AUDIT REPORT

Player Information Privacy

Audit Services

FY2023

bclc

Table of Contents

Date: March 27, 2023

From: Rao Wandawasi, Director, Audit Services

To: Mark Goldberg, Chief Information Officer & V.P, Business Technology

Marie-Noëlle Savoie, Chief Compliance Officer & V.P, Legal, Compliance, Security

RE: PLAYER INFORMATION PRIVACY

I. Introduction

In accordance with the Audit Plan presented to the Audit Committee, Audit Services conducted an audit of BCLC's Player Information Privacy environment. The audit report is presented for information and discussion. For the issues identified in the report, an "agreed upon action plan" is developed in collaboration with management. These action plans are tracked by the Audit Services team for timely implementation. Any delays or non-execution of the action plan is compiled and presented to the Audit Committee.

II. Objective and Scope of Audit

The objective of this audit was to validate aspects of BCLC's Player Personal Information (PPI) landscape, as well as the corresponding technology services used to enable the collection, usage, storage, and destruction of PPI. Additionally, the effectiveness and efficiency of the control environment was reviewed.

The scope of this engagement includes PPI at BCLC, and not at Casino Service Providers and third-party vendors. The cyber component of this engagement focused on three systems:
s 15(1)(l)

Details of the systems are listed in Appendix 1.

Areas subject to Audit Services review include, but were not limited to, the following:

- Control Testing: Determine the effectiveness and consistent use of controls specific to PPI and privacy.
- Access & Escalation Process: Verify the overall privileged system access process regarding PPI and privacy; additionally, determine staff knowledge and reasonableness of the incident escalation process.
- Privacy Framework: Validate PPI collection, storage, use, and disposal; additionally, map system controls and touch points.
- Regulations: List all pertinent regulatory requirements pertaining to PPI and privacy, and test BCLC's overall compliance.
- Training: Test the enterprise's training effectiveness, frequency, and completeness with regards to PPI and privacy; additionally, determine the reasonableness of training compared to the level of access.
- Futureproofing: Identify BCLC's nimbleness in adapting to changing expectations and environment; assess the enterprise's future vision and the preparedness, ability, resolve, and action undertaken today to deliver on this vision.

III. Importance of Player Information Privacy

For BCLC players to willingly share personal information, they must trust that their PPI will be handled with sufficient diligence and protected with care. Key reasons to prioritize player information privacy are as follows:

- Reputation & Trust: As a customer-facing organization that operates Casino, Lottery, and PlayNow gaming platforms, BCLC collects and stores massive quantities of PPI from across British Columbia (BC), Manitoba, and Saskatchewan. From a trust and reputational perspective, it is imperative that BCLC responds appropriately to protect PPI.

> Privacy is not something that a player is merely entitled to; it's an absolute prerequisite.

- Operational Requirements: If a player's privacy is compromised and they suffer consequences, it is likely that they may not return to our various gaming channels in the future.
- Regulation: BCLC must comply with the provisions of BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) when handling and storing PPI or face monetary and/or legal penalties.
- Social Purpose: From a social purpose perspective, information privacy is a corporate responsibility for an organization that maintains PPI. This goes beyond the applicability of privacy laws and regulations; this highlights the very core of the organization's culture, ethics, and values.

Given the importance of player information privacy, coupled with the magnitude of PPI being collected in modern business practices, it can be challenging for organizations to stay on top of all policy requirements as well as best practices. Periodic reviews and regular updates to underlying tools and technology will aid the overall process tremendously.

IV. Details of Key Issues

s 13, s 15(1)

s 13, s 15(1)

s 13, s 15(1)

s 13, s 15(1)

s 13, s 15(1)

2. Streamlining of Information Security Practices

Observations:

A mature information security program typically includes the following:

- Defined set of policies (rules to adhere by)
- Processes and procedures to aid in actioning the policies, which are driven by standards and guidelines
- Responsibility assigned to a role within the organization for actioning on PPI
- Accountability assigned at the management level for the effective functioning of the overall program
- Structured process to purge old information per established guidelines, thereby ensuring nothing is retained beyond policy-specified period

Audit Services reviewed the information security program (and PPI) and noted the following:

A. <u>Policies, Standards, Processes, and Guidelines</u>

BCLC has created the following enterprise-level policies and procedures, specific to information security and PPI:

- Privacy Management Policy
- Privacy Breach Policy
- Enterprise Incident Response Plan
- Records Management Policy
- Records Destruction Procedures

In reviewing the above policies and procedures, Audit Services noted the following:

s 13, s 15(1)

- Reporting for Privacy Breach: s 13, s 15(1)

> If you want employees to do something, make it easy for them.

- Practices Noted Across Systems: The following practices were noted across the three systems in scope for this audit:

System / Application	Description	Issues Noted
s 15(1)(l)	Information Attributes: *Free-text postings* Information synonym to "BCLC Wikipedia" for technical and operational intelligence A total of 1,199 users including contractors and third-party vendors	s 15(1)
s 15(1)(l)	Information Attributes: *Telephone recordings* System decommissioning in April 2023 PPI will be extracted from s 15(1)(l) before decommission and migrated to BCLC SharePoint	s 15(1)
s 15(1)(l)	Information Attributes: *Completed marketing campaigns* This information is considered transitory and hence disposed when no longer required Retaining PPI creates legal and security risks	s 15(1)

B. Clarity in Roles, Responsibilities, and Accountabilities

A key information security activity is to define roles, responsibilities, and accountabilities for employees with access to PPI.

> Data Privacy will be one of the most important issues of this decade.
> - *Forbes*

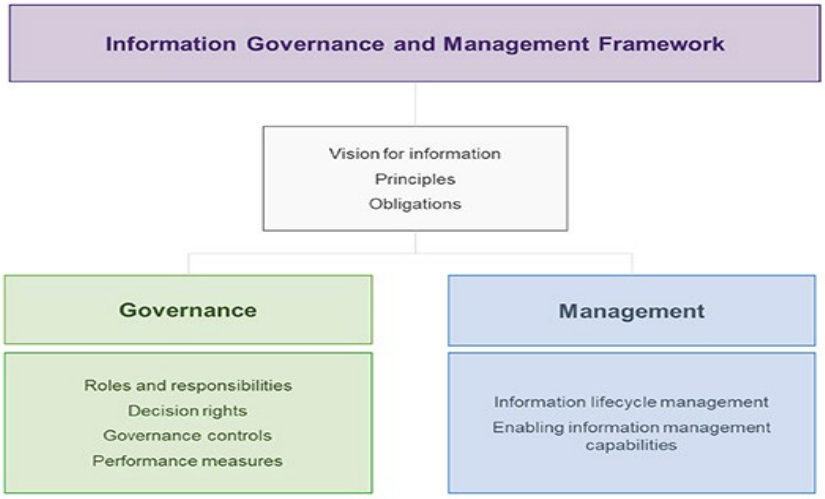

Figure 1 - Information Governance and Management Framework document structure

Source: *University of Queensland Information Governance and Management Framework*

Specific to roles, responsibilities, and accountabilities within BCLC's information management ecosystem, the following was noted:

- PPI Inventory Ownership: In July 2021, Audit Services developed a flowchart displaying PPI attributes collected, stored, and transferred across major systems and applications. The business relies on this information flowchart and PPI attributes to manage information privacy. However, no owner is tasked to update and maintain this flowchart.
- Responsibility & Accountability: s 15(1)

Impact:

s 15(1)

All of the above will ultimately affect the organization's reputation and trust.

Agreed Upon Action Plan:

s 15(1)

B. Clarity in Roles, Responsibilities, and Accountabilities

- An owner will be identified and tasked with the responsibility to update the PPI process flowchart deliverable on a regular basis, and continued ownership of the document. Using the PPI process flowchart deliverable as a reference, will assign information owners for each critical system. Personnel responsible (or accountable) for the different activities will be listed.

Responsible Person:

A. i. Mark Goldberg, Chief Information Officer & V.P, Business Technology (with support and inputs from Dan Beebe, Chief Operating Officer)

ii. Marie-Noëlle Savoie, Chief Compliance Officer & V.P. Legal, Compliance, Security

B. Marie-Noëlle Savoie, Chief Compliance Officer & V.P. Legal, Compliance, Security

s 15(1)

3. Opportunity to Strengthen the Privacy Management Framework

Observations:

Information governance involves the managing of information collection, information usability, availability, integrity, security, and the timely destruction of information based on policies, procedures, and standards. One of the key objectives of information governance is ensuring the existence of privacy. This is achieved by proper use of information and prevention of PPI misuse. Additionally, it helps advance the organization by:

- Breaking down information silos within the organization
- Ensuring information is used properly
- Improving information quality
- Aiding in business decision-making

Audit Services reviewed the overall data governance framework from an information privacy perspective and noted the following:

A. Information Culture – Ever Increasing Volume of Digital Records

Gone are the days of holding as much data as technologically possible. Retaining data indefinitely is no longer an asset to the business, as information that is no longer useful can complicate decision-making and cloud insights. Retaining information without timely purging also broadens the attack surface for potential information theft, which results in player information privacy concerns.

> As cloud storage and computing cost come down, businesses are now swimming (or drowning) in data.

It is important for the organization to balance the value of information collection, analysis, and storage to the corresponding risks of privacy, security, and compliance.

> There were five exabytes of data created between dawn of civilization through 2003, but that much data is now created every two days.

B. Mandatory Privacy Breach Reporting

Based on changes to FIPPA effective February 1, 2023, organizations will be required to report privacy breaches of PPI to the Privacy Commissioner of British Columbia and affected individuals, if BCLC reasonably expects that significant harm to the individual could result. The organization should consider the following:

- Continue to evaluate the impacts of this change to FIPPA
- Determine if we, as a crown entity, are appropriately positioned to comply on reporting, if any situation arises

s 15(1)

C. Mandatory Privacy Management Program

Under FIPPA, public bodies are required to develop a privacy management program, the intent being that the organizations are properly equipped to manage and protect PPI in their custody. A typical program will include:

- PPI mapping (information mapping)
- Relevant and appropriate policies
- Risk assessment and remediation tools and procedures
- Education and training plans
- Process to manage personal information with Casino Service Providers

BCLC should continue to evolve the program to ensure information privacy is handled appropriately and the elements within the program meet all the mandatory requirements.

> An investment in privacy protection today can help prevent a costly data breach tomorrow.

Impact:

Having the appropriate framework for the privacy management program will provide the organization with a comprehensive setup to oversee and manage the risk of information privacy.

A well-established methodology will provide the additional confidence to the organization regarding the exhaustiveness of controls.

If any of the above are missing, not sufficiently monitored, or incomplete, it exposes the organization to an information privacy vulnerability which directly impacts organizational reputation and trust. This could potentially also have monetary impact.

Agreed Upon Action Plan:

A. s 15(1)

Will review internal policies and ensure they are aligned to evolving business trends and regulations specific to information retention and destruction.

B. Continue evolving the internal information breach incident identification and reporting methodology to ensure compliance with the new government requirement. Additionally, work with Casino Service Providers and key external stakeholders with who PPI is shared to confirm that adequate information security controls exist, and that if a breach incident were to occur that the structure exists to ensure timely and adequate reporting.

C. The privacy breach reporting process will be evaluated and modified to make it more user-friendly and easier to access by adding a link to the main page of the HUB.

D. Review the existing privacy management program and determine its adequacy and comprehensiveness. Based on new regulatory requirements, determine if additional steps or protocols need to be included to ensure compliance.

Responsible Person:

Sarah Marshall, Director, Information Governance

s 15(1)

4. Opportunity to Strengthen Information Privacy Awareness and Training

Observations:

The *Information Governance* training is mandatory for all employees during onboarding, and subsequently annually through periodic updates. Employee educational awareness and training courses are considered preventive controls specific to information management and information privacy. They provide numerous benefits, including the following key points:

- Practices on how to deter and avoid an information breach
- Information on how to input, store, and transfer PPI
- Highlight both acceptable and non-secure applications
- List the do's and don'ts of information management

A. Practices That Could Affect PPI

Audit Services reviewed the awareness/training program and the corresponding relation to information privacy practices and noted the following:

- No Monitoring of s 15(1)(l) Content: A large number of users (1,199 employees and contractors) have access to s 15(1)(l) and many use this free-text web application for various purposes. s 15(1)

ii. Information Security does not have visibility of user access to different projects/groups

> If you don't know what you have, there is no way you can protect it.

- s 15(1) Typically, the top concern for system Product Owners is maintaining functionality, accessibility to system, etc. s 15(1)

B. Training Offerings

There is currently a single course offered specific to PPI. The *Information Governance* course is mandatory for all employees and Level 1 Contractors to complete every year, and it covers best practices in handling sensitive information. Audit Services' review of this process highlighted the following:

- 15(1)

> Be not afraid of progressing slowly, be afraid only of standing still.
> (Specific to learnings from training translating into practice.)

s 15(1)

BCLC Employees, although not at 100%, have a much higher rate of completion of 97%.

- Privileged User Training: The standard training offering satisfies general requirements, but more advanced training courses should be available and made mandatory to those who have escalated privileges regarding PPI.

Impact:

s 15(1)

There is sufficient evidence based on recent external, third-party incidents in other organizations that a privacy breach can occur and expose the organization through the mishandling of information by a contractor.

Finally, the entire operating model is based on the fundamental principle of "trust". Therefore, any mishandling or exposure of personal information can impact the very core of our operations.

Agreed Upon Action Plan:

A. Will explore an automated alerts function to monitor s 15(1)(l) posting. Additionally, will periodically remind/inform existing and new employees and contractors about s 15(1) Periodic reminders will be shared via HUB on this topic.

B. s 15(1)

Advanced courses will be explored and developed if required, for privileged users who access and handle PPI.

Responsible Person:

A. Mark Goldberg, Chief Information Officer and V.P., Business Technology
Sarah Marshall, Director, Information Governance

B. Sarah Marshall, Director, Information Governance
Mark Lane, Director, Cyber Security

s 15(1)

APPENDIX 1

Description of Systems Referenced

System	Description
s 15(1)(l)	A s 15(1)(l) Customer Relationship Management platform that drives marketing automations, content management, and customer data analytics
s 15(1)(l)	Issue and defect tracking web-based product used by Agile project teams
s 15(1)(l)	Wiki-style collaboration web-based platform that houses organizational project details
s 15(1)(l)	Customer Service Centre (CSC) performance management software that records conversations, employee desktop screens, and captures metadata during discussions
s 15(1)(l)	CSC live chat solution for customer engagement through web, mobile, or social messengers that stores chat transcript and history
s 15(1)(l)	CSC software routing callers to an agent best suited for customer needs using customizable data; contains historical reporting, call monitoring, and call recordings
s 15(1)(l)	Gaming platform for retail lottery products
s 15(1)(l)	Gaming platform for eLottery products
s 15(1)(l)	Gaming platform for PlayNow products
s 15(1)(l)	Gaming platform for casino products
s 15(1)(l)	Casino incident reporting system
s 15(1)(l)	Enterprise resource planning software

APPENDIX 2

Key Terms Defined and Explained

Player Personal Information (PPI)

Information that can be tied to an individual person, which must be protected and used in a manner that protects the individual's rights to privacy. Information includes data; but data doesn't necessarily include information.

Information Security

Controls focused on how information is protected from the many external and internal threats that exist and can mitigate inadvertent misuse. However, just implementing these measures alone without sufficient information privacy protocols does not fully address information theft or concerns around misuse.

Information Privacy

Controls involving the managing of PPI of partners, employees, and all other stakeholders interacting with the organization in a manner that supports its intended purpose. It is a sub-set of information security concerned with the proper handling of data.

Information Breach (i.e., Hack, Cyber Incident)

An incident involving the unauthorized or illegal viewing, access, or retrieval of information. It is an act designed to steal or publish information for an unsecured or illegal location. This scenario is also known as a "data spill" or a "data leak".

Privileged User

A user who is authorized (and therefore trusted) to perform higher security-relevant functions with increased administrative permissions.

Distribution List

Executives and Management	**Enterprise Risk Management**
Sandy Austin	Jennifer Barbosa
Dan Beebe	
Pat Davis	
Alan Kerr	
Martin Lampman	
Mark Lane	
Sarah Marshall	
Emily McDonald	
Peter ter Weeme	

Audit Team

Matt Froh

Rao Wandawasi

Karen Wang

Source References

Techopedia.com

Forbes.com

Cybersopia.net

CareerFoundry.com

TechTarget.com

DataVersity.net

blog.RescueTime.com

OIPC.BC.ca