[LOGO]

STANDARD	PASSWORD
Owner: [STANDARD OWNER]	Approved Date: **DRAFT**

SUMMARY

The purpose of this standard is to support the secure use of [ORGANIZATION] computer equipment. These rules are in place to protect both the employee and [ORGANIZATION]. Inappropriate use of computer equipment exposes [ORGANIZATION] to risks including virus attacks, compromise of network systems and services, availability of services and bandwidth in the pursuit of the organizational goals and legal issues. This standard enforces the principle of defense in depth and monitoring the effectiveness of security controls, while ensuring compliance with organizational, legal, and regulatory requirements.

[STANDARD AUTHORITY] has the responsibility to ensure appropriate practices are adopted to conform to this standard and the Digital Security Policy that it supports.

APPROVAL

Approved by:	[STANDARD APPROVER NAME 1]	**Position:**	[STANDARD APPROVER POSITION 1]
Signature:		**Date:**	
Approved by:	[STANDARD APPROVER NAME 2]	**Position:**	[STANDARD APPROVER POSITION 2]
Signature:		**Date:**	

SCOPE

All digital systems utilized for the purpose of carrying out the mission of [ORGANIZATION].

AUTHORITY

This standard has been created under the authority of [STANDARD AUTHORITY] which maintains the right to ensure that this standard is adhered to.

ENFORCEMENT

Any [ORGANIZATION] employee found to have violated this standard may be subject to disciplinary action including, but not limited to, termination of employment. Any violation of the standard by a temporary worker, contractor or vendor may result in, but not limited to, the termination of their contract or assignment with [ORGANIZATION]. As obligated by provincial and federal laws, [ORGANIZATION] will notify appropriate law enforcement agencies when it appears that any applicable laws have been violated.

EXCEPTIONS

A request for exception to this standard must be submitted for approval to the [STANDARD EXCEPTION RECEIVER] by following the process as described in the Digital Security Exception Request Procedure. Granted exceptions will be for up to a one-year term and will be reviewed annually at which time the exception may be revoked, revalidated, or extended for another one-year term. Exceptions will be maintained by [STANDARD EXCEPTION MAINTAINER].

STANDARD

GENERAL

1. The following criteria form the structure for [ORGANIZATION] passwords:
    a. Passwords must be a minimum of eight characters in length.
    b. Words that can be found in a dictionary, including a dictionary of names (especially the user's name, the names of their family members, or their pet's name) are prohibited.
    c. At least one special character (for example, %?!@#) must be included.
    d. At least one numeral must be included.
    e. At least one capital letter, preferably not as the first letter, must be included.
    f. Numerals that relate to the user's birthday or other personal information must not be used.
    g. Password cannot be re-used for at least 10 iterations.
2. [ORGANIZATION] administrators will endeavor to utilize the Active Directory (AD) credential where possible to minimize the requirement for users to re-sign on to [ORGANIZATION] applications and systems.
3. Standard passwords will not expire.
4. If a user suspects they are part of a security event, they must initiate the change of their password as close to the suspected event as possible.
5. In the case of a broader security event, [STANDARD AUTHORITY] shall have the authority to require all [ORGANIZATION] AD passwords, or individual system passwords to be placed in a "reset" mode where the next time the user logs on, they are prompted to change their password.
6. Written or typed passwords are not encouraged, however, if there is a necessity to write or type out a password it must be securely stored in locked drawer or cabinet when not in use.
7. Laptop passwords should be stored in a separate location from the laptop itself, and not in the laptop carrying case.
8. All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must either utilize a One Time Password (OTP) mechanism or be accompanied by a second factor of authentication.
9. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
10. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2 or V3).
11. Password Protection:
    a. Always use different passwords for [ORGANIZATION] accounts from other non-[ORGANIZATION] access (e.g., personal ISP account, option trading, benefits, etc.).
    b. Always use different passwords for various [ORGANIZATION] access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
    c. Do not share [ORGANIZATION] passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive (Confidential) [ORGANIZATION] information.
    d. Passwords should never be stored on-line without appropriate encryption.

e. Passwords utilized to authenticate users on the [ORGANIZATION] domain will be one-way hashed at rest using a current hashing algorithm.

f. [ORGANIZATION] passwords will never be stored on non-[ORGANIZATION] equipment (e.g. home computers) without appropriate encryption.

g. Do not reveal a password in email, chat, or other electronic communication in conjunction with the ID associated.

h. Do not speak about a password in front of others.

i. Do not hint at the format of a password (e.g., "my family name").

j. Do not reveal a password on questionnaires or security forms.

k. If someone requests a password, refer them to this document and direct them to the Director of Information Technology, or designate.

l. Always decline the use of the "Remember Password" feature of applications within the browser of choice.

12. The use of an approved Password Manager is encouraged.

SERVICE ACCOUNT PASSWORDS

1. Passwords for service accounts may be set to not expire (non-expiry).
2. They must not be based on the service account name or any of the following:
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, software.
    c. The word "[ORGANIZATION]" or any derivation.
    d. Birthdays and other personal information such as addresses and phone numbers.
    e. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    f. Not a word in any language, slang, dialect, jargon, etc.
    g. Individual words that can be found in a dictionary, including a dictionary of names (especially the servers' name).
    h. Any of the above spelled backwards.
    i. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
    j. Must never use default vendor supplied passwords.
    k. Service Account passwords cannot be re-used.
3. Passwords associated with Service Accounts must be:
    a. Randomly generated and follow secure password generation procedures (WinGuides.com Password Generator is an example tool that can be used for generating secure random passwords).
    b. Passwords must be a minimum of 15 characters in length.
    c. At least three special characters (for example, %?!@#) must be included.
    d. At least three numerals must be included.
    e. At least one capital letter, preferably not as the first letter, must be included.
4. Service Account passwords must always be protected in transit and during storage (e.g. never stored in clear text in configuration files, etc.).
5. Service Account passwords will never be shared or utilized for more than one Service Account.

6. Where possible, auditing of the Service Account must be enabled on systems where it is present to notify the system owner (or SIEM) of relevant audit information and events (User ID, Date/Time, Location, Access attempts, use of privileges, etc.).

ADMINISTRATOR (ADMIN) ACCOUNT PASSWORDS

1. Administrative accounts are not to have the same password as any other account.
2. Each administrative account password must be sufficiently different for each domain that it cannot be guessed if one account is compromised.
3. Administrative passwords will not expire.
4. If an administrator suspects they are part of a security event, they must initiate the change of their password as close to the suspected event as possible.
5. In the case of a broader security event, [STANDARD AUTHORITY] shall have the authority to require all [ORGANIZATION] Administrators to change their password(s).
6. Admin passwords must not be based on the Admin account name or any of the following:
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, software.
    c. The word "[ORGANIZATION]" or any derivation.
    d. Birthdays and other personal information such as addresses and phone numbers.
    e. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    f. Not a word in any language, slang, dialect, jargon, etc.
    g. Words that can be found in a dictionary, including a dictionary of names.
    h. Any of the above spelled backwards.
    i. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
7. Passwords associated with Admin Accounts must be:
    a. Randomly generated and follow secure password generation procedures (WinGuides.com Password Generator is an example tool that can be used for generating secure random passwords).
    b. Passwords must be a minimum of eight characters in length.
    c. At least one special character (for example, %?!@#) must be included.
    d. At least one numeral must be included.
    e. At least one capital letter, preferably not as the first letter, must be included.
    f. Must never use default vendor supplied passwords.
    g. Admin Account passwords cannot be re-used.
8. Admin Account passwords will never be shared or utilized by any other individual other than the intended Admin.
9. All Administrator level passwords must either utilize:
    a. The password scheme described above accompanied by a second factor of authentication; or
    b. a One Time Password (OTP) mechanism.

DEFINITIONS

1. **One-time Password (OTP)** - is a password that is valid for only one login session or transaction, on a computer system or other digital device.

REVISION HISTORY

Date	Version	Author	Summary of Changes
[REV DATE]	1.0	Curtis L. Blais	Initial Draft