporate data such as online diary. The device provides telephone, Short Message Service (SMS), web browser, word processing and organiser functions. BlackBerry uses proprietary software and hardware to connect to the computing systems of the user’s organisation. The handsets feature a keyboard, thumb-operated track-wheel and intuitive navigation menus.

It is anticipated that the market penetration of devices offering similar services will increase as other vendors release similar technologies in coming months.

One of the principal features of a BlackBerry is that electronic mail (including attachments) can be ‘pushed-out’ (automatically sent) to the handset. The user receives information without having to dial up or manually synchronise with the organisation’s electronic mail system.

When BlackBerry may, should not and must not be used

Under Defence Signals Directorate (DSD) ICT Security Policy for the Use of BlackBerry by the Australian Government:

a) BlackBerry may be used for the transmission and storage of X-In-Confidence and Restricted information.
   If an agency can demonstrate a business need for BlackBerry, the AGIMO guidance, supported by DSD, requires that agencies must:
   i. comply with the Defence Signals Directorate (DSD) ICT Security Policy on BlackBerry
   ii. implement the relevant requirements for email protective markings from the most current release of ACSI 33
   iii. implement the protective markings in accordance with the implementation guide and standards for email protective markings.
   Better Practice Guidance No. 23 – *Use of BlackBerry® Devices*, provides further detail.

b) BlackBerry must not be used for the transmission or storage of Cabinet-in-Confidence, Protected, Highly Protected, Confidential, Secret or Top Secret information.

c) BlackBerry may be used with ICT systems that process Unclassified, X-In-Confidence and Restricted information.
   If an agency can demonstrate a business need for BlackBerry, the AGIMO guidance, supported by DSD, requires that agencies must:
   i. comply with the Defence Signals Directorate (DSD) ICT Security Policy on BlackBerry
   ii. implement the relevant requirements for email protective markings from the most current release of ACSI 33
iii. implement the protective markings in accordance with the implementation guide and standards for email protective markings.

Better Practice Guidance No. 23 – *Use of BlackBerry® Devices*, provides further detail.

d) BlackBerry should not be used with ICT systems that process Cabinet-In-Confidence, Protected or Highly Protected information.

Agencies with a demonstrated business need for BlackBerry must meet the ACSI 33 requirements for deviating from a “should not” (paragraph 1.0.18). The AGIMO guidance, supported by DSD, requires that agencies must:

i. comply with the Defence Signals Directorate (DSD) ICT Security Policy on BlackBerry

ii. implement the relevant requirements for email protective markings from the most current release of ACSI 33

iii. implement the protective markings in accordance with the implementation guide and standards for email protective markings

iv. have the agency’s gateways configured to ensure that emails and attachments classified at Cabinet-In-Confidence, Protected or Highly Protected are not sent to/from BlackBerry.

In addition, the Chief Executive must:

v. meet ACSI 33 requirements and have no waivers in place that are relevant to the proposed implementation of BlackBerry

vi. have no outstanding issues from system security or security audit reports that are relevant to the proposed implementation of BlackBerry

vii. have ICT systems certified and accredited in accordance with requirements of ACSI 33

viii. undertake and complete a post implementation review of BlackBerry within 12 months.

Better Practice Guidance No. 23 – *Use of BlackBerry® Devices*, provides further detail.

e) BlackBerry must not be used with ICT systems that process Confidential, Secret or Top Secret Information.
## GUIDANCE SUMMARY

### BEFORE YOU START
- Seek Chief Executive approval for the use of BlackBerry devices.
- Identify policy and standards relevant to the use of BlackBerry devices.
- Be aware of agency policies and procedures, including any restrictions, for the use of BlackBerry devices.

### PREPARATION BEFORE FIRST USE
- Undertake training in the use of BlackBerry devices, their handling and security requirements.
- Formally acknowledge in writing your agreement to adhere to agency policies and associated procedures before using the device.

### MANAGE USE
- Use BlackBerry in accordance with specific agency information and communications technology (ICT) Security Policy, standards, procedures or guidelines.
- Be aware of your responsibilities regarding the protection, storage and handling of the BlackBerry device.
- Be aware of the risks of using the BlackBerry mobile phone capability and associated messaging services.
- Implement password and access management control practices on BlackBerry that meet policy requirements.
- Because of security risks, do not transmit any security classified emails or attachments above RESTRICTED / X-IN-CONFIDENCE from BlackBerry.
- Classify and add a protective marking to all email.
- Be aware that BlackBerry to BlackBerry messaging (PIN-to-PIN) is not permitted.
- Report damaged, lost or stolen BlackBerry devices.

### AUDITING
- Be aware that agencies will audit compliance with policies and standards for the use of BlackBerry devices.
CHECKPOINTS

BEFORE YOU START

☑ Seek Chief Executive approval for the use of BlackBerry devices.

Seek formal approval from the agency Chief Executive for the procurement and use of BlackBerry devices.

☑ Identify policy and standards relevant to the use of BlackBerry devices.

Relevant policies and standards include:

- The Protective Security Manual. Describes the security policies, standards and individual responsibilities for the protection of Australian Government information and resources.

- 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.

- ICT Security policy for the Use of BlackBerry by the Australian Government DSD Describes the ICT policy on the use of BlackBerry by the Australian Government.

- Better Practice Guidance No.23 – Use of BlackBerry Devices, including Appendix A, BlackBerry Implementation Criteria Provides guidance on where BlackBerry may, should not and must not be implemented and the standards required for the implementation.

☑ Be aware of agency policies and procedures, including any restrictions, for the use of BlackBerry devices.

Effective policies and procedures help to ensure that an agency considers relevant issues and operates in accordance with the appropriate guidelines. Documenting and making these available to BlackBerry users will help to ensure that you are aware of the organisation’s expectations when using these devices.

Policies and procedures used by agencies may include: formal approval requests; assigning each BlackBerry an asset number; having users sign for the asset allocated to them; and / or limiting use to security cleared personnel.
PREPARATION BEFORE FIRST USE

☐ Undertake training in the use of BlackBerry devices, their handling and security requirements.

In many cases the failure to follow policies and procedures is not a result of deliberate actions, but a lack of awareness of requirements. Training in the appropriate use of BlackBerry devices can assist you to implement the agency’s policies and procedures. The completion of training may also help distinguish deliberate misuse from accidental or incompetent usage.

You should also be aware that these devices are likely to be attractive targets for thieves, and that the implications of the disclosure of information contained in them could be detrimental to the Australian Government.

☐ Formally acknowledge in writing your agreement to adhere to agency policies and associated procedures before using the device.

You are responsible for its handling, storage and appropriate use of the device. You must be aware of and agree to act in accordance with the agency’s policy and procedures. The ramifications of failing to apply those policies and procedures must be clear.

MANAGE USE

☐ Use BlackBerry in accordance with specific agency information and communications technology (ICT) Security Policy, standards, procedures or guidelines.

☐ Be aware of your responsibilities regarding the protection, storage and handling of the BlackBerry device.

You must ensure that the BlackBerry device is stored and handled in accordance with the security classification of the information contained in them. Even devices that transmit or store UNCLASSIFIED information have an intrinsic value and must be protected from damage, loss or theft.

BlackBerry devices are issued to an approved individual. They must not be shared between co-workers, staff, friends or family members.

If the device becomes damaged, is lost or stolen please contact your agency client services support team immediately.

☐ Be aware of the risks of using the BlackBerry mobile phone capability and associated messaging services.

You must be aware of the risks of using the BlackBerry mobile phone capability, including while classified conversations are being held nearby.
You should not use the mobile phone for the transmission of IN-CONFIDENCE information unless the mobile phone user is located within Australia.

You must not use the mobile phone for the transmission of RESTRICTED, PROTECTED, CONFIDENTIAL, HIGHLY PROTECTED, SECRET or TOP SECRET information.

You must not use the Short Message Services (SMS) and Multimedia Messaging Service (MMS) paging services to transmit classified material.

☐ Implement password and access management control practices on BlackBerry that meet policy requirements.

The implementation of robust password practices will help to ensure that if the device is lost or stolen, they cannot be easily used, or the information on them easily accessed.

Passwords should be a minimum of 7 characters, and consist of at least 3 of the following character sets:
1. lowercase characters (a-z);
2. uppercase characters (A-Z);
3. digits (0-9); and
4. punctuation and special characters.
   (e.g. ! @ # $ % ^ & *)

Passwords must also:
• be changed at least every 90 days;
• not be changed more than once a day;
• not be reused; and
• not be shared or disclosed to anyone else.

A password enabled screen lock will activate after a system defined period of device inactivity (typically 3 minutes). Additionally, you will need to re-enter your username/password after 60 minutes of continuous use.

After a number of incorrect logon attempts (agency defined), the device will lock and you will need to contact your agency client services support team for it to be unlocked. All user data on the device will also be erased.

☐ Because of security risks, do not transmit any security classified emails or attachments above RESTRICTED / X-IN-CONFIDENCE from BlackBerry.

Do not send any information classified CABINET-IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET to or from a BlackBerry device.

☐ Classify and add a protective marking to all email.

The use of BlackBerry devices will require you to classify and protectively mark all information transmitted to and from the device. This information includes emails and attachments.

The protective marking applied to the email must reflect the highest classification of the content of the email including any attachments. This helps to ensure that the content is
appropriate to be sent to these devices. Permitted classifications, depending on agency policy, may include: UNCLASSIFIED; X-IN-CONFIDENCE and RESTRICTED.

Training will be provided on how to appropriately classify and add a protective marking to emails and attachments.

Be aware that BlackBerry to BlackBerry messaging (PIN-to-PIN) is not permitted.

BlackBerry PIN-to-PIN (direct peer-to-peer communication) bypasses the standard device security features. You should be aware that this facility is not permitted and has been disabled.

Report damaged, lost or stolen BlackBerry devices.

If the device becomes damaged, is lost or stolen you should contact your agency client services support team immediately. They will provide details on the formal reporting requirements, the sanitisation of the data contained on the device and how to obtain a replacement. They may also highlight specific polices or requirements with respect to the handling, storage or use of the device or the need for additional training.

AUDITING

Be aware that agencies will audit compliance with policies and standards for the use of BlackBerry devices.

Setting and disseminating policy without monitoring compliance is bad practice. You should be aware that agencies may initiate internal – and from time to time external – checks of compliance with policies governing the use of these devices.

There will also be regular reviews of internal policies, to test their currency and adequacy, which may necessitate refresher training.

Other Resources

For further information about security requirements, see the following:

Protective Security Manual:

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

Defence Signals Directorate policy on the use of BlackBerry devices:

Australian Government Information Management Office, Better Practice Guidance and Checklists: