Business Resilience Management Policy

POLICY #FRA-04-02

FINAL

PURPOSE

OLG's Business Resilience Management (BRM) Policy, in conjunction with OLG's IT Disaster Recovery Management Standards and OLG Emergency Response Plans, ensures that activities enacted during a time of crisis or unplanned disruption are coordinated and implemented in a controlled manner that reduces negative impact to OLG.

APPLICATION AND SCOPE

This policy applies to all employees.

POLICY STATEMENT (& GUIDING PRINCIPLES)

OLG is committed to safeguarding the health and safety of its employees and customers, protecting its assets and ensuring continuation of critical operations. OLG's BRM program enables resumption of critical business processes following a crisis or unplanned disruption to ensure return to normal business operations.

DEFINITIONS

Business Continuity: the capability of an organization to continue delivery of products and/or services at acceptable, predefined levels following a disruptive incident or disaster.

Business Resilience Management (BRM): the holistic management process that identifies potential threats to an organization, and the impact to business operations that those threats, if realized, might cause. It provides the framework for building organizational resilience, with the capability of an effective response that safeguards the interests of its key stakeholders, and its reputation, brand, and/or value-creating activities.

Business Continuity Plan (BCP): the documented procedures that guide the organization to respond, recover, resume, and restore to a pre-defined level of operation, following a major business disruption or disaster. The BCP includes **Operational Pandemic Plans (PP)** document procedures to guide, respond and restore the organization to a Global or National Health Emergency and/or a Pandemic declaration.

Crisis: an abnormal or unstable situation that threatens the organization's strategic objectives, reputation, and/or viability.

Crisis Management: the holistic management process to develop and apply a response strategy to effectively deal with crises.

Emergency Response Plans (ERP): the documented procedures that guide the organization to immediately act to preserve lives and/or safeguard property and assets.

Incident: any situation that might be, or could lead to, an emergency, a crisis, a disruption in services, and/or a loss of services.

IT Disaster Recovery Plan (DRP): the documented procedures that guide the organization to enable recovery of OLG's Technology (and/or third-party technology services supplied), for the continuation of information services and systems that support critical business functions.

REQUIREMENTS

Business Continuity Planning

1.1. Establish Business Continuity Plans for critical business activities:

1.1.1. Lines of Business and Shared Services are required to complete a threat and/or risk assessment to identify key risks and critical operational processes.

1.1.2. Lines of Business and Shared Services must document and evaluate the impacts of a worst-case disaster scenario on critical business activities, resources, technology, and vital records in a Business Impact Analysis (BIA) annually and ensure appropriate processes and response strategies are captured in a Business Continuity Plan (BCP).

1.2. Implement and operationalize Business Continuity Plans:

1.2.1. Lines of Business and Shared Services notify critical resources of their role in a BCP. Employees are required to participate in regular training, testing, and exercising of plans to ensure adequacy of the response strategy.

1.2.2. Management is required to invoke and deactivate relevant ERPs, BCPs and DRPs.

Incident Management Response

2.1. Activate Emergency Response Plan:

2.1.1. OLG Corporate Security will initiate ERPs in the event of an emergency. Employees will follow Corporate Security direction to ensure employee and customer safety and protection of OLG's assets.

2.2. Triage and Escalate Incident:

2.2.1. Lines of Business and Shared Services review and escalate incidents according to OLG's criticality criteria.

2.2.1.1. If an incident is deemed a crisis, it is immediately directed to OLG's Crisis Manager to engage OLG's Executive Crisis Management Team.

2.2.1.2. If incident is not a crisis and can be resolved through regular incident management processes, management will continue to do so to resolution. As resolution progresses, and it is not possible to recover operations / systems within the timelines required, the incident will be escalated to the Crisis Manager.

2.3. Activate Plans (as appropriate):

2.3.1. Management will invoke and employees will follow relevant BCPs and DRPs during any unplanned disruption or crisis event and communicate status updates to key stakeholders throughout the incident until normal operations have been resumed.

2.4. Engage in Corrective Action:

2.4.1. Lines of Business and Shared Service collaborate with Business Resilience to identify and document any gaps or issues identified with invoked ERPs, BCPs, and DRPs on an After Action Report (AAR).

2.4.2. Business Resilience provides an incident debrief to Executive Management.

Continuous Improvement

3.1. Monitor and Review Plans

3.1.1. Lines of Business and Shared Services review and approve BCPs annually or when material changes to critical activities occur.

3.2. Improvement

3.2.1. Lines of Business and Shared Services create and implement action plans based on gaps identified through AARs, testing, reviews, incidents, or as new standards are developed, to ensure the business can successfully recover in the event of a future disruption.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
OLG employees	▪ Execute role requirements in event of BCP activation.
President and Chief Executive Officer (CEO)	▪ Accountable for Business Continuity Management across OLG.
Executive Crisis Management Team	▪ Declare a crisis and provide direction to Crisis Managers, and OLG management during a crisis. ▪ Close the crisis.
Divisional Vice Presidents/Directors	▪ Ensure BIA, BCP, and PP development, response strategies, exercises, education, training and improvement plans are completed. ▪ Appoint a Business Continuity Coordinator.
Business Resilience	▪ Develop BRM strategy, framework, oversight, and facilitation of OLG Business Resilience and Crisis Management Programs.
Business Continuity Coordinators (BCC)	▪ Manage business continuity critical activities during a crisis and liaison between the division and Crisis Manager/Business Resilience. ▪ Train and test required staff, promoting and maintaining business continuity and pandemic awareness.
Business Continuity Plan Owners	▪ Document, implement, train, test, maintain, and approve BCPs. ▪ Invoke BCPs when a business disruption occurs.
Crisis Managers	▪ Monitor events and escalate to the Executive Crisis Management Team in accordance with OLG's crisis criteria. ▪ Communicate crisis declaration and manage responses from BCCs, while providing updates to the Executive Crisis Management Team. ▪ Participate in debrief sessions to review incidents and/or crisis events to discuss and identify gaps for improvement.

RELATED POLICY INSTRUMENTS

- Disaster Recovery Management Standards
- OLG Corporate Security Services: Emergency Information Guides

POLICY OWNER

Director, Business Resilience

POLICY APPROVAL

Approver	Date
Lori Stanghetta, VP Risk Management	October 22, 2022
SVP Risk & Audit	September 30, 2019
Risk, Compliance and Audit Committee	September 30, 2019

REVISION / REVIEW HISTORY

Revision / Review Date	Updated By	Summary of Revision / Review
October 18, 2022	Business Resilience	▪ Updated to new Policy Template and review ▪ Supersedes Business Resilience Management Policy #CP-11-02-001
September 30, 2019	Business Resilience	▪ New Corporate Policy