AR0700 – USER IDENTIFICATION AND PASSWORD

1.0 PURPOSE
To ensure that access to Interior Health ("IH") owned or shared electronic 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 Systems are clearly defined.

2.0 DEFINITIONS
See Appendix A.

3.0 POLICY
3.1 Scope
This Policy applies to all staff and agents of IH who access, use, operate or administer access to those Systems. It is understood that some systems are legacy and it may not be technically feasible to incorporate all security safeguards.

3.2 Principles
Access to Systems should be limited to authorized Users only.

Maintaining effective Information Security is the responsibility of all IH staff and other stakeholders who have access to IH’s electronic information resources.

A User-ID and password constitute a unique User identity. Each User is responsible for all activities associated with their IH-assigned User-ID and password.

A User-ID and password is the equivalent of a legal signature.

IH’s policies for User-ID and password management are 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 publically available information and therefore does not present a risk to production services. See Section #3.5 on Generic User-IDs.

5. User-IDs for system administrators must be unique as well as identify that they are for system administrative purposes.

3.4 User Identification for System Administrators

User-IDs for system/service/application administration (“sysadmin”) must use stronger or additional password controls (e.g. use of complexity). Where supported by critical infrastructure and core systems, multi-factor authentication must be considered.

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 sysadmin privileged 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) There is a senior manager or delegate of IH properly authorized and 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 B for the current IH Password Standard for Users and Sysadmins.

3.7 Password Safeguards

Passwords must be protected from unauthorized access, manipulation and disclosure to others. Users are required to take appropriate measures to ensure the confidentiality of their User-ID and Password.

IH’s 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 or disclosing their passwords to anyone.
ii. 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)
b) Safeguard User-IDs, passwords and users must not store their password in any automated function such as a function key, macro or password saving program.

c) Log out or lock the System when leaving it unattended.

d) Change a password immediately and report it to IH’s Information Privacy and Security Office if it is suspected that the password has become compromised.

e) Comply with the IH Password Protection Guidelines in Appendix C.

Where feasible, Sysadmins 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, and not at any other time.

b) Passwords must be encrypted.

3.8 Strong Authentication

Passwords are one method of User authentication on IH Systems and may not be sufficient for all access situations. Where greater assurance of User authentication is required, stronger mechanisms such as Two-Factor Authentication (2FA or multi-factor authentication) 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 PROCEDURE

4.1 Staff and Agents

4.1.1 Review this Policy and all related policies prior to commencing employment or a relationship with IH and on an annual basis thereafter.

4.1.2 Report any breaches of this policy to a supervisor, designate, and to the IH Privacy & Security Office without fear of reprisal. If necessary, complete an incident report in coordination with Information Privacy & Security. All reported breaches are kept strictly confidential.

4.1.3 Update security questions under Password Reset tool to allow self-service resetting of passwords.
4.2 **System Administrators**

System Administrators are responsible for:

4.2.1 Facilitating and enforcing the use of individual User-IDs, passwords and controls that comply with this Policy.

4.2.2. Enforce User change to temporary passwords at first logon and after any password resets by technical support staff or system administrator.

4.2.3. On a new System installation, change all vendor-supplied default passwords to a password compliant with this Policy.

4.2.4. Where possible, deactivate or remove all vendor-supplied default accounts (including service accounts).

4.3 **Managers / Chief of Staff**

4.3.1. Review this Policy and all related policies and on an annual basis thereafter.

4.3.2. For privacy, confidentiality and security breaches:
   a). Notify the IH Information Privacy & Security Office, and
   b). Investigate and act on reported incidents in coordination with the IH Information Privacy & Security Office

4.4 **Information Management and Information Technology / Information Privacy and Security**

4.4.1 Oversee the security of IH Systems.

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

4.4.3 Investigate 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 Information Systems
3. IH Policy: AR0500 Email
4. IH Policy: AR0450 Managing Privacy & Security Breaches
5. IH Password Management Tool
   ➢ https://services.interiorhealth.ca/PasswordManagement/
6. 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
   ➢ http://www.27000.org/iso-27002.htm
8. Payment Card Industry Security Standards Council, Payment Card Industry Data Security Standard (PCI-DSS) v2.0
9. Canadian Institute of Chartered Accountants, Information Technology Control Guidelines (ITCG)
   ➢ http://www.cica.ca/publications/information-technology/item61004.aspx

10. Information Systems Audit and Control Association, Control Objectives for Information and related Technology (COBIT).
    ➢ http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

11. COACH: Guidelines for the Protection of Health Information.
    ➢ http://www.ehealthontario.on.ca/en/privacy/guides
APPENDIX A

1.0 DEFINITIONS

“Access” means authorized individuals who have the right or need to know in order to access personal or confidential information. This would include viewing information on paper or in electronic form, or through dialogue.

“Agents” means any third party individual directly/indirectly associated with Interior Health in a business relationship; including but not limited to: allied health care professionals, non-IH healthcare professionals, students, volunteers, contractors, subcontractors, researchers, vendors and suppliers.

“Authentication” is the process of identifying an individual based on a user name (ID) and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

“Confidentiality” is the duty to ensure that personal information is kept private and is accessible only to authorized persons;

“Confidential Information” whether oral, written, electronic or film, includes the following:

a) personal information about clients, staff and agents that includes their:
   - name, address or telephone number
   - race, national or ethnic origin, colour, or religious beliefs or associations
   - age, sex, sexual orientation, marital status or family status
   - Personal Health Number (PHN), identification number, symbol, or other particular assigned to them
   - fingerprints, blood type or inheritable characteristics
   - health care history, including a physical or mental disability
   - information about their educational, financial, criminal or employment history
   - personal views or opinions, except if they are about someone else
   - and anyone else’s opinions about themselves

b) business information collected or created by Interior Health that exists regardless of form and includes, but is not limited to:
   - information provided to Interior Health by an external vendor or service provider which, if disclosed, would harm the business interests of the third party
   - information prepared as part of pending or ongoing litigation, law enforcement investigation, quality assurance review, Workers Compensation Board or Ombudsman investigation
   - information related to credentialing, discipline, privilege, quality assurance reviews and external review of quality of care
   - in-camera deliberations of Interior Health where such topics as budget strategies, personnel, labour relations, land acquisitions or litigation may be discussed
   - unpublished statistical information and internal correspondence related to organizational initiatives
   - information supplied in confidence to a mediator or arbitrator to resolve or investigate a labour relations dispute
c) all information that, if disclosed without authorization, could be prejudicial to the interests of Interior Health and associated individuals or agencies; and

d) organizational business information that would harm Interior Health’s financial interests and/or information that relates to the management of Interior Health that has not yet been implemented or made public; such as information that identifies the security architecture and infrastructure of the organizations’ information systems

“Control” means 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.

“IMIT” means the IH Information Management and Information Technology department.

“IH” means the Interior Health Authority.

“Least Privilege” means 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” is a “strong authentication” mechanism; a system wherein two or more different factors are used in conjunction to authenticate a user to a network or IH 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.

“Password” means a form of authentication data that is used in combination with a user-ID to control access to a System.

“Privacy” is the right of an individual to determine what information about themselves may be collected, used, and shared with others. Privacy is related to access where those who are authorized and have the right or need to know in order to access patient or other types of confidential information.

“Remote Access” means accessing a System from outside of an IH facility or site.

“Staff” are the officers, directors, employees and physicians engaged by Interior Health.

“System” means any IH shared electronic information system.

“Systems Support Staff / Sysadmin” means systems administrators, analysts, service desk and/or security personnel who maintain and manage IH’s electronic information systems.

“Threat” means a potential cause of an unwanted incident, which may result in harm to a System or organization.

“User” means any Staff or individual who has been authorized for access to and use of a System.

“User-ID” means a code or string of characters used to uniquely identify a user on a System.
APPENDIX B

1.0 INTERIOR HEALTH PASSWORD STANDARDS

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

1.1 Standard User

- Password length is a minimum of 8 characters
- Password does not contain users account name or part of the users full name that exceed 2 consecutive characters
- Password uses complexity, combining three 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, will be required to unlock the account.

1.2 System Administrator

- Same as a standard user, but must use a password with a minimum length of 12 characters and mandatory special characters (e.g. complexity)

Note:

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
  - 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 etc.)
- Should not be written down or stored on-line.
APPENDIX C

1.0 PASSWORD PROTECTION GUIDELINES

Users must ensure password protection for all IH electronic information systems, including computing devices such as a PC, laptop, tablet and other mobile devices such as a smartphone.

All passwords are to be treated as sensitive, Confidential IH Information. Passwords are part of your legal signature which the individual is accountable for.

Here is a list of Don’ts:

- Don’t share IH passwords with anyone
- Don’t reveal your password over the phone to anyone
- Don’t reveal your password in an email message
- Don’t reveal your password to anyone, this includes your boss, secretary, administrative assistant
- Don’t reveal your password to co-workers whilst away or on vacation
- Don’t share your password with a friend, neighbor or family member
- Don’t talk about your password in front of anyone
- Don’t hint at the format of your password
- Don’t write your password down, and store it in plain sight or within easy access (e.g. on notes near your PC)
- Don’t use the “remember password” feature that some applications have (e.g. Internet Explorer).

If someone demands a password, refer them to this Policy or have them call the HSSBC Service Desk.