Government of Alberta

GoA-owned Apple iOS mobile devices

Policy Advisory Guide

Effective Date: December 8, 2011

Version 2: February 20, 2013

Office of the Corporate CIO
Enterprise Services
Service Alberta

1. Executive Summary

This Policy Advisory Guide sets the requirements for management of GoA-owned Apple iOS mobile devices to ensure those devices, information residing on those devices, and that access to Government of Alberta (GoA) information technology (IT) systems are protected.

GoA-owned Apple iOS mobile devices are portable self-contained computing devices and include GoA-owned Apple iPhones, Apple iPads, and Apple iTouch's. The GoA has recently began deploying Apple iOS devices and this Policy Advisory Guide focuses on establishing security requirements and providing security advice for these devices in the workplace.

2. Background

The GoA has established a set of Information Management and Technology (IMT) policy instruments, including directives identified in this section. This Policy Advisory Guide provides further guidance and direction to Ministries and personnel to comply with existing directives.

2.1 Information Security Management Directive #1: Organization of Information Security

The Government's Information Security Management (ISM) Directives apply to departments. The Executive Director of the Corporate Information Security Office (Chief Information Security Officer) has authority to enforce compliance with information security policy instruments, including the ISM Directives.

2.2 Information Security Management Directive #2: Asset Management

This directive requires that information must be identified, labelled where appropriate and handled in accordance with the assigned information security classification. Therefore, controls to safeguard information on portable computing devices must be commensurate with the security sensitivity of the information.

2.3 Information Security Management Directive #3: Human Resources Security

This directive requires that all personnel be made aware of GoA security policies and requirements at commencement and on a regular basis. It also requires that personnel receive additional training that may be required based on their individual circumstances. The access rights of personnel to information technology systems must be removed upon termination, and reviewed upon change of employment.

The directive on Human Resources security also refers to the GoA's Use of Internet and E-mail Directive that outlines acceptable behaviours and use of information technology systems.

2.4 Information Security Management Directive #4: Physical and Environmental Security

This directive requires that information on media be protected from unauthorized disclosure when the media is re-assigned or disposed of.

2.5 Information Security Management Directive #5: Communications and Operations Management

This directive establishes the requirement that IT systems must be monitored and the resulting monitoring activities reviewed.

2.6 Information Security Management Directive #6: Access Control

This directive sets high level security requirements and implementation expectations in six area of Access Control:

- Business Requirements for Access Control
- User Access Management
- User Responsibilities
- Network Access Control
- Operating System Control
- Application and Information Access Control
- Mobile Computing and Teleworking

2.7 Information Security Management Directive #8: Incident Management

This directive requires that security incidents be reported and that incident management procedures be established to ensure a quick, orderly response to security incidents.

2.8 GoA-owned iOS Devices (iPads, iPhones and iTouch) Directive

This directive establishes the requirements for GoA Ministries to adopt acceptable use standards for business use of GoA-owned Apple iOS mobile devices.

2.9 Internet and E-mail Use Policy

This document outlines the minimum standards for Internet and E-mail usage for authorized GoA employees, contractors, vendors and agents. It addresses issues including acceptable usage and reminders to respect media copyrights and license agreements.

3. Scope of Policy Advisory Guide

Requirements set in this guide apply to all Ministries, including Agencies, Boards and Commissions, that receive Mobile Device Management (MDM) services from Service Alberta. Ministries that do not receive MDM Services from Service Alberta may use this Policy Advisory Guide as optional guidance.

This Policy Advisory Guide applies to GoA-owned Apple iOS mobile devices owned by the GoA and provided to personnel for use in carrying out their duties. This Policy Advisory Guide does not address use of personally owned Apple iOS Mobile Devices.

4. Definitions

Mobile Device Management (MDM) Services are provided by Service Alberta to ensure authorized users and devices can access GoA networks, IT systems and applications and ensures that authorized devices are compliant with minimum technical and security standards.

SecurNet is a Wireless Local Area Network (WLAN) managed by Service Alberta that provides authorized GoA users and devices with the same level of access as they would have through wireline network services.

GuestNet is a WLAN managed by Service Alberta that provides Internet access for GoA users and guests.

5. Mobile Device Management Requirements

5.1 Eligibility

GoA personnel may be assigned a GoA-owned Apple iOS mobile device upon approval from their Ministry. Ministries are responsible for establishing the appropriate approval level.

5.2 Provisioning

GoA-owned Apple iOS mobile devices will be provisioned by Service Alberta personnel to apply a standard base build with standard security controls described in this Guide and a set of recommended applications.

The current version of Apple iTunes will be pushed to the user’s GoA workstation. Immediately upon a new version of iTunes being made available by the vendor, the new version will be a mandatory installation for users of iTunes software.

5.3 Management Console

All GoA-owned Apple iOS mobile devices must be managed by a MDM Console operated by Service Alberta. This management console will:

- enforce compliance with minimum technical and security control standards on each device;
- provide the capability to wipe all data from a device or make the data otherwise unavailable;
- reset user authentication credentials on the device;
- identify applications residing on the device;
- add or remove applications from the device and disable the ability for users to install applications that may identified on a banned application list;
- ensure that the device has current the operating system version and current application versions.

5.4 Device Security Controls

5.4.1 Device Encryption

The GoA File and Media Encryption standard requires that where full device encryption is applied, a pre-boot authentication method must be used. Pre-boot authentication is a process where users are required to authenticate (e.g. provide a passcode) prior to any elements of the file system residing on the device are accessible. While iOS 5 and higher provide for device encryption, it does not provide for pre-boot authentication. The file system is accessible prior to users entering their personal passcode. This means it is possible for an adversary to decrypt information stored on the device through the layer of encryption provided by iOS if they have physical access to the device and possess sufficient technical skills.

Applications may apply a level of encryption with Apple's Enhanced Data Protection (EDP) function to information managed by the application, providing additional protection making it more difficult of an adversary to access unencrypted data. Apple's E-mail program applies EDP to provide additional protection to E-mail and contact information. If an application uses EDP, it will not be able to share its information with other applications.

When GoA users or program areas are selecting mobile device applications that may store or process sensitive information, EDP should be considered as one of the requirements.

The data stored on GoA-owned Apple iOS mobile devices should be encrypted using 256-bit AES encryption. Encryption and decryption are performed by a cryptographic hardware module rather than in software. This encryption algorithm meets the GoA's Cryptographic Algorithm Standard.

5.4.2 Device Passcode

GoA-owned Apple iOS mobile devices are required to use a passcode with passcode rules that meet those established in Information Security Management Directive #6: Access Control.

The minimum standards for GoA-owned Apple iOS mobile devices are:

- the device will be set to have a minimum passcode of four characters;
- the device will be set to delete all data, automatically, after ten failed authentication attempts; and
- if the device has not been used in more than fifteen minutes it will auto-lock and require the user to re-enter their passcode.

5.4.3 Digital Certificates

Digital certificates for the purpose of authenticating the end-user or GoA-owned Apple iOS mobile devices are an option that can be installed on iOS devices by an administrator or by an end-user. Information Security Management Directive #6: Access Control requires that all systems or services issuing two-factor authentication credentials must be approved by the Corporate Information Security Office (CISO).

Digital certificates may reside on GoA-owned Apple iOS mobile devices for the purpose of authenticating applications or web services to the user or device. GoA will rely on digital certificates provided natively in the iOS and my remove certificates not required and may add certificates required for services.

All digital certificates used to authenticate a GoA-owned Apple iOS mobile device or user to a GoA service must be signed by a certificate service approved by the CISO.

GoA-owned Apple iOS mobile devices must use digital certificates to authenticate to the GoA Exchange service through ActiveSync, with a unique certificate assigned to each user and issued by a certificate service approved by the CISO.

GoA-owned Apple iOS mobile devices authenticating to internal GoA WLANs such as SecureNet must authenticate with a unique certificate assigned to each device and issued by a certificate service approved by the CISO.

5.4.4 Communications Security

All GoA business information transmitted to and from a GoA-owned Apple iOS mobile device must be protected with encryption meeting GoA standards as described in the GoA's Cryptographic Algorithm Standard. Protection must be provided at the application level and must not rely on encryption provisions provided by the WLAN operator or wireless service provider.

Some mobile device applications may not choose to use encryption or all appropriate elements (e.g. some logon pages to web E-mail services). These applications should not be used for transmission or storage of information sensitive to the GoA.

5.4.5 Find My Mobile Device Service

GoA-owned Apple iOS mobile devices should be enabled with a service that will help users determine the physical location of their device in the event it has been lost or misplaced.

This service should be available only to the assigned user of the device. This service should not be accessible for administrators to track the location of the device and therefore the location of the user under normal operating procedures.

5.5 Access to GoA Domain Services

5.5.1 Messaging

Users who have been provisioned with a GoA-owned Apple iOS mobile device will be provisioned with access to their GoA Exchange E-mail through Microsoft ActiveSync which provides access to their GoA E-mail, calendar and contact information.

Users should not use the following third-party applications on their GoA-owned Apple iOS mobile device:

- messaging applications,
- calendar applications, or
- "drop-box" style application.

Third-party applications, such as these, may expose confidential information. Storing information on a third-party application can also make GoA information inaccessible or difficult to access if it becomes subject to a legal hold or a Freedom of Information and Protection of Privacy Act (FOIP) request.

5.5.2 SecureNet

Users may connect their GoA-owned Apple iOS mobile device to SecureNet for the purpose of accessing the internal GoA network. This will provide users with access to internal resources such as file and print services, access to internal web sites and access to SharePoint sites.

5.6 Apple iTunes Store and Applications

5.6.1 GoA Apple iTunes Account

During provisioning, Service Alberta will assign an Apple iTunes Account to the user for use on an assigned GoA-owned Apple iOS mobile device.

Users will be provided with their GoA Apple iTunes account password and are required to change it upon receipt and be responsible for maintaining the password security.

Users will be responsible for all transactions carried out on their GoA Apple iTunes account and must only use this account for GoA business purposes. Users will be responsible for making arrangements within their Ministry for payment of charges to the iTunes Account.

Use of GoA Apple iTunes accounts must be in accordance with the Terms of Use published by Apple which may be updated from time to time.

The management of GoA Apple iTunes accounts is the responsibility of the user.

5.6.2 Personal Apple iTunes Account(s)

Personal iTunes Accounts may be used to make purchases from the iTunes store and place purchases on GoA-owned Apple iOS mobile devices.

This provision provides users with the opportunity for to use the device for personal purposes. All personal use must be consistent with the Use of GoA Internet and E-mail Policy.

5.7 Media and Information Storage

Applications on GoA-owned Apple iOS mobile devices should be compliant with licensing agreements.

Information stored on GoA-owned Apple iOS mobile devices should be compliant with copyright laws and regulations.

5.8 User Expectations

5.8.1 User Awareness and Training

Users of GoA-owned Apple iOS mobile devices are responsible for acquiring the necessary learning and understanding of the IMT Security Standards as they apply to the safeguarding of equipment and information, including:

- ensuring unattended equipment has appropriate protection;
- ensuring the safety of sensitive information from unauthorized access;
- protecting authentication credentials;

- storing personal or sensitive information on GoA-owned Apple iOS mobile devices only if required and only for as long as required to meet the business need;
- updating operating system versions and applications regularly in order to have the most current security patches on the device; and
- familiarizing with GoA's acceptable use guidelines as outlined in the Use of GoA's Internet and E-mail Policy.

5.8.2 Reporting Security Incidents

Users should report all security incidents, including loss or theft of the GoA-owned Apple iOS mobile device, to the appropriate Ministry Service Desk.

5.8.3 Care for your GoA-owned Apple iOS mobile device

Information on your GoA-owned Apple iOS mobile device is valuable and sensitive. The security controls available for your device help protect against attackers, but are not exhaustive. Users should treat their device like a file folder of important confidential documents. Physical protection of the device is a users best defence.

Reasonable precautions should be taken by users to ensure the security of the device and the information the device contains. Such measures include, but are not limited to maintaining personal possession of the device, visual scrutiny of the device, or storing the device out of sight using a locking mechanism or in locked premises. Taking care and reasonable precautions when outside of the work environment with a GoA-owned Apple iOS mobile device, will ensure the device is protected from loss, theft or damage.

5.8.4 Backing Up your GoA-owned Apple iOS mobile device

Users should backup their GoA-owned Apple iOS mobile device to a GoA workstation and select a password to protect their backup information. Backups should contain all user data including the users GoA E-mail ID.

Users should not back up information to non-GoA workstations such as their personal and home computer or iCloud. The iCloud backup service is disabled on the device and should not be reactivated.

5.8.5 Jailbreaking

Users are should not 'jailbreak' or 'unlock' a GoA-owned Apple iOS mobile device or install software except using methods approved by the manufacturer or wireless service provider. Jailbreaking or unlocking a device can allow others to circumvent passcodes that have been set and compromise the security of the device.

5.8.6 Using Wireless LANs

Users may connect their GoA-owned Apple iOS mobile device to SecureNet provided the device has been configured with a unique certificate for the purpose of authenticating to SecureNet.

When on GoA sites, Users are encouraged to use SecureNet for their Internet access. If SecureNet is not available Users are encouraged to connect to GuestNet.

Users may connect their GoA-owned Apple iOS mobile device to other wireless LANs as required but Users are encourage to consider the stability of the wireless LAN network prior to connecting the device.

5.9 Decommission or Re-Assignment

Upon decommission or re-assignment of the user the GoA-owned Apple iOS mobile device must be wiped making data residing on the device unavailable prior to decommission or re-assignment.

6. Contact List

For questions about this Policy Advisory Guide, please contact:

Office of the Corporate CIO
CIOC.Secretariat@gov.ab.ca

7. Revision History

Date	Version	Description
December 8, 2011	1	New publication issued by OCCIO
February 14, 2013	2	Amended to reflect practice regarding backups