Fraud Risk Management Policy

POLICY #FEA-04-01

FINAL

PURPOSE

This policy sets the requirements for OLG employees to minimize the risk of fraud which is essential to upholding OLG's reputation and safeguarding the trust of our customers, employees, partners, charities and Ontario government.

APPLICATION

This policy should be read and followed by all OLG employees and applied in conjunction with other OLG policies, including OLG's Code of Business Conduct (the "**Code**") and those related to compliance & ethics.

POLICY STATEMENT

All employees play a role in preventing, detecting, and reporting fraud. Employees are expected to report any suspicious or unusual activity to their managers, supervisors, People & Culture, or through Integrity Matters (OLG's confidential, anonymous whistleblower program).

DEFINITIONS

Fraud: Fraud is the vulnerability that OLG faces from individuals obtaining an unjust or illegal advantage through intentional deceit, falsehood, concealment, breach of trust or other fraudulent means which negatively affects OLG's financial, reputational, legal and/or other business interests.

Individuals committing fraud can include OLG employees, vendors, retailers, customers, or others outside of the organization.

Fraud can occur in many different operational areas at OLG and evolve with our business. Common types of *internal* fraud that OLG may face include, but is not limited to:

Asset Misappropriation	Fraudulent Statements	Corruption
Theft of cash (skimming of revenues or receivables)	*Improper revenue recognition* (inappropriately recognizing revenue in one period that should be recorded in another)	*Personal interests* (collusion with customers and/or vendor)
Payroll (false workers' compensation claims, falsified expense reports)	*Misstatement of assets, liabilities and/or expenses* (understating loans and payables)	*Conflicts of interest* (hiring someone close to them over another more qualified applicant)
Billing schemes (recording false credits, rebates or refunds to customers)	*Accounting misstatements* (misrepresentation of suspense accounts for fraudulent activity)	*Insider trading* (using business information not released to the public to profit on supplier stock)
Procurement (sale of critical bid information, contract details or other sensitive information)	*Non-financial* (falsified employment credentials e.g., qualifications and references)	*Kickbacks* (employee receives payments from vendor in exchange for business advantages)

Common types of *external* fraud that OLG may face include, but is not limited to:

Customers	Vendor	Criminals
Misrepresentation of personal information (intentionally using another name, address, age)	*Supplier misrepresentation of information* (intentionally misrepresenting experience, revenues, assets, liabilities)	*Cybercrime* (using computers and networks for phishing, ransomware, impersonation)
Theft or forgery (identity theft, stolen credit cards, bank cards, forged documents)	*Bid-rigging* (collusion between competing vendor during bidding process)	*Counterfeiting* (deliberate attempt to imitate currency, credit cards, another person's identification)
Cheat at Play (subverting the rules through player and staff collusion, card counting, bonus abuse)	*Payments* (requesting payment for goods or services not supplied)	*Cheat at play* (subverting the rules through player and staff collusion, software or bots)
Chargebacks (stolen credit card used on iGaming platform and legitimate cardholder requests a refund, or registered player loses money and requests a refund)	*Overbilling* (invoicing at a higher price than the quality or complexity of the work performed)	*Money laundering* (ill-gotten money is converted to gaming currency, then back to clean money)

CONFIDENTIALITY AND PROTECTION FROM REPRISAL

Employees do not have to be certain of fraud before reporting suspicious or unusual activity but must make all reports in good faith. If it is found that the employee made a false report maliciously or in bad faith, the employee may be subject to corrective and/or disciplinary action up to termination of employment.

As outlined in the **Code**, OLG provides protection from reprisal for all reports made in good faith. All reports are investigated by OLG's Corporate Investigations team. Investigations will be carried out on a must-know and need-to-know basis except where the interests of fairness require otherwise.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
OLG Employees	▪ Comply with this Policy and related policy instruments (outlined in the following section) ▪ Participate in mandatory fraud risk management training ▪ Understand fraud risks and controls relevant to position ▪ Report any suspicious or unusual activity immediately to manager, supervisor, People & Culture or through Integrity Matters ▪ Maintain confidentiality during an investigation, whether participating in an investigation or the subject of the investigation
OLG Management	▪ Identify and familiarize yourself with types of fraud that could occur within areas of responsibility ▪ Design and execute controls that address identified fraud risks. This includes identifying fraud risks to which procedures and systems are exposed; developing and maintaining effective controls to prevent and detect fraud; and ensuring that controls comply with the *Fraud Risk Management Framework* which outlines an approach to identify, assess, mitigate and monitor fraud risks

ROLE	RESPONSIBILITIES
	▪ Be alert for any indications of irregularities in financial transactions, business reports or other business activities
Executive Leadership Team (ELT)	▪ Promote this policy, including the role of all employees to prevent, detect and report fraud ▪ Ensure operational policies and processes are in place to enable the management of fraud risks within area of responsibility ▪ Report any fraud risk indicators and/or actual fraud matters to the Operational Risk Management department on a regular basis (quarterly or more frequently) ▪ Report all fraud-related incidents annually to support the MOU attestation ▪ Ensure timely resolution of any deficiencies or gaps in the fraud risk management control environment within area of responsibility
Operational Risk Management	▪ Develop, review, and update this Policy and *Fraud Risk Management Framework* ▪ Provide guidance on the implementation of this policy, and the *Fraud Risk Management Framework* ▪ Lead the development of fraud risk management training ▪ Consolidate, escalate, and report all fraud risk matters to the VP, Risk Management
Vice President, Risk Management	▪ Review and report any significant fraud risk matters, including reports of fraud and deficiencies in the fraud risk management program ▪ Establish and communicate fraud risk management policy and practices ▪ Ensure timely resolution of any gaps in OLG's enterprise fraud risk management program

RELATED POLICY INSTRUMENTS

- Anti-Money Laundering Policy
- OLG Code of Business Conduct
- Conflict of Interest Rules
- Ethics & Compliance Management Policy
- Insider Trading and Tipping Prevention Policy

POLICY OWNER

Senior Director, Operational Risk

POLICY APPROVAL

Approver	Date
VP, Risk Management	October 26, 2022
SVP Risk & Audit	February 5, 2020

REVISION / REVIEW HISTORY

Revision / Review Date	Updated By	Summary of Revision / Review
August 2022	Operational Risk Management	▪ Updated to new Policy Template and review ▪ Supersedes February 2020 Fraud Risk Management Policy