IT SERVICES

Mobile Device Security Guidelines

Overview

This document outlines how BCIT Policy 3502 (Information Security) applies to the use and management of both institutionally and personally owned mobile devices used to conduct institutional business. Mobile devices must be appropriately secured to prevent sensitive data from being compromised, reduce the risk of spreading viruses, and mitigate the abuse of BCIT's computing infrastructure. IT Services (ITS) reserves the right to modify this guideline as necessary. Any changes to this guideline will be communicated appropriately.

Who is affected?

These guidelines apply to all BCIT employees (administration, faculty and staff and contractors or other affiliates that **may** require BCIT email synchronization) who use corporately and/or personally owned mobile devices to access any BCIT information including, but not limited to, '@bcit.ca' email, calendar entries, address book information, and data that can be accessed via a web browser. Please note that in certain situations a mobile device may be wiped in order to ensure that BCIT's interests are protected.

What do I need to do with regard to my mobile device?

1. **Accept the settings outlined in the "Specific Security Requirements" section of this document:**
   These settings will be installed during the synchronization process and **cannot** be changed by the device owner (i.e., the synchronization server will continually re-apply the policies).

2. **Choose a strong password:**
   Security settings force a password with a minimum of 4 characters, but ITS recommends that you enhance the strength of your password by using 6 characters.

3. **Understand the concept of "device wipe":**
   BCIT Issued Devices: When a system administrator wipes a device, all data will be erased (i.e., institutional and personal data and personal applications).
   Personally Owned Devices: When a system administrator wipes a device, all institutional data will be erased. ITS will not intentionally remove personal data or personal applications. In the event that this happens, ITS will not be held accountable.
   Note: *Institutional data is that which pertains to BCIT email, calendar and contacts*

4. **Regularly back up data:**
   Consider using multiple backup mechanisms and if you travel, have a portable backup device that you can take with you.

5. **Promptly report a lost or stolen device so that it can be remotely deactivated:**
   It is also advisable to change your email password to prevent unauthorized use of the device. Device owners will be held responsible should any BCIT data be compromised as a result of the loss.

6. **Follow safe disposal practices.**

Specific Security Requirements

	BCIT Issued Device (I.e., A device required to perform BCIT business) **Use of a BCIT Issued device must adhere to BCIT Policy 3502**	**Personally Owned Device**
Security Settings		
Device timeout	The device is locked after 30 minutes.	The device is locked after 30 minutes.
Device encryption	The device content is fully encrypted.	Institutional content on the device is fully encrypted.
Password protection	Password length is set to 4 characters (minimum).	Password length is set to 4 characters (minimum).
Password attempts	The device will automatically be **wiped** after 10 failed password attempts.	Institutional content will automatically be **wiped** from the device after 10 failed password attempts.
Cost		
Device Acquisition	Client departments may absorb the initial cost for the device.	BCIT will not be responsible for costs incurred to obtain a device.
Monthly Charges	BCIT's Centralized Telecommunications Budget will absorb the **basic** monthly charges (i.e. voice, text, and data). Excessive monthly charges will be charged back to the client department.	BCIT will not reimburse for any monthly charges.
License(s)	ITS will absorb the cost for a maximum of two (2) licenses only. Client departments will absorb the cost of licenses for additional devices.	ITS may absorb the cost for a maximum of two (2) licenses per employee.
Device Replacement(s)	Client departments will absorb the cost for device replacement.	BCIT will not be responsible for costs incurred to replace a lost, stolen or damaged device.
Monitoring		
Capturing Location Information	ITS may capture Location (GPS) information about this device.	ITS will **not** capture Location (GPS) information about your device.
Capturing Messages	ITS may capture or record call log, SMS or e-mail messages.	ITS will **not** capture or record call log, SMS or e-mail messages.
Personal Application Information	ITS may capture personal application information on this device.	ITS will **not** capture personal application information on your device.
Data Wipe	ITS reserves the right to wipe all data from your device.	ITS reserves the right to wipe institutional data and applications from your device (NOT personal data).
Additional Applications		
Applications other than mail, calendar and address book	Not available at this time.	Never.

General		
Disposal	When you are ready to dispose of this device, remove all sensitive information and return the unit to the ITS Service Desk.	When you are ready to dispose of your device, advise the ITS Service Desk to have all corporate data removed automatically.
Separation from BCIT	In the event that the employment relationship with BCIT ends, this device will be returned to IT Services.	In the event that the employment relationship with BCIT ends, advise the ITS Service Desk to have all corporate data removed automatically.
Lost or Stolen Device	Report all lost or stolen BCIT Issued devices to: • The ITS Service Desk • Safety and Security department • Your department	Report all lost or stolen personally owned devices to: • The ITS Service Desk
"Unlocked" or "Rooted" Devices	These devices will not be permitted to access BCIT data.	These devices will not be permitted to access BCIT data.
Device Support	ITS will provide limited support for setup and warranty repair for these devices.	ITS will not provide support for these devices.
Personal Use	BCIT recognizes that you may need to occasionally use this device for brief personal use provided such personal use does not: • Indirectly interfere with BCIT's operation of electronic communications resources • Interfere with the staff member's employment or other obligations to BCIT (in accordance with Policy 1504: Standards of Conduct and Conflict/Interest) • Violate any laws or legal requirements	No restrictions on personal use.
Liability	This device must not be used in contravention with any law or statute (i.e. BCMVA – Chapter 318 – 214.2). BCIT will not pay fines or damages incurred through illegal activities.	The client is responsible for all usage.
MDM Agent/Profile Configuration Changes	Configuration or functional changes/enhancements made be made to the MDM Agent/profile as directed by BCIT Leadership. Notifications will be posted in the "Loop". Staff may not remove the MDM software from BCIT issued devices.	Configuration or functional changes/enhancements made be made to the MDM Agent/profile as directed by BCIT Leadership. Notifications will be posted in the "Loop". Staff may elect to remove the MDM software from their device at any time.