OLG CORPORATE POLICY

TITLE: **Protection of Privacy**

OWNER: **Legal Services and Litigation – Privacy Office**

STATUS: **Final**

Table of Contents

PURPOSE 3
APPLICATION AND SCOPE 3
POLICY STATEMENT 3
DEFINITIONS 4
REQUIREMENTS 7
ROLES AND RESPONSIBILITIES 11
POLICY OWNER 15
RELATED POLICIES AND PROCEDURES 15
REFERENCES AND FORMS 16
REVISION / REVIEW HISTORY 16
APPROVALS 16
APPENDIX A: DEFINITION OF “PERSONAL INFORMATION” UNDER FIPPA 17
APPENDIX B: OLG’S ENTERPRISE COMPLIANCE FRAMEWORK 18
APPENDIX C: PRIVACY BREACH RESPONSE PROTOCOL 19
APPENDIX D: PRIVACY BREACH EVALUATION CRITERIA 20

PURPOSE

The purpose of this policy is to establish OLG's approach, responsibilities and requirements for compliance with Part III of the *Freedom of Information and Protection of Privacy Act*[1] and related Regulations (collectively 'FIPPA') under OLG's Enterprise Compliance Framework. The policy also embodies and supports an organizational culture that is aware of our obligations to protect Personal Information in OLG's custody and/or under its control.

APPLICATION AND SCOPE

This policy applies to all OLG Divisions and Employees and governs any collection, use, disclosure, retention, or otherwise processing of "Personal Information" (as defined under FIPPA) in the custody and/or control of OLG, regardless of the format, storage or medium of the information.

While some Personal Information under OLG's control may be excluded from the application of FIPPA, i.e. certain employment related information, OLG Employees and Divisions are required to treat all Personal Information in OLG's custody or control as governed by this policy. Employees should consult OLG's Privacy Office if there is any actual or suspected contravention of this policy.

As set out below, each Division is responsible for ensuring that appropriate controls and procedures are in place so that Service Providers and Vendors with custody of personal information that is under OLG's control will comply with the OLG's obligations under FIPPA.

POLICY STATEMENT

OLG must collect, use, disclose, retain, safeguard and dispose of Personal Information in its custody and/or under its control in accordance with Part III of FIPPA. Privacy Breaches or other breaches of OLG's obligations under FIPPA may lead to reputational damage, civil liability or regulatory sanctions. Therefore, OLG has designated FIPPA as a Core Regulatory Obligation under the Enterprise Compliance Framework and all Divisions are thereby subject to enhanced oversight regarding FIPPA compliance.

[1] R.S.O. 1990, c. F.31.

DEFINITIONS

Custody: (of a record) means the physical possession of a record or the repository in which it is stored, excluding unsolicited or accidental possession. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security, but does not include the right or authority to determine the life cycle of the record.

Core Regulatory Obligation: those regulatory obligations viewed by OLG as higher risk and addressed with enhanced oversight and reporting by Corporate Compliance. A list of Core Regulatory Obligations is set out in Appendix B of OLG's Enterprise Compliance Management policy.

Control: (of a record) means the right or authority, directly or indirectly, to determine the management of a record (recorded information) throughout its life cycle, including its creation, capture, security and subsequent restricting, and regulating and administering its use, disclosure or disposal. For interpretive purposes, OLG has 'control' of a record, as defined above if one or more of these factors exist:

- the record was created by an employee, officer or board member of OLG in the course of his or her duties
- the record was created by an outside consultant or contractor retained by OLG and reasonably relates to the scope of the retainer
- the record was created by a third party retained by a person who has entered into a contract with OLG and where the record reasonably relates to the subject matter of the contract between that person and OLG
- the record is specified in a contract or agreement as being required for OLG information, inspection, review or approval
- OLG has the authority to regulate the record's creation, use and disposition and has the right to access the record
- OLG requires the information contained in the record to comply with applicable law or to protect its rights. This includes its obligation to provide the information to its regulators upon demand and its obligation to ensure compliance by third parties to certain laws
- OLG reasonably requires authority over the information contained in the record in order to meet its mandate to conduct and manage lottery schemes in Ontario
- OLG is responsible for the creation, use or disclosure of the record in accordance with applicable law and can be sanctioned or held liable for any inappropriate or unauthorized creation, use or disclosure of the record

Delegate: an official to whom the Head's powers and duties, as set out in FIPPA, have been delegated.

Directory of Records: a publication required by FIPPA that describes the type of records and manuals maintained by Ontario government institutions, including Personal Information banks.

Divisions: OLG Divisions including Operations, People and Culture, Corporate Affairs, Information Technology, Finance, Enterprise Strategy & Analytics, Governance, Legal & Compliance, Horse Racing and Business Design. Each Division contains departments that must also comply with this policy.

Employee or Employees: full-time, part-time, or contracted staff member; temporary or seasonal staff member; student; intern.

Enterprise Compliance Framework (ECF): defines the foundational practices and core compliance activities to promote regulatory compliance and to manage regulatory compliance risk. For a visual representation of the ECF, please see Appendix B.

Freedom of Information & Protection of Privacy Act **(FIPPA):** legislation governing the collection, use, disclosure and retention of Personal Information and the regulations made thereunder (including Regulations 459[2] and 460[3]).

Head: the official designated under FIPPA who is accountable for compliance with the Act for the enterprise, including making decisions with respect to access to information, management of records, and for ensuring that Personal Information is managed in accordance with privacy requirements. At OLG, the Head is the President and CEO (P/CEO).

Information and Privacy Commissioner of Ontario (IPC): the Ontario government organization that acts independently to uphold and promote open government and the protection of personal privacy.

Personal Information: information about an identifiable individual as defined by section 2(1) of FIPPA. Among other things, Personal Information includes an identifiable individual's name where it appears with other Personal Information, identification information (e.g. Social Insurance Number), contact information, race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status, education, medical history, personal email address, psychological or psychiatric history, criminal or employment history personal views, and information relating to financial transactions in

[2] R.R.O. 1990, Reg. 459: Disposal of Personal Information.
[3] R.R.O. 1990, Reg. 460: General.

which the individual has been involved. For the definition of "Personal Information" as provided in FIPPA, see Appendix A.

Personal Information Bank: a collection of Personal Information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual (as defined in section 2.1 of FIPPA).

Privacy Breach: the unauthorized collection, use, disclosure, alteration, retention or access to Personal Information. A Privacy Breach may involve the Personal Information of a single individual or group of individuals. Privacy Breaches must be handled in accordance with the Privacy Breach Response Protocol in Appendix C.

Privacy Breach Response Protocol: A protocol setting out the steps that OLG's Employees and Divisions must take in response to any actual or potential Privacy Breach at OLG and the Division/individual accountable for each step. The Privacy Breach Response Protocol is set out in Appendix C to this policy.

Privacy Impact Assessment (PIA): a process/tool to assess whether new technologies, information systems, initiatives and/or proposed programs or policies that involve the collection, use, disclosure or retention of Personal Information present a privacy risk and meet privacy requirements under this Policy, and to identify mitigation measures to address risks or gaps that are detected.

Privacy Office: The OLG department responsible for OLG's privacy program, including the development and maintenance of policies, protocols and procedures. The Privacy Office provides organizational leadership in managing privacy incidents/ breaches.

Record: any record of information however recorded, whether in printed form, on film, by electronic means or otherwise as defined by section 2(1) of FIPPA.

Regulatory Leads: Employees designated by OLG Divisions to promote privacy compliance and help business leaders manage regulatory risk.

Regulatory Obligations: Obligations prescribed by law and associated regulations, directives, guidelines and regulatory standards.

Service Provider: Any person or entity operating a lottery scheme that is conducted and managed by OLG, including but not limited to, any contract worker, temporary employee or other third party who has a contractual relationship with OLG and who is responsible for the day-to-day operations for a lottery scheme that they or it operates on behalf of OLG.

Vendor: Any person or entity providing a product or service to an OLG Division, including

but not limited to, any contract worker, temporary employee or other third party who has a contractual relationship with OLG and who is responsible for providing OLG with a product or service.

REQUIREMENTS

1. Implement Policies, Procedures and Controls

1.1. Policies

1.1.1. OLG must post a privacy statement on its public website(s). The statement must provide details about the collection, use, disclosure, and/or other processing of Personal Information, as well as the security of Personal Information gathered by OLG, including information gathered through OLG's websites.

1.1.2. OLG will designate a senior official to manage the Privacy Office and staff as required. Together, the senior official and staff will constitute the Privacy Office (as defined above).

1.1.3. The Privacy Office, as directed by the Head or Delegate, must create and maintain a corporate policy establishing requirements for OLG Divisions to ensure that Personal Information is collected, used, disclosed, and/or otherwise processed in accordance with FIPPA.

1.1.4. OLG Divisions must design and implement functional policies, procedures and/or control activities that align with this policy and ensure their operations are in compliance with FIPPA and this Policy. In addition, where Service Providers and Vendors collect, use, disclose, and/or otherwise handle Personal Information on behalf of OLG, Divisions must prescribe contractual provisions that require Service Providers and Vendors to design and implement functional policies, procedures and/or controls to comply with the requirements under FIPPA and this Policy. Where appropriate and practicable, contractual provisions should also permit OLG to periodically audit, monitor and test for compliance with FIPPA by Service Providers and Vendors. The Privacy Office will be available to assist Divisions in creating and implementing functional policies, procedures and controls.

1.2. Procedures

1.2.1. Personal Information must be collected in accordance with FIPPA. All individuals whose Personal Information is collected by OLG must be presented with a notice of collection where required by law and, where applicable, appropriate consent to collect and process

Personal Information must be obtained by OLG. The Notice of Collection must detail OLG's authority to collect Personal Information, specify the intended use(s) of the Personal Information and provide contact information for questions about the collection.

1.2.2. To identify and address privacy risks regarding projects and initiatives involving the collection, use, disclosure, or retention of Personal Information, OLG Divisions are accountable to engage the Privacy Office to conduct Privacy Impact Assessments ("PIAs") sufficiently early in the project management lifecycle so as to ensure sufficient mitigation of risks. The Privacy Office will conduct PIAs where appropriate based on the nature of projects and initiatives, and will use a risk-based approach in determining the scope of PIAs. The Privacy office may engage Corporate Compliance as necessary to assist in the completion of PIAs.

1.2.3. To ensure that privacy compliance is formally integrated in the project management lifecycle at OLG, the Privacy Office must participate in Corporate Compliance's partnership with Corporate Project Governance (N.I.C.E.) to provide subject matter expertise regarding projects and initiatives conducted by OLG Divisions and Departments.

1.2.4. To ensure that Personal Information in OLG's custody or under its control is appropriately safeguarded, the Information Security Office ("ISO") must conduct appropriate and risk-based threat risk assessments or other assessments regarding projects and other streams of work undertaken by OLG Divisions and must provide advice regarding the implementation of reasonable security controls.

1.2.5. ISO will continue to implement, maintain, and carry out related information security policies.

1.2.6. Corporate Compliance, in consultation with the Privacy Office and OLG Divisions, must conduct compliance risk assessments and other periodic assessments to understand each Division's control environment and risk mitigation activities with regards to FIPPA. Compliance risk assessments do not eliminate the need for OLG Divisions to conduct PIAs as stipulated in requirement 1.2.2 of this policy. Compliance risk assessments complement PIAs and will consider the results of PIAs to understand the how privacy risks are being managed by OLG Divisions.

1.3. **Controls**

1.3.1. Each OLG Division must obtain evidence that Service Providers and Vendors that collect, use, disclose, or retain Personal Information at the direction of their Division have complied with OLG's applicable

functional policies and procedures relating to FIPPA. In compliance with the Enterprise Compliance Management policy, OLG Divisions must manage and address any identified risks and ensure their Service Providers and Vendors do the same.

1.3.2. Access to Personal Information within OLG will be restricted to authorized personnel who reasonably require it to carry out their responsibilities.

1.3.3. Individuals may request access to their Personal Information in OLG's custody and/or control in accordance with FIPPA and OLG policies.

2. Training and Education

2.1. The Privacy Office will create appropriate training tools and modules on the requirements in Part III of FIPPA, including the appropriate collection, use, disclosure and retention of Personal Information, as well as the Privacy Breach Response Protocol. These training materials will be made available to all OLG Divisions and Employees and training will be mandatory for Employees as part of onboarding. In addition, ongoing training will be assigned to individual employees based on role and responsibility as identified by each Division and recommendations developed by Corporate Compliance. Corporate Compliance may also make recommendations to the Divisions regarding who should be required to complete annual training. Divisions are accountable for enforcing training requirements regarding post-onboarding and ongoing training.

2.2. The nature and extent of training and education completed must be proportionate to the risk profile of each Division and appropriate for an Employee's responsibilities.

2.3. OLG Divisions must require their Service Providers and Vendors to train and educate their personnel who routinely access Personal Information in the custody or under the control of OLG on compliance with FIPPA and must include these requirements by contract.

3. Monitoring and Testing

3.1. OLG Divisions must implement practices to supervise and govern the collection, use, disclosure and retention of Personal Information by employees in accordance with FIPPA, this Policy (and the Related Policies set out below) and applicable departmental procedures and control activities. OLG Divisions must engage Corporate Compliance as necessary to assist in the development and implementation of such practices.

3.2. As part of privacy risk management and in accordance with the OLG Enterprise Compliance Management policy, Corporate Compliance, with support from the Privacy Office, must use a risk-based approach in monitoring and testing each OLG Division's privacy controls.

3.3. With respect to Service Providers and Vendors, Corporate Compliance (with support from the Privacy Office and in collaboration with Risk and Audit) must monitor and test privacy controls prescribed by contractual obligations.

4. Manage Breaches and Issues

4.1. OLG's Privacy Office, in partnership with Corporate Compliance and under the direction of the Head or Delegate, has created the Privacy Breach Response Protocol and will make this protocol available to all Divisions and Employees.

4.2. The Privacy Office, as directed by the Head or Delegate, and with legal advice and direction as required, will advise on the implementation of and adherence to the Privacy Breach Response Protocol in the event of breach.

4.3. In accordance with the Privacy Breach Response Protocol, OLG Divisions and Employees must promptly report Privacy Breaches, control weaknesses, and/or other privacy risks regarding their operations or the operations of their Service Providers or Vendors to the Privacy Office and Corporate Compliance.

4.4. In the event of a Moderate or High rated Privacy Breach (as defined in the Privacy Breach Evaluation Criteria – Appendix D), the Privacy Office must inform and consult with OLG Divisions, including but not limited to Corporate Affairs, Information Technology, and Governance, Legal & Compliance regarding potential risks, mitigation strategies, and external communications related to the Privacy Breach. After consultation, the Privacy Office must make a recommendation to the VP Legal Services & Litigation regarding notification to affected individuals and/or the IPC. The VP Legal Services & Litigation shall determine whether notification to affected individuals and/or the IPC is appropriate in the circumstances, and must coordinate with the Privacy Office, Corporate Affairs, and Information Technology to carry out any notification to external parties.

4.5. In the event of a Privacy Breach, OLG Divisions impacted by the breach must promptly take steps to determine the cause of a breach, mitigate any harm or potential harm and reduce the likelihood of a future occurrence and, if a Service Provider is involved or impacted by the breach, OLG shall ensure and obtain evidence that Service Providers and Vendors do the same.

4.6. Corporate Compliance, in partnership with the Privacy Office, must track, monitor and report internally on privacy issues across OLG Divisions (and their Service Providers and Vendors), including remedial actions.

5. Reporting

5.1. OLG Divisions must provide information, as requested by Corporate Compliance, for consolidated regulatory compliance reporting which includes privacy matters.

5.2. OLG Divisions must ensure that Service Providers and Vendors provide the information they are required to provide to OLG pursuant to contractual obligations for OLG reporting.

5.3. Corporate Compliance, in consultation with the Privacy Office, must report on privacy outcomes and state of compliance for Senior Management, Executive Committee and the Audit & Risk Management Committee of the Board (ARMC).

ROLES AND RESPONSIBILITIES

Board of Directors, through the ARMC, is responsible for overseeing regulatory compliance across OLG as prescribed in the ARMC Terms of Reference.

Head of the institution is the official with accountability for compliance with FIPPA and is responsible for:

- Ensuring that OLG complies with FIPPA and any applicable policies, directives, Memorandums of Understanding (MOUs) and guidelines,
- Determining whether to appoint a delegate for access and privacy matters and ensuring that programs have been established for complying with FIPPA, and
- Signing a delegation of authority (DOA) document if the head's powers and duties are to be delegated.

Executive Committee sets strategic direction for the enterprise and shall:

- Communicate expectations for privacy compliance and set risk tolerance,
- Ensure there are appropriate resources within OLG to appropriately collect, use and disclose Personal Information, and
- Oversee compliance with FIPPA and privacy risk management across OLG Divisions and their Service Providers and Vendors.

Risk and Audit is responsible for:

- Conducting periodic audits of OLG departments and Divisions to identify controls required to mitigate privacy risks, assess the effectiveness of the controls in place and ensure consistency with industry standards regarding privacy,
- Providing recommendations and documenting mitigation plans to address privacy risks identified during audits, and
- Monitoring, validating, and reporting on the status of recommendations and implementation of mitigation plans or other actions to be taken as a result of an audit.

VP Legal Services and Litigation is responsible for

- Overseeing the Privacy Office including by supporting and providing direction and legal advice to the Privacy Office as required,
- Supporting the Privacy Office in the investigation, management and response to Privacy Breaches as required and leading investigations and responses where appropriate, and
- Report to senior leadership regarding Privacy Breaches or other privacy manners where appropriate or required.

OLG Divisional Heads (on behalf of their respective Divisions) own the risk of non-compliance with FIPPA and supervise operations, including those conducted and managed by OLG. Through their respective Employees, OLG Divisions are also responsible for initiating and following the Privacy Breach Response Protocol. Divisional Heads are expected to:

- Conduct and manage, and where applicable operate, their business in compliance with FIPPA and ensure their Service Providers and Vendors do the same,
- Align day-to-day operational practices with this policy and assign Regulatory Leads as appropriate to help manage privacy risks,
- Consult with the Privacy Office and Corporate Compliance to assess privacy risks for significant strategic, operational decisions, policy matters and conduct PIAs, when applicable, and
- Supervise the implementation of appropriate controls and remediation of issues to mitigate privacy risk and safeguard Personal Information.

Managers and Supervisors are expected to:

- Conduct their duties in compliance with FIPPA and ensure that employees do the same,
- Verify that Employees complete onboarding training if they collect, use or disclose Personal Information,
- Participate in and engage the Privacy Office to complete PIAs and other privacy risk assessments,
- Report privacy issues to the Privacy Office and Corporate Compliance immediately upon discovery in order to determine what notification requirements, if any, arise from the issue reported, i.e. breach notification to the IPC or affected individuals,
- Address privacy issues in an appropriate and timely manner.

Employees are expected to:

- Understand FIPPA requirements for their area of responsibility, take reasonable measures to protect the privacy of Personal Information and seek clarification or advice from the Privacy Office where unclear about requirements,
- Maintain the security and confidentiality of physical records that contain OLG personal information by keeping their workstations free of unsecured physical records, securing records containing Personal Information in locked filing cabinets or drawers, and securely disposing of transitory records in accordance with OLG records retention and information security policies.
- Maintain the security and confidentiality of electronic records containing Personal Information by ensuring that devices containing them are reasonably secure from unauthorized access through both physical and electronic access controls.
- Complete privacy training if they collect, use or disclose Personal Information, and
- Initiate and follow the Privacy Breach Response Protocol if they become aware of a potential or actual Privacy Breach.

Privacy Office:

- Create, periodically review and (if required) update corporate privacy artifacts including policies and training programs,

- Annually review OLG's internal definition of Personal Information, and communicate any revisions to ISO, Risk and Audit, and other key stakeholders,
- Conduct risk-based reviews of projects and other streams of work undertaken by OLG Divisions for compliance with FIPPA and applicable OLG policies. Participate in Enterprise Information Management's data lake use case processes and Corporate Compliance's partnership with Corporate Project Governance (N.I.C.E.) to provide subject matter expertise throughout the project management lifecycle. Provide advice to assist OLG Divisions (and their Service Providers and/or Vendors when applicable) with the implementation of privacy policies, procedures and controls and completion of PIAs,
- Respond to reported Privacy Breaches to identify potential risks, mitigation strategies, and plans of action.
- Contribute to the monitoring and testing of privacy compliance in partnership with Corporate Compliance,
- Report privacy issues to Corporate Compliance for consolidated reporting and investigate reported privacy issues to ensure they are remediated,
- Participate in compliance risk assessments led by Corporate Compliance when those assessments evaluate privacy risks,
- Provide privacy advice to OLG senior leadership as required,
- Review training tools and modules at least once every two years to identify any necessary updates or additions,
- Contribute to the update of OLG's Directory of Records, and
- Coordinate notifications to the IPC and/or affected data subjects of a Privacy Breach if it is determined that notification is warranted after consultation with OLG Legal Services.
- Notify other OLG Divisions of Privacy Breaches to secure breach response support.

Corporate Compliance is responsible for monitoring compliance with FIPPA and shall:

- Create and maintain the ECF, including expectations to promote compliance with FIPPA,
- Support the Privacy Office with the development of privacy policies and programs to

ensure alignment with the ECF,

- Lead privacy risk assessments using a methodology aligned to OLG Enterprise Risk Management,
- In partnership with the Privacy Office, review and effectively challenge controls and training programs and issue remediation plans developed by OLG Divisions (and their Service Providers and Vendors),
- Consult with the Privacy Office to create monitoring/testing plans for privacy compliance and investigate privacy issues, and
- Assess compliance with FIPPA and report to Senior Management, Executive Committee and ARMC.

Information Security Office (ISO) is responsible for

- Conducting threat risk assessments or other assessments regarding projects and other streams of work undertaken by OLG Divisions to assess compliance with applicable OLG information security policies, and to identify information security risks and corresponding controls.
- Providing advice to assist OLG Divisions (and their Service Providers and/or Vendors when applicable) with the implementation of information security policies, procedures and controls.
- Establishing enterprise security programs and controls to protect Personal Information in electronic format that is in the custody or under the control of OLG, and
- As otherwise described in OLG policies.

Enterprise Document & Records Management (EDRM) is responsible for establishing programs and policies to retain Personal Information in accordance with FIPPA requirements.

POLICY OWNER

Legal Services and Litigation – Privacy Office

RELATED POLICIES AND PROCEDURES

- CP-02-07-003: Records Management – Off-Site Storage Services

- FP-04-08-002: Mobile Communication Devices
- FP-04-05-009: Information Classification and Handling
- FP-04-05-013: Application Service Provider Security
- CP-04-05-018: Third Party Access
- FP-04-05-019: Data Protection
- OLG Information Classification and Handling Procedures
- CP-06-03-003 Enterprise Compliance Management
- CP-10-01-001 Code of Business Conduct
- CP-08-01-001 Enterprise Documents & Records Management
- CP-08-01-005 Records Classification Scheme and Retention Schedule

REFERENCES AND FORMS

- *Freedom of Information and Protection of Privacy Act* (FIPPA) RSO 1990, and Regulations
- Ontario Public Service Freedom of Information Guideline
- Ontario Public Service Privacy Impact Assessment Guidelines
- Introduction to Privacy by Design (PbD) http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/

REVISION / REVIEW HISTORY			
Version/Revision Date	**Requested By**	**Updated By**	**Summary of Revision**
October 18th, 2019	Senior Vice President, Governance, Legal and Compliance, General Counsel and Corporate Secretary	Manager, Privacy Office	Original version to supersede the privacy provisions of the Freedom of Information and Privacy Legislation policy.

APPROVALS		
Approver	**Authorization**	**Date**
Information & Technology Committee	Email approval	March 27th, 2020
Tony Wong, Senior Vice President Governance, Legal and Compliance, General Counsel and Corporate Secretary	Email approval	March 11th, 2020

APPENDIX A: DEFINITION OF "PERSONAL INFORMATION" UNDER FIPPA

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31, s. 2(1)

"Personal Information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

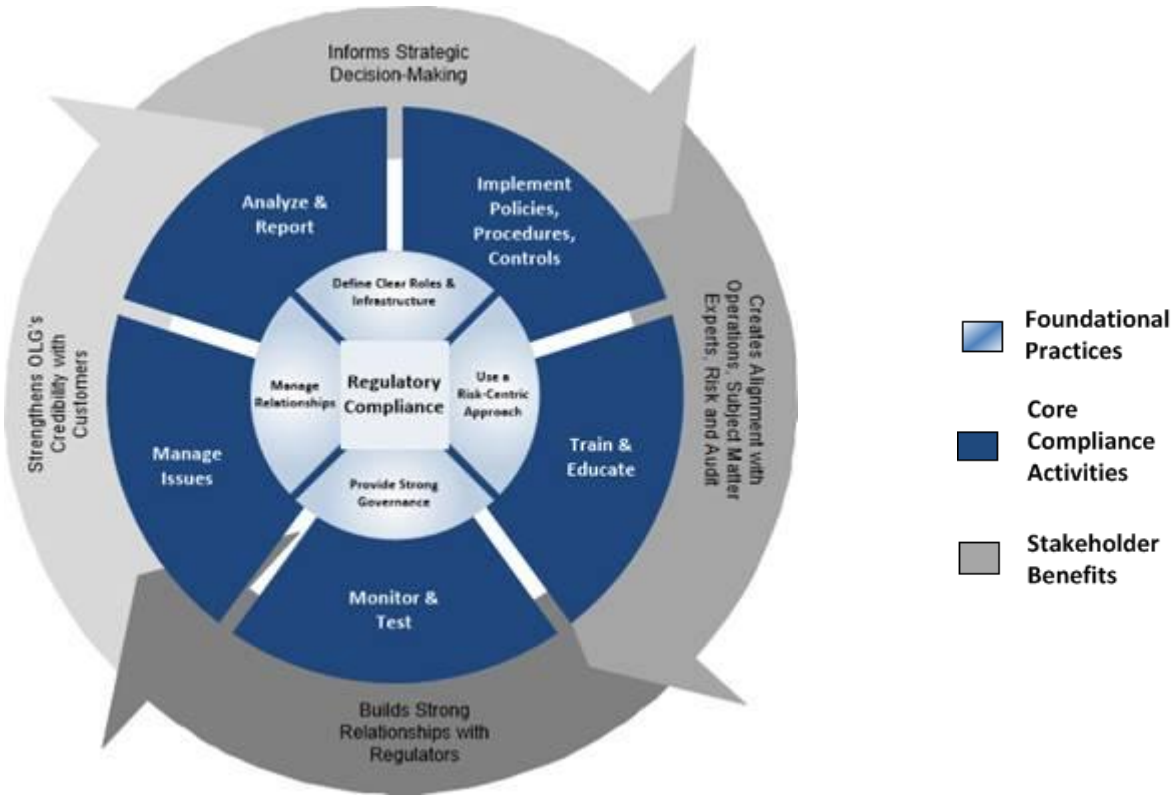
(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual;

Personal information does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

APPENDIX B: OLG'S ENTERPRISE COMPLIANCE FRAMEWORK



Define Clear Roles & Infrastructure: Develop and maintain a structured compliance management framework with clearly defined roles, responsibilities and interactions

Use a Risk-Centric Approach: Identify, assess and address Regulatory Compliance Risks. Embed risk assessment practices throughout the framework to encourage risk-centric decision-making

Provide Strong Governance: Senior Leadership and the Board set tone from the top, establish regulatory risk appetite and monitor compliance outcomes

Manage Relationships: Use a proactive and structured approach to interact with internal & external stakeholders in order to build relationships and share the right information, at the right time

Implement Policies, Procedures, Controls: Set expectations and baseline standards to direct employees

Train & Educate: Inform staff about their regulatory compliance obligations and develop the skills, knowledge and competencies required to comply

Monitor & Test: Oversee and evaluate compliance performance using a standardized approach for measurement, analysis and control verification

Manage Incidents & Issues: Address incidents at the root cause to prevent similar occurrences or escalation into serious issues

Analyze & Report: Analyze compliance outcomes and prepare consolidated reporting for management and the Board

APPENDIX C: PRIVACY BREACH RESPONSE PROTOCOL

Employees must follow the Privacy Breach Response Protocol to investigate, remediate and report a suspected Privacy Breach.

Be sure to

Document…

- Incident date & description
- OLG systems impacted
- # of affected individuals
- Type of PI in scope
- Any 3rd parties notified
- Suspected causes
- Containment & mitigation steps taken

Examples of a Privacy breach:

- Lost or stolen equipment that contains Personal Information (laptops, cell phones).
- Improper disclosure of or access to Personal Information by unauthorized individuals or groups.
- Personal Information databases accessed by internal employees for non-authorized purposes.
- Using an individual's Personal Information for purposes outside the reason that was originally provided when the information was collected.
- Cyber-attacks or other information security incidents exposing Personal Information
- Over collection of Personal Information or collecting it indirectly

APPENDIX D: PRIVACY BREACH EVALUATION CRITERIA

Overview

Privacy Breaches should be assessed by the Privacy Office, with support from Corporate Compliance and other OLG Divisions as required, to:

1) Identify potential risks to any individual(s) whose Personal Information was impacted in the breach;
2) Identify potential risks to OLG as a result of the breach;
3) Assign an appropriate rating based on identified risks, and
4) Take appropriate containment and/or mitigation strategies.

Risks to Individuals

A Privacy Breach should be assessed to determine whether it could result in a **real risk of significant harm** to the individuals affected. Assessments should consider factors such as:

1. What (if any) potential harms could be suffered by the affected individuals as a result of the breach. Examples of harm include but are not limited to:
    - identity theft,
    - financial loss or loss of opportunity,
    - physical harm,
    - damage to or loss of property,
    - embarrassment or humiliation, and
    - damage to reputation and relationships.
2. The significance or severity of the harm(s) identified as possible consequences of the breach. Relevant factors in determining the significance or severity of harm include:
    - The anticipated number of individuals affected who could suffer each of a breach's potential harms
    - The Personal Information involved and its level of sensitivity in context of the breach. While certain information is inherently of a higher risk when improperly processed (such as social insurance number, health/medical information, or financial/payment information), the sensitivity of Personal Information can vary depending on the purposes for which it is processed by OLG and the circumstances of the breach;
    - The number of Personal Information elements breached;
    - The risk of successive breaches based on the initial breach;
    - The permanence of the harm's consequences;

- The anticipated recipients of the breached information;
- The ease of perpetrators identifying breach victims; and
- The speed required for protective measures taken by victims to be effective.

3. The likelihood of a potential harm actually being suffered by an affected individual. Relevant factors in determining the likelihood of harm coming to fruition include:
    - Whether any internal or external parties gained access to Personal Information and the circumstances through which they gained access;
    - Whether any internal or external parties who gained access can be reasonably expected to intentionally or unintentionally do harm to individuals affected by the breach;
    - The relative ease of an internal or external party deliberately or accidentally causing a potential harm;
    - Whether the breached information was encrypted, anonymized or otherwise secured;
    - Whether or not the breached information can be retrieved or the breach can be reversed; and
    - How long breached information has been exposed.

Risks to OLG

The Privacy Office should consult with Corporate Affairs, Legal, Information Technology, Corporate Compliance and other OLG Divisions to identify whether the breach poses any potential risk to OLG as well as the likelihood of a given risk coming to fruition. Risks of Privacy Breaches to OLG include:

- Regulatory proceedings and investigations;
- Civil liability;
- Reputational damage; and
- Impacts to business continuity.

Privacy Breach Rating

Based on the risks identified by relevant internal stakeholders, the Privacy Office in consultation with Legal, and other Divisions as required should assign each breach a rating having regard to the consequences set out in the chart below. After a risk rating is assigned, OLG shall take actions corresponding to the risk rating which are consistent with the Recommended Responses set out in the chart below.

Rating	Consequences	Recommended Responses
Low	• The potential objective harm to individuals is of low/ no impact. • The potential objective harm to OLG is low/no impact. • It is unlikely potential objective harm to individuals or OLG will actually occur, or any harms already realized are of minimal impact. • One or small number of individuals are impacted • The types of personal information impacted by the breach are generally not considered sensitive.	• The Privacy Office or Corporate Compliance must investigate and document the circumstances of the breach, including the cause, date/time, number of individuals impacted, and action items to be taken (if any). • The Privacy Office, with the support of Corporate Compliance and applicable OLG departments, must identify and document any appropriate mitigation steps to prevent or reduce the impact of the breach and coordinate to ensure they are taken in a timely manner.
Moderate	• The potential objective harm posed by the breach is of moderate impact to individuals. • At least one of the potential risks posed by the breach is of moderate impact to OLG. • Some objective harm has been suffered by individuals or OLG, or some harm is reasonably likely to occur. • A small to moderate-sized volume of individuals is or may be impacted by the breach. • The breach poses or is the result of a low or	• Take actions as required for a breach rated 'Low'. • The Privacy Office must notify the VP Legal Services and Litigation who, at their discretion, may notify other OLG stakeholders as deemed necessary. • After consultation with the Privacy Office, Corporate Affairs, IT (and other internal stakeholders as required) the VP Legal Services and Litigation must determine whether impacted individuals will be notified of the breach and take action accordingly. • If the breach is the result of or poses the risk of an

Rating	Consequences	Recommended Responses
	moderate information security risk to OLG.	information security incident, the Privacy Office must provide assistance to the Information Security Office (as required) regarding privacy compliance/risk mitigation.
High	• A significant number of individuals impacted. • The breach poses or is the result of a high-risk information security incident. • At least one potential objective harm posed by the breach is of high risk to individuals and/or OLG. • Multiple moderate objective harms have impacted or are likely to impact individuals or OLG. • The breach was deliberately perpetrated by an internal or external actor. • Health, financial, or social insurance information is impacted.	• Take actions as required for a breach rated 'Moderate'. • The Privacy Office must notify the VP Legal Services and Litigation who must ensure OLG senior leadership is notified as required. • After consultation with the Privacy Office, Corporate Affairs, IT (and other internal stakeholders as required) the VP Legal Services and Litigation must determine whether impacted individuals, the IPC, and other stakeholders will be notified of the breach (and timing of notification) and take action accordingly. • The VP Legal Services and Litigation or SVP GLC to report to senior leadership on the status of any mitigation steps taken to reduce or prevent harm to OLG or individuals.

Containment and Mitigation

Upon notification of a breach, the Privacy Office should immediately confirm whether the breach involves access to or the security of any OLG database, application or system. Any breach that involves or could potentially involve the improper access to or security of any OLG database, application or system should immediately be forwarded to ISO for triage and response.

Considering the nature of the breach, identified risks to affected individuals and OLG, and the rating assigned to the breach the Privacy Office, Corporate Compliance, Legal, Corporate Affairs, Information Technology, and/or any other consulted OLG Division should jointly develop a mitigation plan to limit the impacts of a breach as required. Potential components of a breach mitigation plan may include:

a) Temporary or permanent changes to technical, administrative, or physical controls regarding the security of Personal Information;
b) Notifying affected individuals or the Information and Privacy Commissioner of Ontario of the breach;
c) Temporary suspension of certain business processes or employee access to Personal Information pending updates to policies, procedures, or controls;
d) Preparation of external communication collateral regarding the breach; and
e) Consultation with external legal counsel regarding next steps.

Ultimate accountability for containment and mitigation shall be with the head of the Division that has been impacted by the breach.