BETTER PRACTICE GUIDANCE

23. Use of 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 (e.g. 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 whole-of-government security considerations.

The Defence Signals Directorate (DSD) has developed ICT security policy on the use of BlackBerry in the Australian Government. This may be obtained from www.dsd.gov.au/library/index.html

This Better Practice Guidance No. 23 – Use of BlackBerry Devices and Better Practice Guidance No. 24 – User Requirements for BlackBerry Devices have been developed to assist Chief Executives in considering the approval, requirements and appropriate use of BlackBerry in their ICT environment in accordance with government security policy and consistent with a risk managed approach.

Comments about the checklist 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 checklist 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 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

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

BEFORE IMPLEMENTING BLACKBERRY
- Develop agency policies and procedures, including any restrictions, for the use of BlackBerry that align with Australian Government policies and standards and that adhere to Defence Signals Directorate (DSD) information security requirements.
- Implement processes to security classify, protectively mark and control the flow of information that may be transmitted to/from BlackBerry.
- Undertake a BlackBerry pre-implementation review.

MANAGE USE
- Provide staff with training on the use of BlackBerry and security requirements.
- Ensure that staff acknowledge formally in writing their agreement to adhere to specific agency and Australian Government policies and associated procedures.
- Ensure that users classify and protectively mark all email in accordance with the highest classification of the content or attachment in accordance with Australian Government standards.

INFRASTRUCTURE ISSUES
- Only use an “enterprise” server (BES) to support BlackBerry that is controlled, either directly or under contracted arrangements, by the Australian Government.
- Agencies must ensure that content is transferred between a BlackBerry device and an agency’s ICT systems in accordance with DSD security policy.
- Ensure that email originating outside the agency is not sent to BlackBerry unless it is UNCLASSIFIED, X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) or RESTRICTED and labelled accordingly.

REVIEW AND AUDIT
- Undertake a BlackBerry post implementation review.
- Audit compliance with policies and standards for the use of BlackBerry devices.
CHECKPOINTS

CHIEF EXECUTIVE APPROVAL

☐ Identify policy and standards relevant to the approval, deployment and use of BlackBerry.

Relevant policies and standards include:

- The Protective Security Manual (PSM). 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.

- Appendix A - BlackBerry Implementation Criteria (attached). Provides guidance on where BlackBerry may, should not and must not be implemented and the standards required for the implementation.

For agencies considering using BlackBerry with ICT systems that process CABINET-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED information, unless all of the identified requirements are fully met, BlackBerry must not be used with these systems.

The table also shows the requirements that must be met for using BlackBerry with systems that store or transmit UNCLASSIFIED, X-IN-CONFIDENCE or RESTRICTED information.

☐ Seek Chief Executive approval for the implementation of BlackBerry.

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), including the approval and use of BlackBerry.
BEFORE IMPLEMENTING BLACKBERRY

❑ Develop agency policies and procedures, including any restrictions, for the use of BlackBerry 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 BlackBerry devices.

Better Practice Guidance No. 24 provides further information on the user requirements for BlackBerry.

Appendix A provides guidance on where BlackBerry may, should not and must not be implemented and the minimum standards required for the implementation.

❑ Implement processes to security classify, protectively mark and control the flow of information that may be transmitted to/from BlackBerry.

Agencies must security classify and protectively mark all email including to/from BlackBerry. Controls must also be implemented at the email servers and gateways to restrict the delivery of inappropriate security classified information into and out of an agency, including to BlackBerry.

The levels of security classified information that may, should not and must not be transmitted to/from BlackBerry are described in the DSD “ICT Security Policy for the Use of BlackBerry by the Australian Government”.

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 BlackBerry.

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.

Software tools to assist in applying protective markings to email, user training and protective marking server controls must be implemented before BlackBerry may be deployed.

❑ Undertake a BlackBerry pre-implementation review.

Agencies deploying BlackBerry may consider undertaking a pre-implementation review. This review would assess the planned deployment strategy, mitigation controls, policies and procedures against the requirements defined in the relevant policy and guidance documents.

Defence Signals Directorate can assist in ensuring the necessary steps have been followed.
MANAGE USE

☑ Provide staff with training on the use of BlackBerry and security requirements.

In many areas of administration, 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 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.

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

Staff using a BlackBerry 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.

Better Practice Guidance No. 24 provides further information on the user requirements for BlackBerry.

☑ Ensure that users classify and protectively mark all email in accordance with the highest classification of the content or attachment in accordance with Australian Government standards.

Users must be conscious of the security classification of information that they are sending to or from BlackBerry and whether that information is appropriate to be transmitted to these devices. Agencies must ensure that users classify and protectively mark all agency-originated email or attachments in accordance with the highest classification of the content.

In accordance with DSD security policy information classified CABINET-IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED, CONFIDENTIAL, SECRET OR TOP SECRET must not be stored or transmitted to or from BlackBerry.

INFRASTRUCTURE ISSUES

☑ Only use an “enterprise” server (BES) to support BlackBerry that is controlled, either directly or under contracted arrangements, by the Australian Government.

By using an enterprise server controlled by the Australian Government, some risks associated with the use of BlackBerry may be mitigated. The BES server will be situated behind a controlled gateway environment and will permit the implementation of consistent agency policy and device settings as described in the DSD BlackBerry policy. An example policy that must be implemented using this facility is the disabling of peer-to-peer (PIN to PIN) communications.
Agencies must ensure that content is transferred between a BlackBerry device and an agency's ICT systems in accordance with DSD security policy.

Email protective marking filtering mechanisms must be implemented to provide a higher level of security by automatically preventing information classified above X-IN-CONFIDENCE or RESTRICTED being sent to BlackBerry.

These mechanisms are described in the “Implementation Guide for Email Protective Markings for Australian Government Agencies”.

Ensure that email originating outside the agency is not sent to BlackBerry unless it is UNCLASSIFIED, X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) or RESTRICTED and labelled accordingly.

Communications originating outside the agency may also include classified information. The policies and standards applied to external communications must also be applied to internally generated information.

Each agency must develop and implement procedures that ensure emails and attachments, whatever their source, are appropriately classified and protectively marked. Only UNCLASSIFIED, RESTRICTED or X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) emails and attachments may be transmitted to BlackBerry devices. Emails that do not have protective marking must not be transmitted to BlackBerry devices. Agency policy may define a subset of these classifications - for example, an agency may only permit UNCLASSIFIED information to be forwarded to a BlackBerry device.

This requirement is further described in the “Implementation Guide for Email Protective Markings for Australian Government Agencies”.

REVIEW AND AUDIT

Undertake a BlackBerry post implementation review.

Agencies implementing BlackBerry must undertake a post implementation review. This may assist in identifying policy and implementation inconsistencies and assess the mitigation controls for completeness against the Risk Management Plan (RMP), System Security Plan (SSP), Standard Operating Procedures (SOP) and the implementation of email protective marking controls.

This review must be completed within twelve months of the ‘live’ production implementation of BlackBerry.

Audit compliance with policies and standards for the use of BlackBerry devices.

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 BlackBerry devices.

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)

DSD policy on the use of BlackBerry devices

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

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

Australian Government Information Management Office, Better Practice Guidance and Checklists:
APPENDIX A – BLACKBERRY IMPLEMENTATION CRITERIA

The following table provides guidance on where BlackBerry may, should not and must not be implemented and the standards required of that implementation.

START

Are your agency's ICT facilities accredited to store, process or transmit information classified at the levels of:
• UNCLASSIFIED
• SECRET
• TOP SECRET

YES

DSD's BlackBerry policy states:
BlackBerry MUST NOT be used to:
• Store…;
• Transmit…; or
• Be ‘used with’ ICT systems processing…
… this level of classified material

THEN

Agencies MUST NOT use BlackBerry

NO

DSD's BlackBerry policy states:
BlackBerry MUST NOT be used to:
• Store… or
• Transmit…;
… this level of classified information

THEN

Agencies MUST NOT use BlackBerry to
• Store…;
• Transmit…;
… this level of classified information

AND

Are your agency's ICT facilities accredited to store, process or transmit information at the levels of:
• CABINET-IN-CONFIDENCE
• PROTECTED
• HIGHLY PROTECTED

YES

DSD's BlackBerry policy states:
BlackBerry MUST NOT be used to:
• Store…;
• Transmit…; or
• Be ‘used with’ ICT systems processing…
… this level of classified information

THEN

Agencies MUST NOT use BlackBerry

NO

Are your agency's ICT facilities accredited to store, process or transmit information classified at the levels of:
• UNCLASSIFIED
• X-IN-CONFIDENCE
• RESTRICTED

YES

DSD’s BlackBerry policy states:
BlackBerry may be used to:
• Store…;
• Transmit…; and
• Be ‘used with’ ICT systems processing…
… this level of classified material

THEN

Agency’s MUST implement this minimum set of requirements:
• Agency head must approve the requirement and use of BlackBerry
• Agencies must undertake a Threat and Risk Assessment as defined by ACS33
• BlackBerry devices must be supplied supported managed, and used in accordance an agency’s ICT policy
• Comply with the policy requirements and BES IT settings of DSD’s ‘ICT Security Policy for the use of BlackBerry’
• Implement all relevant requirements of the March 2005 (or later) release of ACS33 including but not limited to
  • Electronic Mail Protective Markings
  • Electronic Mail Security
  • Telephones and Pagers
  • Password Selection
• Implement protective markings in accordance with the
  • ‘Implementation Guide for Email Protective Markings for Australian Government Agencies’; and
  • ‘Email Protective Marking Standard for the Australian Government’

Additional mandatory requirements if ‘used with’:
• CABINET-IN-CONFIDENCE
• PROTECTED
• HIGHLY PROTECTED

ICT systems
• Satisfy all requirements as described in ACS33 for deviating from a “SHOULD NOT”
• Agency systems must meet the relevant requirements of ACS33, there must be no waivers in place
• There must be no relevant outstanding issues from system security reviews or security audit reports
• ICT systems must be certified and accredited in accordance with requirements of ACS33
• Agencies must undertake an independent (DSD or I-RAP) post implementation review of BlackBerry including Risk Mitigation Plan System Security Plan, Standard Operating Procedures, and risk mitigation controls

Note:
This figure must be read in conjunction with the:
• PSM;
• ACS33; and
• the requirements under “When BlackBerry may, should not and must not be used” in this Guide.