OLG FUNCTIONAL POLICY

TITLE: **Information Classification and Handling**

POLICY #: **FP-04-05-009**

OWNER: **IT Risk Management and Compliance**

STATUS: **Final**

Table of Contents

TITLE:	Information Classification and Handling
POLICY #:	FP-04-05-009
OWNER:	IT Risk Management and Compliance
STATUS:	Final

PURPOSE

The purpose of the Information Classification and Handling policy is to help Ontario Lottery and Gaming Corporation (OLG) employees determine what information can be disclosed to non-employees, as well as understand the relative sensitivity of information to determine what must not be disclosed outside of OLG without proper authorization.

APPLICATION AND SCOPE

This policy applies to all OLG departments, sites, and employees.

DEFINITIONS

Employee: Any full-time, part-time, student or contracted individual who is granted access to OLG information.

Originator/Information Owner: The individual who is accountable and responsible for an information asset, typically an OLG business representative at the Director or Vice President level. The Information Owner must define and apply the appropriate label.

Information Assets: OLG information that is either stored or shared via any means, including cloud based services. This includes electronic information, information on paper, and information shared visually or verbally, such as by videoconferencing or by telephone.

Location: Refers to any location that may or may not be OLG physical property, but contains OLG information assets that an employee is responsible for (e.g. software at home).

Business Partner: Any entity, person, or company to which OLG has a contract to provide goods or services. In this policy's context, it is referring to entities which entrust OLG with their information.

Third Party Confidential: Information which OLG has in its possession, to which we are not the owner.

Encryption Technologies: Technology used to protect against a security breach that can endanger or expose OLG information by making information unreadable to non-OLG sources.

REQUIREMENTS

1. General

1.1. This policy includes, but is not limited to, information that is either stored or shared via any means, such as electronic information, information on paper, and information shared visually, by videoconference or by telephone.

1.2. All employees must familiarize themselves with this policy. It should be noted that the sensitivity levels defined within this policy are intended to emphasize and enforce common sense steps that every employee can take to protect all OLG information.

1.3. All OLG information assets are to be categorized into one of the classifications defined herein, and labeled with the designated classification where it is deemed appropriate and feasible by the Information Owner and the OLG Information Security Office. An Information Owner is defined as one who is accountable and responsible for an information asset, typically an OLG business representative at the Director or Vice President level.

1.4. The use of a default classification will provide a baseline approach for all information assets until they can be classified and labeled according to this policy.

2. Roles and Responsibilities

2.1. All OLG employees who have any access to OLG information and/or access to OLG computer systems are responsible for the protection of information that has been entrusted to their care. Employees are defined as any full-time, part-time, student or contracted individual who is granted access to OLG information.

2.2. The responsibility for defining the classification of an item of information (i.e., a document, a file or storage media) remains with the Information Owner.

2.3. It is the responsibility of any employee who locates any OLG information asset which is not secured according to its default label or its designated label to take action that is appropriate to the information asset. This includes, at a minimum, reporting the incident to the OLG Information Security Office.

3. Information Classification Categorizing

3.1. All OLG Information Assets are to be categorized into one of the information classification categories defined in the Information Classification Table.

3.2. The default classification for all OLG information assets is “Internal”.

3.3. All information assets which are not labeled “Public” must have an appropriate

level of access control.

4. Information Classification

4.1. The following table provides a description for each of the classification codes.

Information Classification Table	
Classification	**Description / Example**
Public	Non-sensitive information intended for public release. Information which is intended for the citizens of Ontario.
Internal	Sensitive information intended for OLG employees only. This is the assumed and default classification for all OLG information assets.
Confidential	Sensitive information intended for a specific subset or group of OLG employees. A subset of this classification is “Third Party Confidential”, meaning information that is entrusted to OLG by another party, such as a business partner or customer.
Restricted	Extremely sensitive information intended only for specific/individual OLG employees.

5. Labeling and Handling

5.1. All OLG information is to be labeled in an appropriate way that identifies its classification. This label must be applied in such a way that is clearly identifiable and consistent on all pages, sections or views of the information.

5.2. The Information Owner must apply the appropriate label.

5.3. Classification labels for information should be used in email messages and on printed material.

5.4. Users or recipients must maintain an assigned label.

5.5. Labeled information assets must be protected with a process and/or a mechanism that is appropriate to its sensitivity.

5.6. Secure storage of electronic or printed materials must be applied according to the classification of the information. This may include physical locks and approved encryption utilities.

5.7. The transmission and distribution of information must be done in accordance with its classification. This must include approved secure communication for transmission of OLG information.

5.8. Internet email messages (ie: messages sent from Lotus Notes to an internet email address) are considered public information. The internet based standard for transmitting email messages between parties does not incorporate any

access control.

5.9. The disposal or destruction of any OLG information asset should follow the OLG Standards for Data Destruction and Data Retention.

5.10. If any media contains information that relates to more than one classification, the label and any access controls will be based upon the more stringent of the classifications. For example, a diskette that contains both Public and Confidential information will be labeled as Confidential with the subsequent access controls for that classification.

5.11. The OLG labeling policy and process applies to any new/future information assets created as of September 1, 2007.

6. Compliance and Enforcement

6.1. OLG Information Security Office is responsible for the enforcement of all OLG Information Security Policies.

6.2. Policy violations will be dealt with accordingly.

Refer to Human Resources - Corrective Counseling and Discipline, HRPP-08-03.

6.3. Please note that any or all parts of this OLG policy may be superseded at any time by the Provincial or Federal levels of the Canadian Government.

7. Exceptions

7.1. The OLG Information Security Office is responsible for any and all exceptions to this policy any considerations for an exception must be forwarded to OLG Information Security Office for review and approval.

POLICY OWNER

Queries concerning this policy should be directed to the IT Service Centre or the Information Security Office.

REFERENCES AND FORMS

HRPP-08-03: Corrective Counseling and Discipline

REVISION / REVIEW HISTORY			
Date	**Requested By**	**Updated By**	**Summary of Revision**
22/11/2006	Danny Conte, IT Security Office	Dan O'Connor, IT Security Office	New policy
27/04/2007	Elaine Etcher, HR	Dan O'Connor, IT Security Office	Added reference for Corrective Counselling and Discipline Policy
11/12/2008	IT Security Office	IT Security Office	Annual Policy Review
21/11/2009	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Dec 2010	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Dec 2011	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Nov 2012	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Oct 2013	Corporate Policy Services	Corporate Policy Services	Reformat of policy template - AODA requirement
Nov 2013	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Nov 2014	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Dec 2015	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Nov 2016	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
July 2017	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
July 2018	Annual Policy Review	IT Security Office	Annual Policy Review
August 2019	Annual Policy Review	IT Security Office	Annual Policy Review
Sept 2021	Annual Policy Review	IT Security Office	Annual Policy Review

OLG Internal

Department/Stakeholder Review & Approval Signatures		
Department Approver	**Authorized Signature**	**Date**
Stephen Madden Sr Director, Security Architecture & Standards	Stephen Madden	Mar 07, 2007

OLG Internal