Supply, Use and Security Standard for Blackberry Devices

This document describes the requirements for a UNSW-owned Blackberry to be supplied and/or supported by ICT Services at UNSW. (Personally-owned Blackberry devices will not be supported at this time).

Authorisation: Requests for the supply and/or support of UNSW Blackberry devices must be approved by a senior staff member (Director/Head/Manager) with the appropriate financial delegation and authority before connection to the Blackberry server will be actioned.

Mandatory Password: Because of their email capacity, and the sensitive information which they may contain or be able to access, UNSW Blackberry devices must be password-protected.
- Minimum requirement is a low-level password of between 6-8 characters, which may be all alpha, all numeric, or a mixture of both;
- Default time-out will be set to 10-15 minutes and can be extended by the user;
- Note: If required by the user, device can be configured so that password is not required for making or receiving telephone calls.

WAP (Wireless Access Protocol) disabled and Internet Access only via Blackberry Server:
- Same functionality can be accessed through Intranet connection;
- Reason: The prohibitive cost of direct access to these functions and/or other Telco branded browsers.

3rd party Software Installation is Prevented unless:
- The application has been certified by Research in Motion (RIM) - if yes, then not considered 3rd party and can be freely installed.
- Reason: Untested third party applications may cause conflicts or otherwise interfere with Blackberry functionality.

Lost/Stolen Device:
A simple and effective 24/7 process has been agreed with Optus to allow reporting and disabling of lost or stolen devices. Details including UNSW Access Code will be provided to users and must be kept separate from the device.

Documentation to be Provided to User:
User will be provided with information regarding password requirements, brief instructions re. most-used functions and process to follow in case of loss or theft of device.

Disposal:
Used devices containing sensitive information must be returned to the relevant supporting ICT Group for forensic cleaning before disposal or any other change of usage.

Ethical, Legal and Responsible Use:
Users are reminded that devices must be used in accordance with UNSW Policy “Acceptable Use of UNSW ICT Resources”.

FINAL v1.0
J Beatson
March 21 2007