GoA-owned Apple iOS

Mobile Devices

(iPads, iPhones and iTouch)

GoA IMT Directive

IMT Directive	
Security Classification:	**Unrestricted**
Status:	**Final**
Approved by:	**Kate Rozmahel, Corporate CIO**
Effective Date:	**2011-12-08**
Scheduled Review:	**2012-12-08**
Last Review:	**2011-12-08**

Status: Active ☒ **Inactive** □

GoA-owned Apple iOS Mobile Devices

GoA IMT Directive

1. Summary Description

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

2. Purpose

The purpose of this directive is to set direction and requirements which must be followed by GoA employees, contractors and agents who have been provided a GoA E-mail account and have a business need to connect to GoA information and applications (including GoA E-mail, GoA Address Book and work calendars) through the use of a GoA-owned Apple iOS mobile device. The introduction of mobile devices in the workplace is in-line with the established Information Management Technology (IMT) strategy. Specifically, GoA-owned Apple iOS mobile devices will be able to provide services that will enhance employee productivity such as portable document reading and easily accessible Internet and e-mail services.

3. Scope

This directive applies to all GoA-owned Apple iOS mobile devices.

4. Directive Statements

The GoA supports the use of GoA-owned Apple iOS mobile devices to improve service delivery, increase operational effectiveness and minimize costs. This directive identifies the controls which all Ministries must follow to create GoA-wide information management best practices that help all GoA employees leverage a common technology infrastructure.

Personal use of a GoA-owned Apple iOS mobile device, beyond a business need, can compromise data confidentiality and privacy protection. In accepting the terms of this directive, users of mobile devices are subject to all applicable GoA policies, directives, standards and procedures.

4.1 Procurement

4.1.1 Employees who have a legitimate business need for a GoA-owned Apple iOS mobile device must receive approval from their Ministry. Ministries are responsible for establishing the appropriate approval level.

4.1.2 Services for GoA-owned Apple iOS mobile devices are defined within the GoA Service Catalogue.

4.2 Risk Mitigation

4.2.1 Mandatory Passcodes

4.2.1.1 All GoA-owned Apple iOS mobile devices must have a secure logon process including an employee-specific password. Users must follow good security practices in the selection and use of passwords.

4.2.1.2 Passwords must be a minimum of four characters in length and must remain on the device.

4.2.1.3 The GoA-owned Apple iOS mobile device must be set to automatically wipe the contents of the device if there are ten consecutive failed attempts at the password.

4.2.2 User Responsibilities

4.2.2.1 Users of GoA-owned Apple iOS mobile devices are responsible for acquiring the necessary learning and understanding for the IMT security standards, applying 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 business needs;
- updating operating system versions and applications regularly in order to have the most current security patches on the device;
- familiarizing with GoA's acceptable use guidelines as outlined in the *Use of Government of Alberta's Internet and E-mail Directive*;
- reporting lost or stolen GoA-owned Apple iOS mobile devices immediately to the user's Ministry Service Desk or to the point of contact designated by the user's Ministry.

4.2.3 Device Modifications

4.2.3.1 Users must not 'jailbreak' or 'unlock' a GoA-owned Apple iOS mobile device. Users are required to install software using methods approved by the manufacturer or wireless service provider.

4.2.4 Remote Wipe

4.2.4.1 The GoA reserves the right to wipe all contents of a GoA-owned Apple iOS mobile device when there is deemed to be a security concern. The primary use of this feature is when a GoA-owned Apple iOS mobile device is either lost or stolen.

4.3 Configuration

4.3.1 iTunes Accounts

4.3.1.1 GoA-owned Apple iOS mobile devices will be assigned a GoA Apple iTunes Account during set up.

4.3.1.2 The management of GoA Apple iTunes Accounts is the responsibility of the user.

4.3.1.3 GoA Apple iTunes Accounts must be used for all purchases and downloads of GoA-owned mobile device business applications.

4.3.1.4 Personal iTunes Accounts may be used for transferring non-business related applications to the GoA-owned Apple iOS mobile device provided these applications do not compromise copyright laws and are deemed appropriate for GoA equipment.

4.3.1.5 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.

4.3.2 Applications

4.3.2.1 A list of recommended applications will be maintained in the *iPad Recommended Apps Standard* document.

4.3.2.2 All user application purchases must follow Ministry-specific processes for approval and reimbursement.

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

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

4.3.3 Device Configuration

4.3.3.1 All GoA-owned Apple iOS mobile devices being used on the GoA Domain must have a Mobile Device Management (MDM) program installed on the device. The user is not permitted to uninstall the MDM program.

4.3.3.2 Configuration of GoA-owned Apple iOS mobile devices must be in line with the *iOS Configuration Standard*.

4.3.4 Synchronization, Patching and Back-Up

4.3.4.1 Users of GoA-owned Apple iOS mobile devices must have Apple iTunes loaded on their GoA workstation. GoA-owned Apple iOS mobile devices must only be backed-up to a GoA Apple iTunes Account on a GoA-owned workstation.

5. Implementation

Ministry CIOs will define the appropriate and specific uses of GoA-owned Apple iOS mobile devices in their Ministry. Details outlining the implementation of the policy statements listed above can be found in the *GoA-owned Apple iOS Mobile Devices Policy Advisory Guide*.

6. Communication

This directive will be communicated directly to Ministry CIOs and published on the IMT Standards website for reference. Ministry CIOs will be responsible for communicating the directive within their respective Ministries.

7. Relevant Legal Instruments

FOIP – *Freedom of Information and Protection of Privacy Act*
Records Management – *Records Management Regulation, Government Organization Act*
Electronic Transactions – Electronic Transaction Act
Records Retention and Disposal - Alberta Evidence Act

8. Compliance

Ministry Deputy Heads are accountable and Ministry CIO's are responsible for ensuring compliance with this directive and for taking appropriate action to remediate non-compliance.

9. Exceptions

Exceptions to this directive will be handled through the IMT Policy exception process.

10. Related Documents

- Information Security Management Directive #1: Organization of Information Security
- Information Security Management Directive #2: Asset Management
- Information Security Management Directive #3: Human Resources Security
- Information Security Management Directive #4: Physical and Environmental Security
- Information Security Management Directive #5: Communications and Operations Management
- Information Security Management Directive #6: Access Control
- Information Security Management Directive #8: Incident Management
- GoA Internet and E-mail Directive
- Electronic Transactions Act

11. Authority

The overarching authority for the development of IMT Policy is the *GoA Information Management and Technology Policy Definition* document dated January 14, 2009, and approved by the Minister of Service Alberta.

The Corporate Chief Information Officer sets this directive, under the authority of the Minister of Service Alberta, to establish requirements under strategic theme #4 (Enabling the productivity of GoA employees) of the *GoA Information Management and Technology (IMT) Strategic Plan*.

Original signed by________________________________
Kate Rozmahel, Corporate Chief Information Officer

January 11, 2012________________________________
Date

12. Owner

Service Alberta, Enterprise Services

14. Contact

Office of the Corporate Chief Information Officer
Service Alberta
Kate.Rozmahel@gov.ab.ca

Category: IMT Hardware			
Key Words:			
Amendment History			
Revision	**Date**	**Amendments**	**Amended by**
Version 1.0	**2011-12-08**		