

## GCSB Security Notice– BlackBerry PDA Use

Dated: 30 June 2005

**Background** This notice supercedes the previous BlackBerry PDA security notice released December 2004.

The BlackBerry is a hand-held PDA that also acts as a mobile phone. It is currently being marketed by at least one local service provider.

This device is being marketed widely within New Zealand and is making its way into various Government Departments and Agencies.

Subject	See Page
General BlackBerry Issues	2
Specific Technical Issues	2
Implementing BlackBerries	2
Policy for the Use of BlackBerry Services	3

**Conventions** This document provides policy guidance at two levels:

**Mandatory policy statements** are obligatory and are formulated using the word **Must**. As a mandatory statement is to be rigorously adhered to, such statements are necessarily high-level.

**Discretionary policy statements** are used wherever such statements represent best practice and are formulated using the word **Should**. Such statements take account of instances when best practice cannot be fully applied.

Any agency that decides not to comply with a **discretionary** policy statement **must** document the reason for doing so.

**Inquiries** Enquiries relating to this notice or to preferred or evaluated products should be directed to:

<http://www.gcsb.govt.nz/> or [liaison@gcsb.govt.nz](mailto:liaison@gcsb.govt.nz)

or contact GCSB on (04) 498 7633.

## UNCLASSIFIED

### General BlackBerry Issues

BlackBerry handheld devices operate in one of two modes:

- a) Internet mode, which has no encryption and limited security options.
  - b) Enterprise mode, which encrypts email to and from the handheld. Note that this entails the agency setting up and managing its own "BlackBerry Enterprise Server (BES)".
- 

### Specific Technical Issues

Specific technical issues regarding the currently available BlackBerry models are:

1. The BlackBerry operates in an 'always on' mode and can be subject to sustained attack without the knowledge of the user.
  2. All email sent to or from a BlackBerry transits a server located in Canada via the public Internet. This risks exposure of the transmitted information to unintended parties and creates a potential vulnerability to Denial of Service attacks.
  3. The device can be used in 'peer-to-peer' mode, without any specific controls on what information is transferred and under what conditions it is transferred.
  4. Newer versions of BlackBerry come "Java-enabled" which gives users the ability to download any software onto the handset.
- 

### Implementing the BlackBerry

The introduction and use of the BlackBerry, or any other similar wireless device, by a Government agency **must** be done in accordance with that agency's IT security policy. If such policy does not exist or does not cover the use of such devices, the agency **must not** allow the introduction of these devices unless or until suitable IT security policies are in place.

The BlackBerry **must** be implemented using Enterprise mode. Under no circumstances will NZ Government Agencies allow the use of the BlackBerry operating under 'Internet' mode.

The BlackBerry Enterprise Server (BES) software implemented **must** be version 4.0 or later.

"PIN-to-PIN" communications, the "BlackBerry Web Client" and the "BlackBerry Desktop Redirector" **must not** be used to transmit classified information.

BES **must** be installed and configured in accordance with the standards set out in the document "ICT Security Policy for the use of BlackBerry by the NZ Government", available for download at [www.gcsb.govt.nz/](http://www.gcsb.govt.nz/).

---

## UNCLASSIFIED

### Policy for the Use of BlackBerry Services

At present, the following additional specific points apply to Government agencies' use of the BlackBerry:

1. Agencies **must** supply any BlackBerry devices used by staff and **must** manage the security of the devices. Any personally owned BlackBerry must **not** be used to conduct Government-related business, and **must not** be allowed to connect directly to agency IT networks.
  2. Agencies **must** have suitable security policies and associated procedures governing the use of BlackBerry services, including password policy.
  3. Agencies **must** ensure that all staff acknowledge the policies and procedures before they are allowed to use BlackBerry services. It is **recommended** that agencies provide specific training to staff in the use of the services, and in the security requirements.
  4. BlackBerry usage **must** be restricted to the Enterprise service, i.e., BlackBerry **must not** be used in Internet mode.
  5. Peer-to-peer networking on BlackBerry devices **must** be disabled.
  6. BlackBerry devices **must not** be used to store username and password information for other devices and systems.
  7. BlackBerry devices **must not** be used to store, transmit, or receive any information classified as CONFIDENTIAL, SECRET or TOP SECRET.
  8. BlackBerry devices **must not** be permitted to (physically or logically) connect to any device or system that stores or processes CONFIDENTIAL, SECRET or TOP SECRET information.
  9. BlackBerry devices **should not** be permitted to (physically or logically) connect to any device or system that stores or processes RESTRICTED or SENSITIVE information.
-