Acceptable Use of IT Resources Policy

POLICY #ET-05-03

FINAL

PURPOSE

The purpose of this policy is to outline the acceptable, responsible, and secure use of the information and information technology (I&IT) in Ontario Lottery and Gaming Corporation (OLG). It is intended to protect the company's information and information technology resources against illegal or damaging actions by employees, either knowingly or unknowingly.

APPLICATION AND SCOPE

This policy applies to all OLG employees, contractors, and authorized users who interact with OLG systems, networks, information owned by or entrusted to OLG, data, and all information technology owned or leased by OLG.

DEFINITIONS

Authentication: The process of verifying the identity of people, applications, and services before giving them access to digital systems and resources. Typically, a logon prompt initiates the authentication process, but it can take many forms.

Company: Refers to Ontario Lottery and Gaming Corporation (OLG).

Employee(s): Includes full-time, part-time and temporary employees, contractors and 3rd party service providers employed to perform work or are granted access to OLG's IT network and resources.

Non-business: Refers to websites or data that are either personal in nature or unrelating to one's job or employment with OLG.

Malware: Any software intentionally designed to cause disruption to a computer, server, client, or computer network and enact a breach or leak to private/confidential information, gain unauthorized access to information or systems, deprive access to information, or knowingly interferes with a user's computer integrity or security in any form.

Password/ Passphrase: A memorized secret consisting of a sequence of words, symbols or other text that authenticates a user to a computer system or application. A passphrase is similar to a password in usage but is generally comprised a string of words as a phrase for added security.

Phishing: A form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

Ransomware: A type of malware that blocks access to data or systems until a specific set of criteria is met such as a ransom demand.

Spam: Categorized as unsolicited or potentially unauthorized messages that may be harmful to a system or network.

REQUIREMENTS

1. Ownership & Access

1.1. OLG's information technology (IT) - such as computer equipment, software, operating systems, storage media, network devices and cloud services - are intended for OLG business use.

1.2. All information, including email messages, created, or stored on OLG's IT resources, including back-ups, are company property.

1.3. All requests for access to OLG information and IT must follow a defined, auditable process. The process must specify the required level of authorization.

1.4. OLG may, at its discretion, limit or deny:

- installation and use of software;
- installation and/or the use of computer hardware, devices or peripherals;
- access to certain websites and/or applications;
- end users' ability to install software, and/or alter system configuration settings

1.5. OLG employees must not attempt to bypass or otherwise circumvent any access restrictions.

2. Confidentiality, Data & Privacy

2.1. Employees have **no expectation of privacy** when using OLG information technology resources. OLG monitors all information technology usage, including intercepting and reviewing personal and business communications for the following purposes:

- As part of OLG's Data Loss Prevention (DLP) program to ensure sensitive OLG data such as Personal Information is properly protected and only leaves OLG's ecosystem for authorized business purposes.
- Troubleshoot hardware and software problems;
- Prevent unauthorized access and system misuse;
- Retrieve business related information;
- Investigate possible violation of any OLG Policy or Standard, including this policy, or local, provincial or federal laws;
- Comply with legal requirements;
- Reroute or dispose of undeliverable mail;
- Perform information technology administration;
- Provide information for employee conduct reviews;

2.2. Data & Privacy (Refer to OLG's Data Classification and Handling Policy and Procedures for details)

- Data Handling: OLG data is the property of OLG, including OLG customer and employee personal information, and must be handled in accordance with OLG Policies and Procedures. Special care must be taken for sensitive data. The use of Personal Information is restricted and OLG's Protection of Privacy Policy must be followed.
    - Do not receive, send or store Personal Information in an email system – whether your OLG email address or a shared address. Consult with your Enterprise Information Technology contact to assess alternatives for sending and receiving personal information securely. If an alternative is not immediately available and you must receive, send or store personal information through email, please follow any mitigations recommended by Enterprise Information Technology, follow your line of business risk acceptance process, and develop an action plan to implement a secure alternative. .
- Data Classification: Label OLG Data according to its sensitivity level (e.g., public, internal, confidential, restricted). If you aren't sure, ask your manager for guidance.

- Data Retention: Read, understand, and follow OLG retention policies. Emails that are records, including any attachment(s) must be saved to a secured shared drive or SharePoint site on an ongoing basis. **Attesting to this Acceptable Use Policy confirms you have saved all emails that are records appropriately up to the date of this attestation.**

3. Email and Internet

3.1. When using OLG information technology, you are accountable for your actions. Be vigilant and cautious of suspicious emails containing links and/or attachments as they can allow threat actors into OLG's infrastructure, allow them to steal data, or cause a ransomware event at OLG. Be careful when sending information via email or sharing information to ensure the person you are sending the information to is authorized to view it and that you have the right contact name.

3.2. Participate in OLG education opportunities that provides guidance for safe cyber practices.

3.3. It is unacceptable to use OLG information technology for the following purposes:

- Post, transmit or distribute information that constitutes or encourages a criminal offense or civil liability;
- Use unapproved Internet-based (cloud) channels to send or upload non-public information. This includes your personal email account or your personal cloud storage;
- Upload OLG Data into an untrusted artificial intelligence (AI) platform such as ChatGPT. If you aren't sure which ones can be trusted, please contact Connect;
- Use OLG information technology to restrict or inhibit any other user from using the information technology, in whole or in part;
- Access personal web-based email systems (such as Gmail, Hotmail, or Yahoo email), either directly or through indirect channels (such as anonymous proxies);
- Send spam emails, email bombs or abuse the email system in any other way;
- Send emails, documents or software programs containing malicious software (malware);
- Distribute digital materials that are:
    - protected by copyright or other intellectual property rights without prior authorization from the rights holder(s);
    - considered defamatory, obscene, sexually explicit, child pornography, hate literature, or otherwise illegal;
    - an invasion of privacy, appropriation of personality, or unauthorized linking or framing.
    - **Note:** OLG reserves the right to remove any such information, software or material from its IT resources.
- Use information technology for private business activities, amusement, or entertainment purposes, to distribute hoaxes, chain letters, personal or private advertisements. Email messages concerning non-OLG business must not be sent, forwarded, or replied to using large email distribution lists.
- Use information technology in such a way to be considered harassment or which may contribute to a hostile work environment, as defined by the Non-Discrimination Procedure in the Human Resources Policies, Practices and Procedures Manual. Profanities, obscenities, derogatory or defamatory remarks must not be used in email messages. Refer to OLG's People & Culture policies for further guidance.
- Misrepresent, obscure, suppress, or replace one's identity in email messages. The digital signature of each employee must reflect the actual originator of the email.
- Misrepresent oneself to external people as an official agent or representative of OLG and to state the company's views on topics related to the business while participating in discussion groups, chat rooms, and other public internet forums, unless it is in one's job responsibility and expressly authorized in writing by an OLG Executive. For additional information please refer to the OLG Code of Business Conduct.
- Access non-business websites that may constitute legal liability, embarrassment for the company or other legal issues.

- Results in a violation of any OLG Policy or Standard;
- Anyone who discovers that they have connected with a website that contains inappropriate material or causes their OLG equipment to misbehave in any way must immediately disconnect from that site and call Connect for further guidance. The ability to connect with a specific website does not in itself imply that employees are permitted to visit that site.

3.4. Incidental personal use of OLG information technology is permissible if it:

- Does not consume more than a trivial amount of resources;
- Does not interfere with the employee's productivity or with work being performed by another employee;
- Does not preempt any business activity;
- Is not for pay or profit;
- Does not violate software licensing agreement;
- Does not expose OLG information and/or information technology to security risks;
- Complies with the other provisions of this policy.

4. Account and Password Management

4.1. Employees must protect their account passwords/passphrases, maintain account confidentiality, secure authentication devices, and monitor account activities. If you suspect an account has been compromised, immediately report it to Connect. You are responsible for your OLG account.

4.2. Passwords/passphrases must comply with the Password Management Policy.

5. Anti-Virus and Endpoint Protection

5.1. The current company-approved anti-virus and endpoint protection software is installed, running and updated on each employee workstation. Employees may not block this software from running or updating.

5.2. Email attachments may only be opened if they are expected and originate from a known and trusted party. Immediately contact Connect if you believe you opened a malicious document or clicked a malicious link in error. Seconds count.

6. Equipment

6.1. OLG issued devices must never be left unattended while users are logged in. Users must either log out or invoke a password-protected screensaver before leaving them unattended.

6.2. Logging in or using any OLG computer equipment for which users are not authorized for is prohibited, except for authorized IT Support personnel for troubleshooting purposes only.

6.3. Employees must take reasonable precautions to protect and secure their laptops and mobile devices, removable storage media, and other portable computer equipment, especially those containing non-public information. OLG provides the tools and technology to protect and secure portable computer equipment and the information stored in them. Contact Connect if you have a need to transfer sensitive information and you aren't sure how to do it.

6.4. All OLG corporate computers (laptops and other multi-user workstations) must be connected to the OLG corporate network for at least once every 30 days via in-office connection or via Virtual Private Network (VPN). This will ensure all necessary security patches and anti-virus software updates are downloaded and installed. If an OLG computer does not connect to the network for more than a month, the computer may be rendered unusable without notice.

6.5. Employees must inform their manager and the Information Security Office if they intend to take their OLG issued device out of Canada to prevent unnecessary account or device locks. If longer than a week, your HR Business Partner must also be informed.

7. Software

7.1. Only employees who are authorized by their roles or job functions are permitted to add, change, remove or copy software from OLG computers. All other employees are prohibited to install unlicensed or unauthorized software on OLG computers. Refer to the Software License Compliance Standard.

7.2. The following categories of software are prohibited from being installed and/or used on any OLG workstation or 3rd party computers unless authorized specifically by the Information Security Office:

- Any network sniffing tool, or tool which captures network packets;
- Any hacking tool which can be used for malicious purposes; such as network scanners or denial of service tools;
- Any software which creates or can create a hidden or covert communications channel, or provides remote access;
- Any software which can brute force or otherwise crack passwords;
- Any software which is part of a peer to peer or file sharing community, such as torrents;
- Any software which encrypts files or folders;
- Any software which is known or deemed to be malicious, and or harmful to OLG or weakens its security posture or could place OLG at undue risk.

8. Contractors and Third-Party Service Providers

8.1. Third-party service providers must not use their own unapproved computing equipment on the OLG network due to security risks and potential system impact. Approval can be obtained through the Information Security Office. Refer to *Information Technology – Third-Party Access Standard*.

ROLES & RESPONSIBILITIES

ROLE	RESPONSIBILITIES
OLG Employees & Third Parties	▪ Must comply with this policy and not circumvent, violate, or cause this policy to be violated.
OLG Information Security Office	▪ Responsible for the enforcement of all OLG Information Security Policies.

RELATED POLICY DOCUMENTS

- OLG Code of Business Conduct
- OLG's People & Culture policies
- Cybersecurity Policy (future, currently Anti-Virus and Malicious Code)
- Password Management Policy
- Third-Party Access Technology Standard
- Software Licence Compliance Technology Standard
- Freedom of Information and Privacy Legislation
- Information Classification and Handling Policy
- Enterprise Information Governance Technology Standard
- Data Ethics and Responsible AI Technology Standard
- Generative AI Technology Standard

POLICY OWNER

Director, Cybersecurity Operations

POLICY APPROVAL

Approver	Date
Graham Reed, VP Cybersecurity & Information Security Officer	May 13, 2024
Original policy approved by Executive Committee	July 12, 2010

REVISION / REVIEW HISTORY

Revision / Review Date	Updated By	Summary of Revision / Review
March 13, 2023 - May 2024	Policy Services, Cyber Security & IT Risk team	▪ Updated template with minor revisions to modernize including for Privacy, Retention, Artificial Intelligence, and others. ▪ Added Roles and Responsibilities table, definitions of phishing, password/ passphrase and other, updated related policy instruments section. ▪ Updated job titles based on new Operating Model. ▪ Reviewed by Legal and P&C. ▪ Supersedes Acceptable Use of Information Technology Resources Policy #CP-04-05-001