ONE® ID Password Standard

Ontario
eHealth Ontario

Review Frequency

This Standard shall be reviewed on an annual basis following the date of approval.

Document Control

The electronic version of this document is recognized as the only valid version.

Table of Contents

1.0 Purpose

This Standard sets out the requirements for passwords accepted by eHealth Ontario (the "Agency") for its identity and access management service – ONE® ID. It applies in all cases where user identification and Authentication to the Agency's information infrastructure is required.

This Standard sets out minimal password requirements. The Agency may require more stringent password or other access control requirements to be implemented based on the identified business needs of a specific site or Healthcare Application.

2.1 Objectives

The paramount goal of this Standard is to safeguard the security of Sensitive Information (which may include Personal Information and Personal Health Information) through implementing appropriate access control by means of the use and management of passwords. To this end, this Standard:

- Establishes consistent policies and practices relating to passwords;
- Establishes password requirements that ensure a reasonable level of usability for End Users;
- Seeks to deter and prevent any attempt by a reasonably knowledgeable intruder to compromise End Users' electronic identities and passwords; and
- Puts controls in place in the event that passwords are compromised.

3.0 Scope

This Standard shall apply where access to the Agency's information infrastructure or Healthcare Applications is controlled by ONE® ID.

This Standard does not apply to the Agency's internal corporate systems.

This Standard is incorporated by reference into the *ONE® ID Policy*.

4.0 Password Responsibilities

4.1 Approval

4.1.1 Authority

This Standard is issued under the authority of the Senior Director, Integrated Solutions & Services, eHealth Ontario.

4.1.2 Revision, Review and Approval

This Standard follows the Agency's coordinated method for the revision, review and approval of Agency policies and standards.

4.1.3 Effective Date

This Standard is effective on the date set for its publication, and on the date(s) set as it may be amended from time to time.

4.2 Administration and Interpretation

4.2.1 Responsibility

The Senior Director, Integrated Solutions & Services, is responsible for the administration and interpretation of this Standard.

4.2.2 Interpretation

This Standard shall be interpreted in accordance with the provisions of the *ONE® ID Policy*.

4.2.3 Exceptions and Waivers

The Senior Director, Integrated Solutions & Services, is responsible for making all decisions regarding Clients' requests for exceptions or waivers to the requirements in this Standard.

Any Client who seeks an exemption from the requirements in this Standard shall submit a written application to the Agency, which shall include reason(s) for the request. The Agency shall review all applications and determine whether a waiver may be granted on a case-by-case basis.

5.0 Password Requirements

5.1 Password Composition

5.1.1 Length

- Every password shall be at least eight (8) characters in length.

5.1.2 Character Sets

- Every password must contain at least one character from each of the following character sets:
    - English uppercase characters (A - Z)
    - English lowercase characters (a - z)
    - Base 10 digits (0 – 9)

5.1.3 Special Characters

- A password may contain non-alphanumeric characters, including <space>, !, $, #, /, \, |, _ and %. However, the character for an ampersand (&) may not be used.

5.1.4 Repeated Characters

- The same character may not make up more than half the password.

5.1.5 Use of User Name and Legal / Preferred Name

- The password shall not contain a portion of the User Name or legal / preferred name(s) that comprises more than half of the total characters in the password.

5.2 System Authentication Requirements

5.2.1 User Name and Password

- The ONE® ID system shall assign to an End User a User Name that is based on the identification information that he/she provides.
- The ONE® ID system shall generate a random temporary password for each End User.
- Before accessing any Healthcare Application, an End User must log into the "self-management" page and self-complete his/her ONE® ID Registration by:
    - Changing his/her temporary password to a permanent password; and

- Selecting and providing the answers to three Online Challenge Questions and two Service Desk Challenge Questions.

- The ONE® ID system shall not issue a temporary password to End Users who have a ONE® ID account at a Level of Assurance of "AL1" (as defined in the *eHealth Ontario ONE® ID Level of Assurance Standard*). Instead, during the account activation (self-completion) process, the End User shall:

  - Create a permanent password; and

  - Select and provide answers to three Online Challenge Questions and two Service Desk Challenge Questions.

5.2.2 Password Display

The System shall not display or echo the characters of a password on any output device.

5.2.3 Password Expiration

Permanent passwords shall expire after 365 days of their issuance or last change. Temporary passwords shall expire after 90 days of their issuance or change.

Once a password has expired, access to any Healthcare Application shall be denied until a new password has been created.

5.2.4 Resetting Expired passwords

- Temporary Passwords

  - Once a temporary password has expired, an End User must contact the eHealth Ontario Service Desk for a new temporary password.

- Permanent passwords

  - Within 180 days of expiration (e.g. until the 544th day after a permanent password's issuance or last change), the End User may recover it online by accessing "account management" and answering the On-line Challenge Questions.

  - If a permanent password has expired for 545 days or more from the day the password was last set, accounts with a Level of Assurance of "AL2" or higher shall be locked. For example, if an End User sets his/her password on December 1st 2013, the account shall be locked on the 545th day at 12:01am. The End User must call the eHealth Ontario Service Desk to have the password reset. The Service Desk shall create a temporary password, which the End User must change to a permanent password online.

  - If the permanent password of an account with a Level of Assurance of "AL1" has expired, an End User may reset it from the "account management" page in the ONE® ID system. The End User must first be Authenticated by answering the Online Challenge Questions.

5.2.5 Notification for Password Change

The ONE® ID system shall notify End Users before the password expiry date of the need to change their passwords by:

- Displaying a notice upon each login for 10 days prior to the expiry date;
- Sending a reminder email to End Users 15 days before the expiry date, i.e. 350 days after the password was last set or changed; and
- Once an End User's password has expired, requiring him/her to change his/her password at the next log-on prior to any further interaction with the ONE® ID system.

5.2.6 Changing Passwords

Password changes may be made online (in the ONE® ID system) as follows:

- Temporary passwords generated by the system during Registration or issued by the eHealth Ontario Service Desk must be changed when the End User first logs on.
- When an End User wishes to change his/her old password, e.g. before its expiry date, he/she may do so using the ONE® ID "account management" page.
- In either case, the End User must first be Authenticated by answering his/her Online Challenge Questions.

5.2.7 Reusing Passwords

An End User must not re-use any of his/her previous six passwords.

5.3 End Users' Security Obligations

5.3.1 Password Secrecy

End Users shall not share, disclose or display a password in any way that may make it accessible to another person.

5.3.2 Password Strength

End Users must choose a strong password that meets the minimal composition requirements specified in section 5.1.

5.3.3 Compromised Passwords

Any End User who knows or suspects that his or her ONE® ID password has been compromised shall:

- Report the issue to the relevant site and/or security administrator; and

- Immediately change the password (if possible).

5.4 Temporary Passwords

The ONE® ID system shall generate a random temporary passwords for new End Users or an End User who has requested a password reset (e.g. if the End User has been locked out of his/her ONE® ID account or has forgotten his/her password).

5.4.1 Temporary Password Requirements

Temporary passwords must comply with the same requirements as permanent passwords as set out in section 5.1.

5.4.2 Temporary Password Expiry

If a temporary password expires (i.e., after 90 days) before it is reset, the ONE® ID system shall lock the account. The End User must then request a new temporary password from the eHealth Ontario Service Desk. Expired temporary passwords may not be recovered online.

5.4.3 Requesting a Temporary Password

End Users who have been locked out of their ONE® ID accounts or have forgotten their passwords may request the issuance of a temporary password through contacting:

- the eHealth Ontario Service Desk; or
- a Registration Agent (RA).

If the End User does not remember his/her On-line Challenge Questions, he/she may call the eHealth Ontario Service Desk which, after validating the End User's identity using the Service Desk Challenge Questions, shall issue a temporary password to the End User**.**

If the End User does not remember his/her Service Desk Challenge Questions, he/she must meet with an RA or LRA to update them.

5.4.4 Identity Validation

Before a temporary password may be issued to an End User, his/her identity must be validated by one or more of the following:

- Correctly answering questions based on information about the End User that had been recorded for Authentication purposes (e.g., sex, date of birth, address, professional license number, etc.);

- Correctly answering questions provided at initial Registration, such as the Service Desk Challenge Questions;

- Presenting identification documentation or evidence equivalent to that required at initial Registration, where the request is made through a personal appearance before a RA or LRA.

5.5 Session Management

5.5.1 Lockout Periods

- An End User shall be disconnected from the ONE® ID system after one hour of inactivity.
- After five (5) failed login attempts with an incorrect password, the ONE® ID system shall lock out the End User and display an error message.
    - End Users shall be locked out for sixty (60) minutes but they may recover their passwords during this lockout period by following the password reset process in section 5.4.

5.5.2 Logging and Monitoring

- All accesses to the ONE® ID system shall be logged. An End User shall be notified if his/her password has been reset by another individual.

Appendix A: Glossary

Term	Description
Agency	The corporation formerly known as the Smart Systems for Health Agency, which is continued under the name of eHealth Ontario in English and cyberSanté Ontario in French.
Authenticate or Authentication	Any process that establishes at the start of each online session the validity of an electronic identification.
Client or Client Organization	Any organization that has entered into an agreement with the Agency to access one or more Healthcare Applications.
End User	Any individual who is sponsored by a Client to use one or more Healthcare Application(s).
Healthcare Application	Any electronic health application or resource that an End User may access over the Agency's information infrastructure.
Level of Assurance	The degree of confidence that can be placed in the identity validation or Authentication of an individual.
Online Challenge Questions	Questions that an End User is required to select from a drop-down list during the ONE® ID account activation (self-completion) process. These questions are then used to Authentiate an End User when he/she accesses the ONE® ID system.
Personal Health Information	Has the same meaning as in the *Personal Health Information Protection Act, 2004* [Section 4 (1)].
Personal Information	Has the same meaning as in the *Freedom of Information and Protection of Privacy Act* [Section 2 (1)].
Registe r or Registration	The process by which a unique identity and associated Level of Assurance is established for an End User.
Sensitive Information	Information that if released without authorization would cause harm, embarrassment or unfair economic advantage, i.e., breach of the duty of confidentiality or the duty to protect the privacy of individuals with respect to their Personal Health Information or Personal Information.
Service Desk Challenge Questions	Questions that an End User is required to set up during the ONE® ID account activation (self-completion) process. These questions are then used to Authenticate an End User when he/she calls the eHealth Ontario Service Desk for support.
User Name	Electronic information, which is composed of a string of characters, that uniquely identifies an End User.