Action Plan and Progress Assessment (APPA) for the implementation of audit recommendations from the OAG- Prepared for the Select Standing Committee of Public Accounts

Attention: Mike Bernier, Chair and Rick Glumac, Deputy Chair of the Select Standing Committee on Public Accounts

[Audit of the B.C. Government's Internal Directory Account Management] Released [08/13/19]

http://www.bcauditor.com/pubs

PAC Meeting Plan[1]	**[01/11/19]**	**Prepared by: Gary Perkins, Office of the Chief Information Officer**	**Reviewed by: Jill Kot, Deputy Minister**
1st APPA Update	**[01/12/20]**	**Prepared by: Gary Perkins, Office of the Chief Information Officer**	**Reviewed by: Alex MacLennan, Assistant Deputy Minister**
2nd APPA Update	**[DD/MM/YY]**	**Prepared by: [Name], [Organization Name]**	**Reviewed by: [Name of Deputy Minister or Assistant Deputy Minister]**

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
1. Yes	We recommend that the Office of the Chief Information Officer work with ministries to: a. apply clear roles and responsibilities as defined for the IDIR user accounts provisioning processes b. reconcile the Information Security Policy and Standards as they relate to the maintenance of a central record of access rights for IDIR users	Review roles and responsibilities for the IDIR user accounts provisioning process with each ministry and provide training if necessary. Review the Information Security Policy and Standards to ensure it is current and update if necessary. Implement the Information Security Policy and Standards as it relates to the maintenance of records of access rights for IDIR users. **Target Date:** 31/12/2020	OCIO have reviewed the roles and responsibiliites for IDIR user accounts provisioning process with Ministries and worked with each to establish processes. OCIO reviewed the Information Security Policy and Standards and updated to reflect present practices. This item is complete.

[1] The audited organization will be required to present their initial action plan at this meeting (i.e. First three columns completed for each OAG recommendation included in the audit report)

[2] For each recommendation, the audited organization should state whether or not they have accepted the recommendation and plan to implement it fully by typing either "Yes" or "No" under the number of the recommendation.

[3] Target date is the date that audited organization expects to have "fully or substantially implemented" the recommendation. If several actions are planned to implement one recommendation, indicate target dates for each if they are different.

[4]The Select Standing Committee on Public Accounts (PAC) will request that the audited organization provide a yearly update (i.e completed "Assessment of Progress and Actions Taken" column) until all recommendations are fully implemented or otherwise addressed to the satisfaction of the PAC. This is for the APPA update.

[5] This action plan and the 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 implemented the recommendations. The results of that work will be reported in a separate report prepared by the OAG.

Please provide your email response to:

Email: 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 actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
2. Yes	We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they: a. develop and document ministry specific procedures for setting up IDIR user accounts for new employees and contractors b. establish a formal training and education program for those who are involved in the IDIR service c. implement a process ensuring only properly authorized IDIR user accounts requests are acted upon	Develop and document ministry specific procedures for setting up IDIR user accounts for new employees and contractors. Establish a formal training and education program for those who are involved in the IDIR service. Implement a process for ensuring only properly authorized user accounts requests are acted upon. **Target Date:** 31/03/2020	OCIO worked with Ministries to develop and document procedures for setting up IDIR user accounts. OCIO established a formal training and education program for those involved in the IDIR Service. All ministries developed processes for ensuring only authorized requests are acted upon. This item is complete.
3. Yes	We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they develop and document ministry-specific procedures for establishing access permissions for authorized IDIR user accounts to access applications.	Develop and document ministry-specific procedures for establishing access permissions for authorized IDIR user accounts to access applications. **Target Date:** 31/12/2019	All ministries developed and documented procedures for establishing access permissions. This item is complete.
4. Yes	We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they develop and document ministry-specific procedures for the removal of IDIR user accounts of terminated employees and contractors.	Develop and document ministry-specific procedures for the removal of IDIR user accounts of terminated employees and contractors. **Target Date:** 31/12/2019	All ministries developed and documented procedures for removal of IDIR accounts. This item is complete.
5. Yes	We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they establish processes for reviewing privileged IDIR account users' access rights and monitoring their activities to ensure they are appropriate and authorized.	Establish processes for reviewing privileged IDIR account users' access rights and monitoring their activities to ensure they are appropriate and authorized. **Target Date:** 31/03/2020	All ministries developed and documented processes for reviewing privileged IDIR accounts access rights and monitoring activities. This item is complete.

Please provide your email response to:
Email: 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 actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
6. Yes	We recommend that the Office of the Chief Information Officer work together with the BC Public Service Agency to compare the IDIR user employee profiles with the government employee payroll database and where discrepancies are identified make the appropriate corrections.	Ensure there is an Information Sharing Agreement with the BC Public Service Agency. Develop a process to update IDIR user employee profiles from the employee payroll database. **Target Date:** 31/03/2020	OCIO implemented a process to update IDIR employee profiles from the employee payroll database on a regular basis. This item is complete.
7. Yes	We recommend that the Office of the Chief Information Officer work with ministries to expand the scope of the monthly review of IDIR user accounts to include checking for non-expiring password settings and IDIR accounts that have remained active, even after employees and contractors no longer work for government.	Expand the scope of the monthly review of IDIR user accounts to include checking for non-expiring password settings and IDIR accounts that have remained active. **Target Date:** 31/12/2020	The scope of the monthly review of IDIR user accounts was expanded to include checking for non-expiring password settings and IDIR accounts that have remained active. This item is complete.

Please provide your email response to:
Email: 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 actionplans@bcauditor.com