IT Technology Standard SD 0049-01 Account and Passphrase Standard

Enterprise Technology

1. Overview

Accounts and passphrases are the primary method of securing access to OLG information. Poor passphrase management techniques increase the risk of both system and OLG data compromise. Standards for the creation and management of passphrases greatly reduce these risks.

2. Account and Passphrase Technical Safeguards

2.1. This document shall define the types and attributes for passphrases and uses including but not limited to:

- 2.1.1. Account types and definitions
- 2.1.2. An automatic lock-out feature must be applied that will disable accounts that have excessive failed login attempts
- 2.1.3. Passphrase expiry, strength, history, complexity and other associated control expectations and attributes
- 2.1.4. Additional safeguards for high-risk accounts

2.2. Unnecessary accounts must be disabled and removed within three days.

2.3. Access to the OLG Network via remote access requires stronger authentication and is governed by the OLG Remote Access Policy.

2.4. Information Security Office may limit, deny, or add additional controls for access from any untrusted network.

2.5. Account use events must be recorded and retained according to retention policies.

2.6. Authorized applications must adhere to the OLG Identity Management standard to ensure accounts are appropriately managed.

2.7. Interactive Account use must be attributable to named authorized OLG individuals.

3. Departure of Personnel

3.1. Privileged account passphrases must be immediately changed upon departure of personnel (mandatory or voluntary) or suspected compromise of the passphrase.

3.2. User accounts must be immediately disabled upon departure of personnel (mandatory or voluntary).

4. Default Passphrases

4.1. Passphrases for administrative access to network infrastructure devices must be defined as something other than the standard defaults, for example SNMP community strings of "public", "private" and "system", and must not be the same as the passphrase for LAN IDs.

4.2. Accounts on a system must be reviewed prior to go live, and any unnecessary accounts removed.

4.3. New passphrases must be immediately implemented on all systems upon installation.

5. Disposal of Equipment

5.1. All user accounts and passphrases must be removed / erased from IT equipment prior to disposal or decommissioning, in accordance with SD5009 - Secure Data Removal.

6. General User Requirements

6.1. Passphrases must be memorized and never written down.

6.2. A minimum passphrase length of 12 alphanumeric characters.

6.3. At least three of the following four types of characters:

- Uppercase letter
- Lowercase letter
- Number
- Symbol (ie. !,@,#)

6.4. Passphrase cannot be one single dictionary word in any language. (eg. Triangle)

6.5. Passphrase must not have 3 or more repeating characters. (eg. Rectangle**aaa**123)

6.6. Passphrase must not be on a known breach list.

6.7. Passphrase expiry must be annual as a minimum and must never be reused.

6.8. Account lockout must occur after 10 invalid login attempts within a 30-minute period. The account automatically unlocks 30 minutes after the last invalid login attempt is made. Higher risk systems may require administrative action for an unlock.

6.9. Systems and/or applications must be assessed by ISO to ensure appropriate controls in place commensurate with the risk of the application.

7. Additional End User Specifications (Controls managed by ISO, Operations, and Business Account Managers)

7.1. Passphrases are set as pre-expired when accounts are created or during an administrative reset. This will force users to reset upon first log in.

7.2. Mandatory multifactor authentication. (see OLG's MFA standard which can include but is not limited to an OLG network location, an OLG laptop, OKTA verify)

7.3. Unused accounts must be deactivated and/or deleted after a grace period of 90 days.

7.4. The same User ID is used on all OLG accounts assigned to an employee with OLG's active directory being the source for other applications to follow.

7.5. Users requiring administrative rights across multiple Windows systems require the use of a separate account created by ISO.

7.6. Accounts must be assigned to employees for specific applications on a one-to-one basis. A user having multiple accounts on a single system is considered an exception that must be reported to and approved by the Information Security Office.

7.7. The construction of usernames for end user accounts must follow these rules:

7.7.1. The username is generated using the first initial and last name of the account owner.

7.7.2. In the event there is a conflict with an existing username then the first two letters of the first name are used and prepended to the last name. This is repeated until letters from the first name are used up, followed by the entire alphabet.

7.8. Systems that are not integrated into OLG's Identity framework must have additional safeguards applied such as IP restrictions or other form of approved MFA.

7.9. If an application cannot meet one or more of the technical requirements above, then ISO will establish a risk-based solution.

8. Service Account Passphrase Requirements (Intended for Service/Application owners)

8.1. Service accounts are used to run a service such as a bind account, windows service account, or within a scheduled task. While not intended to be used interactively, some use cases may require this privilege to function properly.

8.2. All Service accounts must be approved by the Information Security Office prior to implementation and assigned to an appropriate custodial department. A documented business case is required for each service account request. They may be interactive or non-interactive, although interactive use should be rare.

8.3. Service account usernames must follow a naming convention such that its intended purpose is clear. All Service accounts must be documented by the ISO.

8.4. Service accounts are managed by an appropriate custodial department (usually application support) including reset requirements as necessary. Custodial department must maintain procedures for resetting, as well as ensure disaster recovery environments are updated. Custodial department will have the account removed from all systems when no longer required.

8.5. Service account passphrases must be securely stored for authorized use only within an ISO approved storage facility. See standard SD3.08.01.01-03 – Privileged Password Management for more information.

8.6. Interactive use of Service accounts must be attributed to an individual.

8.7. Interactive use of a Service account requires a passphrase reset. Exceptions must be approved by the ISO.

8.8. Minimum length of 20 alphanumeric characters including at least one lower case, one upper case, a number, and a special character.

8.9. Passphrase must not have 3 or more repeating characters.

8.10. Minimum passphrase age is 0. Users are allowed to perform subsequent passphrase changes immediately after an initial passphrase change.

8.11. A passphrase must not be re-used.

8.12. Account lockout occurs after 10 invalid login attempts within a 30-minute period. The account automatically unlocks 30 minutes after the last invalid login attempt is made. Some systems may require administrative action for an unlock, depending on risk.

8.13. Non-Interactive service account passwords do not expire.

8.14. Publicly accessible service accounts must have additional safeguards applied such as IP restrictions or other form of approved MFA.

8.15. If a service account cannot meet one or more of the technical standards above, then ISO will establish a risk-based solution.

9. Shared Account Passphrase Requirements (ie. OLG Social Media, Application Owners)

9.1. Shared accounts are used for a group of individuals to support an application or a system. They are typically used to simplify account management and are interactive in nature. Default administrative accounts would also fall into this category, however hardening best practices must also apply.

9.2. All shared accounts must be approved by the Information Security Office prior to implementation and assigned to an appropriate custodial department. A documented business case is required for each shared account request.

9.3. Shared accounts are managed by an appropriate custodial department (usually application support) including reset requirements as necessary. Custodial department must maintain procedures for resetting, as well as ensure disaster recovery environments are updated. Custodial department will have the account removed from all systems when no longer required.

9.4. Shared account usernames must follow a naming convention such that its intended purpose is clear. All shared accounts must be documented by the ISO.

9.5. Interactive use of Shared accounts must be attributed to an individual.

9.6. Shared accounts must have a minimum passphrase length of 12 alphanumeric characters.

9.7. Passphrase cannot be a single dictionary word.

9.8. Passphrase must not have 3 or more repeating characters.

9.9. Shared account passphrases must be securely managed for authorized use only within an ISO approved storage facility. See standard SD3.08.01.01-03 – Privileged Password Management for more information. Other controls such as dual approval or session monitoring may be required based on risk.

9.10. Shared account passphrases must not be shared with more than one individual at a time.

9.11. Passphrases must be reset immediately when someone with knowledge of the password leaves OLG.

9.12. Minimum passphrase age is 0. Users are allowed to perform subsequent passphrase changes immediately after an initial passphrase change.

9.13. A passphrase cannot be re-used.

9.14. As a minimum, account lockout must occur after a maximum of 10 invalid login attempts within a 30-minute period. The account automatically unlocks 30 minutes after the last invalid login attempt is made. At ISO discretion, the implementation of an administrative action for an unlock will be required.

9.15. Shared account passphrases must change at least annually. ISO may require a more frequent change based on risk.

9.16. Publicly accessible shared accounts must have additional safeguards applied such as IP restrictions and/or other form of approved MFA.

9.17. If a shared account cannot meet one or more of the technical standards above, then ISO must establish a risk-based solution including but not limited to increasing complexity or expiry period.

10. Exceptions

10.1. Exceptions to this standard are subject to the review by the Information Security Office (ISO), and must incorporate justification, appropriate assessment by the ISO, and sign-off by the relevant/responsible information owner(s) as per current Standards exception handling process.

11. Common Requirements

11.1. Integration with OLG's Active Directory, OLG's Federated Directory (Okta if SaaS), or OLG's Tivoli Directory ensures requirements of this standard are met.

11.2. Where integration with an OLG directory service is not possible, integration with OLG's Identity Management infrastructure (Accesshelp/Passwordhelp) is required to maintain compliance with this standard.

12. Logging

12.1. Events relating to both successful and failed log on, as well as privileged use must be generated and recorded in a log that is retained in accordance with OLG retention policies. Event data must include at a minimum the username, date/time, ip address, event name, object being changed/added/removed.

13. Definitions

13.1. **Non-Interactive account:** An account that has authorized technical controls applied that prevents interactive use.

13.2. **Interactive account:** An account that can be used by a person to authenticate to an application or system.

13.3. **End User Account:** A named user account directly assigned and associated to a single OLG employee for the purpose of authenticating to a system or application whether managed by OLG or a third party.

13.4. **Service Account:** a generic account used to run a service such as a bind account, windows service, scheduled task or other non-interactive use.

13.5. **Shared Account:** a generic account typically used interactively by authorized users to support an application or system. Social Media accounts, and default administrative accounts would fall into this category. Typically, these accounts would be used to simplify account management and/or apply higher levels of security through the use of OLG's Password Safe.

Related Policy Instruments

- Password Management Policy

Standards Owner

Director, Technology Security

Standards Approval

Approver	Date
Chief Technology Officer	November 10, 2022

Revision / Review History

Revision / Review Date	Updated By	Summary of Revision / Review
January 19, 2022	Director, Technology Security	▪ Initial Version
November 2, 2022	Director, Technology Security	▪ Updated certain sections based on feedback from multiple parties