Title:	Policy Number:	Pages
Security - Password Management	CP 606-2020	3
Approved by:	**Approval Date:**	Dec 8, 2020
Executive	**Last Review Date:**	N/A
Policy Owner:	**Next Review Date:**	January 2022
Chief Security Officer		
Relevant or Related Policies/Legislation/Guidelines:		
The Freedom of Information and Protection of Privacy Act (FOIP) *The Health Information Protection Act* (HIPA) *The Vital Statistics Act, 2009* (VSA)		

Security - Password Management

Purpose Statement

To establish password management requirements for user, system and service accounts.

Scope

This policy applies to all users of the provincial health network.

Definitions

Password means confidential authentication information composed of a string of characters.

Strong password means a minimum of eight alphanumeric characters with at least one upper case, one numeral, one lower case and one special character.

Basic user account means an established relationship between a user and a computer network, service, or application. User accounts are assigned a user ID and are uniquely identifiable and traceable to one user or entity.

Privileged user accounts means a user account that has more privileges than ordinary users. For example, privileged accounts may be able to install or remove software, upgrade operating systems, or modify system or application configurations.

Service accounts means non-human accounts used for running processes, such as web, database and application servers.

User ID means a unique symbol or character string used by an information system to identify a specific user.

Policy Statement

Passwords provide front line protection for user accounts. Weak passwords may compromise the entire provincial health network. As such, employees, vendors and third-party service providers will select and secure strong passwords.

Failure to comply with this policy will result in restricted access to the provincial health network, or disciplinary action, up to and including, termination of employment, appointment or contract with eHealth.

Policy Requirements

General

All privileged user accounts will have passwords that are unique from all other accounts held by that user.

Password construction guidelines

All user, system and privileged accounts will comply with the following password construction requirements:

Password Criteria	Basic User Accounts	Privileged User Accounts	Service Accounts
Minimum Password Length	Eight Characters	10 Characters	20 Characters
Store Password Using Reversible Encryption	Disabled	Disabled	Disabled
Password Complexity	Combination of at least three of the following: - Lowercase character - Uppercase character - Numeral - Symbols	Combination of at least three of the following: - Lowercase character - Uppercase character - Numeral - Symbols	Combination of at least three of the following: - Lowercase character - Uppercase character - Numeral - Symbols
Password Maximum Age	90 Days	90 Days	180 Days
Password History	10	10	12
Password Minimum Age	1	1	0
Lockout on Failed Attempts	4	3	0
Minimum Lockout Duration	15 Minutes	20 Minutes	20 Minutes
Force password change on first logon	Yes	Yes	Yes
Reset After	15 Minutes	20 Minutes	20 Minutes
Minimum Authentication Factors		Multi-factor authentication	

Password protection standards

Employees, contractors, vendors and third-party service providers will treat passwords as sensitive/confidential information. Employees, contractors, vendors and third-party service providers will not:

- Use User IDs as passwords.
- Share passwords with anyone.
- Use an application's "remember password" feature.
- Write down passwords.
- Store passwords in an unencrypted file or computer system.

Employees, contractors, vendors and third-party service providers will immediately report to the Chief Security Officer if:

- Someone demands their password.
- If they suspect that their account/password is compromised. Employees, contractors, vendors and third-party service providers will then immediately change all their passwords.

Application development standards

Application developers will ensure their programs contain the following security precautions:

- Support authentication of individual users, not groups.
- Not store passwords in clear text or in any easily reversible form.
- Support Terminal Access Controller Access Control System + (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

Remote access users

eHealth will control remote access to the provincial health networks through either a virtual private network (in which a password and user id are required) or a form of advanced authentication (i.e., biometrics, tokens, public key infrastructure, certificates, etc.).

Audit

eHealth will perform quarterly audits of password configurations on systems and applications to ensure alignment with the requirements of this password policy.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on a demonstrated business need. Exceptions to this policy must be formally documented by the asset owner and approved by the Chief Security Officer and/or the Enterprise Security Services Department. Policy exceptions will be reviewed on a periodic basis for appropriateness.

LINKED POLICIES/PROCEDURES/RESOURCES

Security - General
Privacy - Corporate
Policy Dictionary