AR0700 – USER IDENTIFICATION AND PASSWORD

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

To ensure that access to Interior Health (IH) owned or shared Digital Information Systems (Systems) is controlled and provided only to authorized users who require access for the performance of their duties. User-identifiers (user-IDs) enable IH to uniquely identify users for the purposes of managing access to Systems. Passwords are used to verify the authenticity of users who access systems.

To ensure that the standards and rules governing the management and use of user-IDs and passwords for Digital Information Systems are clearly defined.

2.0 DEFINITIONS

TERM	DEFINITION
Access	*The ability to view and manipulate information on paper or in electronic form, or through dialogue, based on a user's need or right to know the information.*
Agent	*Any third party or individual directly or indirectly associated with IH in a business relationship; including but not limited to allied health care professionals, non-IH healthcare professionals, students, volunteers, contractors, sub-contractors, researchers, vendors and suppliers.*
Authentication	*The process of identifying an individual based on a username (ID) and password to ensure that the individual is who he or she claims to be.*

AR0700 – USER IDENTIFICATION AND PASSWORD

Authorization	*The process of providing individuals access to systems or information based on their identity.*
Confidentiality	*The duty to ensure that personal information is kept private and is accessible only to authorized persons.*
Confidential Information	*In this policy, confidential information refers to:* *a) Any electronic information that identifies an individual or that can be combined with other information to identify an individual. This definition applies to anyone, living or dead, and includes information like patient/client address, telephone number and personal health number (PHN).* *Any electronic corporate information which has not been authorized for disclosure.*
Control	*Any method of managing risk, including policies, procedures, guidelines, practices, standards or organizational structures, which can be of administrative, technical, management, or legal nature. Control is also used as a synonym for safeguard or countermeasure.*
Digital Information System	*Any IH shared electronic information application or platform. Also referred to as "system or systems"*
Least Privilege	*The security principle that ensures that a user should have only those privileges required for the task at hand and no more.*
Multi-Factor Authentication	*A "strong authentication" mechanism; a system wherein two or more different factors are used in conjunction to authenticate a user to a network or System. Common factors of authentication include something a user knows (i.e. a password), something a user has (i.e., a security token / PIN number), and something a user is (i.e., a fingerprint or retina pattern). Using two factors as opposed to one factor delivers a higher level of authentication and security assurance.*
Privacy	*The right of an individual to determine what information about themselves may be collected, used, and shared with others.*
Privileged Account	*An account used to gain elevated or non-restrictive access to the application, server or platform*
Privileged Access Management	*A system used to securely store privileged account information and automatically generate random secure passwords for privileged accounts.*

Standard User	*Any staff, agent or individual who has been authorized for access to and provided with access to an application or platform. Unlike a Privileged Account, standard user accounts are restricted.*
Threat	*A potential cause of an unwanted incident which may result in harm to a System or organization.*
User-ID	*A code or string of characters used to uniquely identify a standard user, or a privileged account user, on a system.*

3.0 POLICY

3.1 Scope

This policy applies to all staff and agents of Interior Health (IH) who access, use, operate, or administer access to systems.

3.2 Principles

- Access to systems is limited to authorized users only.
- The principle of least privilege shall be used when possible.
- Maintaining effective information security is the responsibility of all systems users.
- A user-ID and password constitute a unique user identity. Each user is responsible for all activities associated with their user-ID and password.
- A user-ID and password is the equivalent of a legal signature.
- The policy for user-ID and password management is based on BC Government, provincial, and industry standards and best practices.

3.3 User Identification Creation

The need to uniquely identify users accessing systems that contain confidential information is a legal requirement for IH and follows the requirements below:

1. Users must be uniquely identified for all systems containing confidential information.
2. Users should be assigned only one individual user-ID per system, unless approved by a designated security administrator for that system in accordance with applicable system policies.
3. Old, redundant or expired user-IDs must not be re-issued to other users.
4. Unique user-IDs may not be required for systems that only contain non-confidential information that is considered publicly available information

and therefore does not present a risk to production services. See Section 3.5 on generic user-IDs.

5. User-IDs for privileged accounts must be unique as well as identify that they are for privileged account use.

3.4 User Identification for System/Service/Privileged Accounts

System/service accounts and privileged accounts must use stronger or additional password controls above that of a standard user (e.g., increased length, use of authorized privileged access management system).

Privileged accounts must be provided in addition to standard user accounts when a person is required to use elevated or non-restrictive access to the application, server or platform in the performance of their duties.

Where supported by critical infrastructure and core systems, and for any cloud-based service, multi-factor authentication must be used.

3.5 User Identification for Generic User-IDs

While able to improve workflow in certain circumstances, generic user-IDs provide no accountability and must therefore be limited in their use and what they can access. In exceptional circumstances, where there is a clear business need identified by a business owner, a generic user-ID may be used for a specific job or group of users, provided;

a) Generic user-IDs must not be used for privileged account functions or access; and
b) Generic user-IDs must not access sensitive or confidential information; and/or
c) Generic user-IDs are only used to access dedicated kiosk machines with limited functionality and enhanced security controls; and
d) An authorized senior manager or delegate of IH is responsible for allocating use of the generic user-ID and all activity attributable to that account;
    i. Maintains a record of the names of the individuals who have access to the generic user-ID, with start/end dates of use;
    ii. Requests a password reset when group members change; and
    iii. Requests deactivation of the generic user-ID when no longer in use.

3.6 Password Standard

Passwords are the most common method of authenticating users on systems and are critical keys to maintaining system security. See Appendix A for the current IH password standard for standard users and privileged accounts.

As per the IH password standard, privileged accounts must not use the same or similar password as the standard user account.

3.7 Password Safeguards

Passwords must be protected from unauthorized access, manipulation or disclosure to others. All account users are required to take appropriate measures to ensure the confidentiality of their user-ID and password.

Systems support staff must not ask users for their passwords, and users must not disclose passwords in response to any request being made, whether verbal or in writing.

Users are required to:

a) Maintain the confidentiality of their passwords by not sharing their passwords to anyone.
   i. Avoid displaying or writing down a password that may be visible to any other person, e.g., typing in a password while another person watches.
   ii. Avoid using an IH password for any non-IH service, account or webpage.
   iii. Avoid storing a password in clear text (i.e., Word, Excel, Notepad)
b) Safeguard user-IDs and passwords; users must not store their password in any automated function such as a function key, macro or password saving program.
c) Change a password immediately and report it to IH's Information Security if it is suspected that the password has become compromised.

Where feasible, privileged account users must also implement the following additional safeguards:

a) Passwords must not be transmitted or stored in clear text. Systems should never display a password as it is entered, or at any other time.
b) Passwords must be encrypted.
c) Passwords may only be stored in an authorized privileged account management system

3.8 Strong Authentication

Passwords are one method of user authentication and may not be sufficient for all access situations. Where greater assurance of user authentication is required, stronger mechanisms such as Multi-Factor Authentication (MFA) shall be implemented. Authentication requirements are determined by a risk assessment considering the type of information to be accessed, location of access, and the type of user transactions performed.

Where technically feasible, strong authentication methods must be implemented for privileged account use.

3.9 Compliance with Policy

Failure to comply with this policy and other related policies may result in disciplinary action including, but not limited to, termination of access, termination of employment, termination of contract, loss of privileges as a student placement or volunteer role, withdrawal of privileges or professional sanctions, and prosecution and liability for loss or damages.

Due to the possibility of security incidents and a rapidly changing threat landscape, additional security policies and/or controls may be enforced without prior notice, including user account suspensions and resetting of passwords.

4.0 PROCEDURES

4.1 Standard account users are responsible for:

4.1.1 Ensuring that the standard account is not used for any elevated or non-restrictive access to an application, server or platform (privileged account access).

4.1.2 Ensuring that all systems used are either locked or logged off, and not left unattended.

4.1.3 Reviewing this policy and all related policies prior to starting employment or a relationship with IH and annually after.

4.1.4 Reporting any breaches of this policy to a supervisor, designate, and to IH Information Security and/or Privacy without fear of reprisal. If

necessary, complete an incident report. All reported breaches are kept strictly confidential.

4.1.5 Updating security questions in the password reset tool to allow self-service resetting of passwords.

4.2 Privileged account users are responsible for:

4.2.1 Ensuring that privileged accounts are used appropriately, and not used for regular activities such as logging on to workstations, checking email, etc.

4.2.2 Facilitating and enforcing the use of individual user-IDs, passwords and controls that comply with this policy.

4.2.3 Enforcing user change to temporary passwords at first log-on and after any password resets by technical support staff or system administrator.

4.2.4 On a new system installation, changing all vendor-supplied default passwords to passwords that comply with this Policy.

4.2.5 Where possible, deactivating or removing all vendor-supplied default accounts (including service accounts).

4.3 Manager / Chief of Staff are responsible for:

4.3.1 Reviewing this policy and all related policies annually thereafter.

4.3.2 Following the process below for any privacy, confidentiality or security breaches:

a) Notify IH Information Security and/or IH Information Privacy
b) Investigate and act on reported incidents in coordination with IH Information Security and/or Information Privacy..

4.4 Digital Health / Information Security are responsible for:

4.4.1 Overseeing the security of Digital Information Systems.

4.4.2 Monitoring the IH computer network for unauthorized access, compliance and other privacy/security vulnerabilities.

4.4.3 Investigating any alleged misconduct in consultation with IH Human Resources, Medical Administration, Risk Management and Internal Audit. All investigations will be performed on a case-by-case basis.

5.0 REFERENCES

1. IH Policy: AR0200 Information Security Policy
2. IH Policy: AR0100 Acceptable Use of Digital Information Systems
3. IH Policy: AR0400 Privacy and Management of Confidential Information
4. IH Policy: AR0500 Email
5. IH Policy: AR0450 Managing Privacy & Security Breaches
6. IH Password Management Tool
   - https://services.interiorhealth.ca/PasswordManagement/
7. Information Security Branch, Office of the Chief Information Officer, Ministry of Citizen's Services, Province of British Columbia - Information Security Policy
   - http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page
8. ISO/IEC 27002 Standards: Code of Practice for Information Security Management
   - http://www.27000.org/iso-27002.htm
9. Payment Card Industry Security Standards Council, Payment Card Industry Data Security Standard (PCI-DSS) v2.0
   - https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
10. Canadian Institute of Chartered Accountants, Information Technology Control Guidelines (ITCG)
    - http://www.cica.ca/publications/information-technology/item61004.aspx
11. Information Systems Audit and Control Association, Control Objectives for Information and related Technology (COBIT).
    - http://www.isaca.org/KnowledgeCenter/COBIT/Pages/Overview.aspx
12. COACH: Guidelines for the Protection of Health Information.
    - http://www.ehealthontario.on.ca/en/privacy/guides

APPENDIX A – INTERIOR HEALTH PASSWORD STANDARDS

Passwords are used as the front-line protection for user accounts, and secure electronic access into IH Digital Information Systems that contain sensitive or confidential information.

a) Standard User

- Password length is a minimum of 8 characters
- Password uses complexity, combining two or more of the following:
  - Lower case (a-z)
  - Upper case (A-Z)
  - Numeric (0-9)
  - Special characters: []{}|;':",.<>?`~@#$%^&*()-=_+
- Passwords are set to expire after 90 days
- Your last 10 passwords cannot be re-used (history)
- After 7 failed login attempts the account is locked out and a call to the Service Desk, or a visit to IH's self-serve password page, is required to unlock the account.

b) Privileged Accounts

- Password complexity requirements are the same as a standard user, but must use a password with a minimum length of 12 characters and mandatory special characters (e.g., complexity)
- Privileged accounts must not use the same or similar password as the standard user account.
- When possible, privileged accounts should be stored in an authorized privileged access management system which will automatically change passwords every 30 days.

Poor or weak passwords have the following characteristics:

- Less than 8 characters
- It is a word found in the dictionary
- Is a common usage word such as:
  - Names of family, pets, friends
  - Computer terms, company name, city name
  - Seasons (e.g., Winter2023)
- Birthday, address, phone number
- Word patterns like QWERTY or ZXCVBNM

Strong passwords have the following characteristics:

- At least 8 characters long
- Contain both upper and lower case
- Have numeric and punctuation as well as letters
- Not a word in any language, slang or dialect
- Makes use of a sequence words, commonly known as a passphrase
- Not based on personal information (e.g., names, birth dates, address)
- Are not written down or stored on-line.