Chapter 17, Saskatchewan Gaming Corporation – Preventing Cyberattacks, Provincial Auditor 2021 Report – Volume 2

Recommendation Indicate New/Outstanding	Page	Current Status (Implemented, Partially Implemented, Not Implemented)	Actions Taken to Implement since PA Report	Planned Actions for Implementation	Timeline for Implementation
New - We recommend Saskatchewan Gaming Corporation maintain well defined action plans clearly addressing all significant risks of cyberattacks that may affect IT systems and data used to support and deliver casino games.	134	Implemented	• IT Cyber Security Risk Register finalized following the NIST Cybersecurity Framework (CSF). • SaskGaming has developed a Risk Assessment procedure to document, track and sign off on risks associated with technology initiatives.	N/A	N/A
New - We recommend Saskatchewan Gaming Corporation adequately configure its network, servers, and workstations to better protect them from security threats and vulnerabilities.	136	Partially Implemented	• Required adjustments to wireless access controls documented and implemented in early Jan. 2022. • Successful rollout of remote access solution completed in Feb. 2022. • Enhanced endpoint protection countermeasures deployed to 100% of the client fleet. • Encryption mechanisms have been deployed to all clients in the environment. • SaskGaming continues to leverage external provider for Incident Response (IR) and proactive services where needed. • SaskGaming continues to actively participate in inter-government collaboration efforts focusing on this specific item to determine long-term strategy.	• SaskGaming will further deploy network segmentation to limit the exposure points of unauthenticated and unauthorized access.	Q4 2022-2023

New - We recommend Saskatchewan Gaming Corporation include all privileged-user groups in its quarterly user access reviews.	137	Implemented	• SaskGaming has created reports to identify all accounts with privileged access. Standard Operating Procedures (SOPs) in place to review these accounts on a periodic basis.	N/A	N/A
New - We recommend Saskatchewan Gaming Corporation update all user account passwords as often as required by its password policy.	137	Implemented	• SaskGaming has created reports to identify all accounts with non-expiring passwords. Standard Operating Procedures (SOPs) in place to review these accounts on a periodic basis.	N/A	N/A
New - We recommend Saskatchewan Gaming Corporation implement further use of multifactor authentication to reduce, to an acceptable level, the risk of unauthorized access to IT systems and data.	137	Partially Implemented	• SaskGaming has completed rollouts of multi-factor authentication mechanisms on key business applications for corporate staff in July 2022. Rollout to operational staff currently in progress.	• SaskGaming will rollout multi-factor authentication mechanisms to key personnel and business systems, reducing the risk of exposed business and customer data.	Q4 2022-2023
New - We recommend Saskatchewan Gaming Corporation update its IT security assessment plan to reflect changes in its practice and to align with IT industry standards.	140	Implemented	• SaskGaming has developed policies specific to vulnerability management and assessment procedures (including timelines for assessments) to align with industry best practices. • SaskGaming has extended the scope of vulnerability assessment testing tools to ensure additional assets are reviewed on a consistent basis and have aligned operating procedures to the timelines indicated in policy.	N/A	N/A

New - We recommend Saskatchewan Gaming Corporation analyze information from security assessments and attempted cyberattacks to better identify and address cybersecurity risks.	140	Implemented	• SaskGaming has completed scenario specific runbooks/playbooks to ensure proper steps are taken in the event of a specific incident or breach. • SaskGaming has created a cyber incident response policy which outlines the key roles, responsibilities and tasks of contributors. • SaskGaming has incorporated lessons learned as part of post incident analysis to identify risks and opportunities for improvement.	N/A	N/A