Chapter 14
Summary of Implemented Recommendations

1.0 Main Points

This chapter lists agencies that implemented recommendations from previous annual integrated audits or IT audit work with no other significant findings included as a chapter in this Report.

2.0 Summary of Implemented Recommendations

The table below sets out, by agency, the recommendations as well as highlights key actions taken by the agency to implement its recommendations.

Past Recommendation (Initial PAS Report, Date of Agreement of PAC)[A]	Key Actions Taken During 2020–21 to Implement Recommendation
Corrections, Policing and Public Safety	
We recommended the Ministry of Corrections, Policing and Public Safety follow its established procedures for removing unneeded user access to its computer systems and data.(*2015 Report – Volume 2*, p. 74, Recommendation 2; Public Accounts Committee agreement January 11, 2017)	For the 2020–21 fiscal year, we found for two of 10 users tested, staff did not ask for removal of user IT access on a timely basis (both removed within nine business days after the users no longer worked at the Ministry). For these two users, we confirmed timely access removal to all significant IT applications (e.g., MIDAS, Criminal Justice Information Management System) and their accounts were not accessed after the user ceased employment with the Ministry. In addition, we found two users who did not have access to the Criminal Justice Information Management System removed on a timely basis (between 17–85 business days after the users no longer worked at the Ministry). For these two users, we confirmed access to the IT network was removed within 22 business days. Without IT network access, the users could not access the System. Furthermore, we confirmed their accounts were not inappropriately accessed after the users ceased employment with the Ministry. In June 2021, the Ministry developed a *Timely Removal from Information Technology Systems* policy, which outlines circumstances when the Ministry expects a user's access to be removed and defines what is considered timely removal (i.e., within three business days). We acknowledge the Ministry is continuing to reduce the number and severity of instances of late user-access removal. The Ministry continues to work with the Public Service Commission to receive notifications when staff leave the Ministry. For the current year, deviations found are not considered to be significant and so we consider the intent of recommendation implemented.

Past Recommendation (Initial PAS Report, Date of Agreement of PAC)[A]	Key Actions Taken During 2020–21 to Implement Recommendation
Justice and Attorney General	
We recommended the Ministry of Justice and Attorney General follow its established procedures for removing unneeded user access to its computer systems and data. (*2015 Report – Volume 2*, p. 74, Recommendation 2; Public Accounts Committee agreement January 11, 2017)	For the 2020–21 fiscal year, we found for two of 11 users tested, staff did not ask for removal of user IT access on a timely basis (between 11 and 112 business days after the users no longer worked at the Ministry). For these two users, we confirmed timely access removal to all significant IT applications (e.g., MIDAS, Criminal Justice Information Management System) and their accounts were not inappropriately accessed after the users ceased employment with the Ministry. In addition, we found for three of 15 users tested staff did not ask for access removal to the Criminal Justice Information Management System on a timely basis (between five and 75 business days after the users no longer worked at the Ministry). For these three users, we confirmed timely access removal to the IT network for two staff and within 15 business days for the third staff. Without IT network access, the users could not access the System. Furthermore, we confirmed their accounts were not inappropriately accessed after the users ceased employment with the Ministry. In June 2021, the Ministry developed a *Timely Removal from Information Technology Systems* policy, which outlines circumstances when the Ministry expects a user's access to be removed and defines what is considered timely removal (i.e., within three business days). We acknowledge the Ministry is continuing to reduce the number and severity of instances of late user access removal. The Ministry continues to work with the Public Service Commission to receive notifications when staff leave the Ministry. For the current year, deviations found are not considered to be significant and so we consider the intent of recommendation implemented.
Justice and Attorney General—Victims' Fund	
We recommended the Ministry of Justice and Attorney General—Victims' Fund prepare key supporting documents at the same time as it prepares its financial statements. (*2019 Report – Volume 2*; p. 58, Recommendation 1, Public Accounts Committee has not yet considered this recommendation as of October 29, 2021)	The Ministry took steps to prepare key supporting documents for the Fund's 2020–21 financial statements for management's timely review. The Ministry provided our Office with key documents to support the Fund's draft 2020–21 financial statements within the agreed upon timelines. There were no material errors identified delaying our audit work timing.
Northlands College	
We recommended Northlands College follow its established procedures for removing unneeded user access to its computer systems and data. (*2020 Report – Volume 2*; p. 68, Recommendation 1; Public Accounts Committee has not yet considered this recommendation as of October 29, 2021)	In 2020–21, Northlands College updated its employee termination process to notify IT staff of an employee's last work day to ensure prompt removal of user access. The appointed auditor found that the College removed unneeded access promptly.

Past Recommendation (Initial PAS Report, Date of Agreement of PAC)[A]	Key Actions Taken During 2020–21 to Implement Recommendation
Saskatchewan Liquor and Gaming Authority	
We recommended the Saskatchewan Liquor and Gaming Authority establish a written agreement with Saskatchewan Indian Gaming Authority (SIGA) indicating when it will receive the audit report on controls for the SIGA Casino Management System. (*2019 Report – Volume 2*, p. 94, Recommendation 1; Public Accounts Committee agreement February 8, 2021)	In July 2019, the Authority signed an agreement with Saskatchewan Indian Gaming Authority (SIGA) about receiving an audit report on the effectiveness of controls for the SIGA Casino Management System within 40 days following March 31 (i.e., by May 10). SIGA provided the Authority with a draft audit report on April 30, 2021, and the final audit report on May 27, 2021. There were no significant changes to the audit report between April 30 and May 27, 2021.
Saskatchewan Indian Gaming Authority	
We recommended the Saskatchewan Indian and Gaming Authority (SIGA) monitor activities of its service provider that manages its Casino Management System. (*2019 Report – Volume 2*, p. 94, Recommendation 2; Public Accounts Committee agreement February 8, 2021)	During the year, SIGA implemented processes to monitor activities of its service provider. It reviews and approves changes made by its service provider. SIGA also monitors access to the Casino Management System to ensure access is authorized and appropriate.
Saskatchewan Polytechnic	
We recommended Saskatchewan Polytechnic establish a policy to guide compensating for losses of its employees. (*2019 Report – Volume 2*, p. 99, Recommendation 1; Public Accounts Committee has not yet considered this recommendation as of October 29, 2021)	During 2021, Saskatchewan Polytechnic established a policy and procedures to guide compensating losses of all members of its community including employees, students, volunteers, Board members and the general public.
Western Development Museum	
We recommended the Western Development Museum consistently document the approval of purchase orders before it purchases the related goods or services. (*2020 Report – Volume 2*, p. 103, Recommendation 1; Public Accounts Committee has not yet considered this recommendation as of October 29, 2021)	Management updated the purchase-order policy for clarity and reiterated to its managers the process to approve purchase orders. Management at head office reviewed each purchase order and invoice during the year to verify that the purchase order was approved before making a purchase. During our testing of purchases, we did not identify any purchases in our sample where an employee made a purchase before obtaining an approved purchase order. For all these purchases, management appropriately approved the purchase order before or on the same day staff ordered the goods or services.

[A] PAS: Provincial Auditor of Saskatchewan
PAC: Standing Committee on Public Accounts