Password Management Policy

POLICY #ET-05-01

FINAL

PURPOSE

To establish the Ontario Lottery and Gaming Corporation (OLG) guiding principles and requirements for the management of passphrases.

APPLICATION AND SCOPE

This policy applies to all OLG employees, all OLG managed systems regardless of network location, and to 3rd party service providers responsible for managing OLG user accounts. This policy does not apply to OLG public / customer facing systems.

POLICY STATEMENT (& GUIDING PRINCIPLES)

Passphrases are the front line of protection for user accounts. A poorly chosen passphrase may result in the compromise of OLG's entire corporate network and/or a significant data breach.

All passphrases used to protect OLG systems or grants access to the OLG network shall be appropriately configured, periodically changed, securely transmitted, and limited to the period of its authorized use.

DEFINITIONS

UserID: Is a sequence of characters that identifies a user when attempting to access a computer system. Sometimes referred to as a username.

Passphrase: A memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage but is generally longer for added security.

Multifactor Authentication: Multifactor Authentication provides additional assurance the person logging in is who they say they are. Defined as any combination of:

1. Something you have (OLG laptop)
2. Something you know (password)
3. Something you are (fingerprint)

REQUIREMENTS

1. **General**
   - 1.1. Each OLG employee with access to OLG systems must take the appropriate action, as outlined in this policy, and other relevant policies to select, manage and secure their passphrase.
   - 1.2. Passphrases and accounts must conform to OLG's Account and Passphrase Standard.
   - 1.3. OLG information security may as a result of a suspected or real threat to the security, integrity, or availability of OLG's computing platform disable, suspend or alter any account or passphrase.
   - 1.4. Multifactor authentication is required to provide an additional assurance of the identity of the authorized user.

1.5. Any suspected incident of account or passphrase compromise must be reported to the IT Service Centre. Passphrases must be changed immediately.

2. **Communicating and Storing Passphrases**

2.1. Privileged and high-risk accounts must be securely stored for authorized use only within an ISO approved storage facility and comply with standard SD3.08.01.01-03 – Privileged Password Management

2.2. Passphrases and UserID's must not be communicated externally within the same email message or other form of electronic communication without authorization from the ISO.

2.3. Passphrases must be memorized or stored in an authorized password vault. Passphrases must never be stored in an unsecured form such as written down on paper or in a spreadsheet.

3. **Enforcement**

3.1. The Information Security Office or its delegates will perform passphrase audits on a periodic and random basis. If a weak or inappropriate passphrase is identified during an audit, the user will be required to change it.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
Information Security Office	▪ Ensuring the compliance and enforcement of this policy. ▪ Ensuring that passphrases are resistant to compromise.
OLG Employees & Third Parties	▪ Must comply with this policy and not circumvent, violate, or cause this policy to be violated. ▪ Ensure passphrases are in their possession and their use is secured.

Queries concerning this policy should be directed to the IT Service Centre.

RELATED POLICY INSTRUMENTS

- Information Security Architecture & Standards

POLICY OWNER

Director, Technology Security

POLICY APPROVAL

Approver	Date
Chief Technology Officer	November 10, 2022

REVISION / REVIEW HISTORY

Revision / Review Date	Updated By	Summary of Revision / Review
March 24, 2022	Policy Services and ISO	▪ Updated sections for clarity ▪ Supersedes Password Management Policy #CP-04-05-01