OLG CORPORATE POLICY

TITLE: **Disaster Recovery Management**

POLICY #:   **FP-04-06-001**

OWNER: **Risk Management & Compliance**

STATUS: **Final**

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 1

OLG Internal Use Only
OLG Internal

TITLE: Disaster Recovery Management

POLICY #: FP-04-06-001

OWNER: Risk Management & Compliance

STATUS: Final

_____

Table of Contents

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 2

TITLE:	Disaster Recovery Management
POLICY #:	FP-04-06-001
OWNER:	Risk Management & Compliance
STATUS:	Final

_____

PURPOSE

The overall purpose of this policy is to communicate the Disaster Recovery Management program, that protects Ontario Lottery and Gaming Corporation's (OLG's) ability to conduct business through recovery of critical data and systems in the event of a disaster.

APPLICATION AND SCOPE

This Policy applies to Ontario Lottery and Gaming Corporation (OLG) Information Technology employees, contractors, consultants and 3rd Party Vendors involved in the management of the Disaster Recovery process and related activities

POLICY STATEMENT

Disaster Recovery Plans must be implemented and maintained to meet business requirements and regulatory controls.

DEFINITIONS

Disaster: a natural, human, or technological event that causes a serious business disruption to operations. The event impacts access to the work area, records, files, and computer resources.

Disaster Recovery Plans: Disaster Recovery Plans (DRPs) address the recovery of OLG's technology and/or 3rd party technology services supplied for the continuation of information services and systems that support critical business functions, in the case of a disaster. Plans are pre-defined and tested annually.

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 3

DISASTER RECOVERY MANAGEMENT PROGRAM

The Disaster Recovery Management program provides a structured approach to ensuring reliability and availability of technology for OLG's critical business services and for regulatory compliance. The Disaster Recovery Management program follows COBIT best practice and is aligned with IT's Incident, Problem, Change, and Service Level Management.

PREPARATION AND MAINTENANCE OF DISASTER RECOVERY PLANS (DRP)

Disaster Recovery Plans (DRPs) for applications developed or hosted in-house, involve matching criteria identified by the business in Systems Development Life Cycle (SDLC) artifacts, to the appropriate DRP Profile Level (See reference - DRP Profiles document). This will be the basis by which the application and infrastructure will be designed.

Annual testing of critical systems ensures plans are accurate and staff have knowledge and experience with executing plans. Annually 3rd party vendors and or Service Providers must also provide evidence of successful DRP testing.   (See references – DRP-Attestation Guideline for Multi-sourcing and OLGs DRP Testing Guide for Gaming Service Providers)

A Disaster Recovery Plan test that does not meet the identified recovery objectives must have a re-test completed within two (2) months.

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 4

OLG Internal Use Only
OLG Internal

_____

RECOVERY PRIORITY

OLG IT has adopted an application centric recovery approach. As a result, each application has a specific Application Disaster Recovery Plan. A master listing of all applications and the sequence in which they would be executed in the case of a disaster, is included in the IT Master DRP document. The prioritization of the recovery is based on two criteria: 1.) Recovery Profile Level and; 2.) Disaster Scenario.

REPORTING

A DRP/FRP Readiness report will be issued to Business management for review on a quarterly basis and issued annually for approval.

ENFORCEMENT

Violation of this policy will be raised at - senior IT management level.

ROLES AND RESPONSIBILITIES

Chief Technology Officer is responsible for:
* Approval of this policy

Information Technology Vice Presidents and Executive Directors are responsible for:
* Ensuring an effective disaster recovery plans are developed and maintained for critical business systems within their areas of responsibility.

Executive Director of Information Security is responsible for:
* Ensuring an effective disaster recovery management process is developed and maintained

Sr IT Service Continuity Manager is responsible for:
* Ensuring an effective disaster recovery management process is developed and maintained, oversight, and timely reporting.

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 5

TITLE: Disaster Recovery Management

POLICY #:   FP-04-06-001

OWNER: Risk Management & Compliance

STATUS: Final

_____

VP IDS & IDS Directors and Functional Managers (DRP Owners) are responsible for:
- Ensuring compliance with this policy within their departments
- Allocating resources to support the preparation and management of Disaster Recovery Plans
- Executing critical plans to ensure staff are prepared and systems available in the event of a disaster

Project Managers & Vendor Compliance Managers are responsible for:
- Ensuring adhere to this policy,

- Ensuring new solutions meet business requirements

- Ensuring 3rd party solutions within their area of responsibility adhere to this policy

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 6

TITLE:	Disaster Recovery Management
POLICY #:	FP-04-06-001
OWNER:	Risk Management & Compliance
STATUS:	Final

POLICY OWNER

Policy Owner: Risk Management and Compliance
Responsible Officer: Chief Technology Officer
Contact: #IT Service Continuity

RELATED POLICIES AND PROCEDURES

FP 04-06-003 Structured Data Backup & Restoration Verification
FP 11-02-001 Business Continuity Management

REGULATORY CONTROLS

AGCO – Alcohol & Gaming Commission of Ontario Lottery & Gaming
ILC – Interprovincial Lottery Corporation

REFERENCES AND FORMS

Forms & Links may be updated from periodically and are provided here for convenience. Please check InsideOLG for updates.

- Disaster Recovery Profiles
- DRP Attestation Guidelines for Multi-sourcing
- OLGs DRP Testing Guide for Gaming Service Providers

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 7

TITLE: Disaster Recovery Management

POLICY #: FP-04-06-001

OWNER: Risk Management & Compliance

STATUS: Final

_____

POLICY REVIEW DATE

REVISION / REVIEW HISTORY			
Revision Date - Version	**Requested By**	**Updated By**	**Summary of Revision**
May 2020	Steve Madden	D.Conte	• Added Re-testing time, and annual DR Readiness approval by business.
May 2019	Dale Kingsley, Sr Security Risk & Service Resilience Manager	Dale Kingsley	• As per Steve Madden, removed time reference language • Updated header to reference Function Policy • Added reference documents (OLGs Testing Guide for Gaming Service Providers), • Updated role titles
July 2017	Dale Kingsley, Sr Manager, Service Continuity	Dale Kingsley	• Updated policy to proper template • Added regulatory section • Removed requirements that limit innovation and agility
March 5, 2015	Dale Kingsley, Sr Manager, Service Continuity	Dale Kingsley	• Updated reference to CP 04-06-003 Data Backup and Restoration Verification name change.

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 8

TITLE: Disaster Recovery Management

POLICY #:   FP-04-06-001

OWNER: Risk Management & Compliance

STATUS: Final

_____

APPROVALS		
Department Approver	**Authorized Signature**	**Date**
Brian Gill Chief Technology Officer		
Stephen Madden Executive Director, IT Risk Management & Planning		

EFFECTIVE: **June 6, 2006**	REVISED: **May 2020**	SUPERSEDED #: **SC 05-002 (partial) & SC 05- 003**	PAGE # 9

OLG Internal Use Only
OLG Internal