INFORMATION SECURITY GUIDELINE

Encrypting Mobile Devices

Introduction

1. This guideline provides directions on how to encrypt the current versions of device operating systems. For additional device-specific instructions, see the original manufacturers' User Guides.
2. This guideline has been issued by the Chief Information Officer to supplement the Encryption Requirements standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Mobile Device Encryption Directions

Operating System	Encryption Directions
IOS	IOS Devices 3GS and above have the ability to be encrypted, simply by using the password lock function on the device. Connection to UBC FASmail forces this through Exchange ActiveSync policies. See: http://www.tomsguide.com/us/how-to-encrypt-ios,news-18338.html and http://support.apple.com/kb/ht4175
Android - Ice Cream Sandwich	http://www.guidingtech.com/15825/encrypt-android-phone-ics-above/
Android – Jelly Bean	https://support.google.com/nexus/answer/2844831?hl=en&ref_topic=3416293
Blackberry Smartphone – 10.2	http://docs.blackberry.com/en/smartphone_users/deliverables/55574/als1342444399047.jsp
Blackberry Smartphone – 7.1	http://docs.blackberry.com/en/smartphone_users/deliverables/41285/1571288.jsp
Windows	For Windows based devices connecting to FASmail, encryption is enabled through Exchange ActiveSync policies. For Windows 8 Devices, see: http://windows.microsoft.com/en-ca/windows-8/using-device-encryption

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Encryption Requirements standard