Office of the Chief Information Officer, Ministry of Technology, Innovation and Citizens' Services

Management of Mobile Devices Released October 2016

http://www.bcauditor.com/pubs

Initial PAC Meeting- 23 November 2016

1st Action Plan Update 23 November 2016

Rec. #	OAG Recommendations[1]	Action Planned	Target Date	Assessment of Progress by Entity[2]	Action Taken[3]
1.	We recommend that the Office of the Chief Information Officer establish requirements to document: - assessments of the risks associated with new mobile device features and services - approvals of risk mitigation plans - acceptance of residual risks	In line with standards in Chapter 12 of the Core Policy Manual, the OCIO will perform risk assessments of each mobile device and operating system.	March 31, 2017	Partially implemented	The OCIO is developing the Mobile Device Security Standard and is developing the next version of the Information Security Policy (v4.0). The OCIO also recently conducted a LEAN project to streamline risk assessments and make the process commonly understood.

[1] This should include all the recommendations listed in the Office of the Auditor General (OAG) report unless previously assessed as fully or substantially implemented. (i.e. only outstanding recommendations need to be reported).

[2] The Select Standing Committee on Public Accounts (PAC) will request an update (i.e Assessment of Progress and Actions Taken column completed) on a yearly basis from the audited organization until all recommendations are fully implemented or otherwise addressed to the satisfaction of the PAC. After the first action plan update only outstanding recommendations (i.e. those not fully or substantially implemented) need to be reported.

[3] This action plan and their subsequent updates have not been audited by the OAG. However, at a future date that Office may undertake work to determine whether the entity has fairly and accurately represented their progress in addressing the recommendations. The results of that work will be reported in a separate report prepared by the OAG.

Please provide your email response to:

Attention: Bruce Ralston, Chair of the Select Standing Committee on Public Accounts

Email: Kate.Ryan-Lloyd@leg.bc.ca, Deputy Clerk and Clerk of Committees

Cc email to: the Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca

Cc email to: the Office of the Auditor General of British Columbia lhatt@bcauditor.com

Rec. #	OAG Recommendations[1]	Action Planned	Target Date	Assessment of Progress by Entity[2]	Action Taken[3]
2.	We recommend the Office of the Chief Information Officer update the policy framework to clearly identify applicability to mobile devices.	In line with standards in Chapter 12 of the Core Policy Manual, the OCIO will reflect the necessary updates in the Mobile Device Security Standard.	March 31, 2017	Partially implemented	The OCIO is developing the Mobile Device Security Standard and is developing the next version of the Information Security Policy (v4.0).
3.	We recommend the Office of the Chief Information Officer provide support to help ministries develop a solution to maintain a detailed inventory of all mobile devices (with or without data plans), including key information such as: assignee, manufacturer, model, operating system level and relevant dates.	The OCIO launched the Mobile Device Management Service (MDMS) that will fulfill this recommendation.	December 31, 2016	Partially implemented	The OCIO continues to onboard mobile devices onto the Mobile Device Management Service (MDMS). The number of devices left to onboard is approximately 8,000.
4.	We recommend the Office of the Chief Information Officer ensure all key initial security settings are applied before a mobile device goes into service.	The OCIO launched the Mobile Device Management Service (MDMS) that will fulfill this recommendation.	December 31, 2016	Partially implemented	The OCIO continues to onboard mobile devices onto the Mobile Device Management Service (MDMS). The number of devices left to onboard is approximately 8,000.
5.	We recommend that the Office of the Chief Information Officer establish in policy a maximum inactivity-until-locked time based on an assessment of the risks to the security of sensitive government information, and enforce this policy through technical means.	Maximum inactivity-until-locked time has been changed to reflect 15 minutes as stated in ISP v3.0 and will be enforced via Mobile Device Management Service (MDMS).	December 31, 2016	Partially implemented	The OCIO continues to onboard mobile devices onto the Mobile Device Management Service (MDMS). The number of devices left to onboard is approximately 8,000.

Please provide your email response to:
Attention: Bruce Ralston, Chair of the Select Standing Committee on Public Accounts
Email: Kate.Ryan-Lloyd@leg.bc.ca, Deputy Clerk and Clerk of Committees
Cc email to: the Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia lhatt@bcauditor.com

Rec. #	OAG Recommendations[1]	Action Planned	Target Date	Assessment of Progress by Entity[2]	Action Taken[3]
6.	We recommend that the Office of the Chief Information Officer replace the existing mobile device management tool with one capable of: - installing and maintaining anti-malware software - preventing high-risk devices from connecting - monitoring and logging mobile device security incidents	The OCIO has launched the Mobile Device Management Service (MDMS) that will fulfill this recommendation.	December 31, 2016	Partially implemented	The OCIO continues to onboard mobile devices onto the Mobile Device Management Service (MDMS). The number of devices left to onboard is approximately 8,000.
7.	We recommend that Office of the Chief Information Officer analyse lost and stolen device reports for potential enhancements to security awareness programs.	OCIO Security Awareness team will review lost and stolen device reports monthly for opportunities to improve security awareness regarding mobile devices.	March 31, 2017	Partially implemented	The OCIO has begun to examine lost and stolen device reports for opportunities to improve security awareness.

Prepared by: Office of the Chief Information Officer, Ministry of Technology, Innovation and Citizens' Services

* Under the Core Policy and Procedures Manual (CPPM), the Government CIO has responsibility for IM/IT policies and standards across ministries, but not Crown Corporations, Health Authorities, School Districts, Universities and Colleges. CPPM is being amended to reflect the transfer of Information Management responsibilities to the newly created Chief Records Officer.

Please provide your email response to:
Attention: Bruce Ralston, Chair of the Select Standing Committee on Public Accounts
Email: Kate.Ryan-Lloyd@leg.bc.ca, Deputy Clerk and Clerk of Committees
Cc email to: the Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia lhatt@bcauditor.com