# Password Policy Tool

# Document Purpose and Overview

Password policies are important to implement in clinics because passwords are a key safeguard of health information. Unfortunately, passwords are susceptible to cybercrimes including interception, brute force and social engineering. Protecting passwords will help prevent incidents of unauthorized access to your EMR and other important information.

It is critical to provide all those working within the clinic the guidelines for creating and protecting passwords and ensuring that everyone is compliant.

# Instructions for use

The instructions below are meant to assist you with making this document your own and to and to build strong privacy and security practices within your clinic. The document is created in a standard word document and can be edited to address the specific agreement needed:

* There are highlighted sections with items that need to be edited or suggestions throughout the document that should be edited to fit your clinic’s specific requirements. Please remove all highlighting as you fill out the relevant section.
* The Scope section provides guidance about commonly applied safeguards. Please read them carefully and make sure that these all apply in your clinic and that there aren’t safeguards missing (add as needed).
* Once you have completed adapting this document to create your password policy, it’s important that it be shared widely in your clinic to ensure that everyone is aware of the policy.

# Questions?

If you have any questions about this document or require further assistance, please contact the Alberta Medical Associations’ Security Privacy and Data Sharing (SPaDS) team at privacySPaDS@albertadoctors.org.

Policy: Password Guidelines

# Policy Details

Creation Date: Friday, December 17, 2021 Revision Date:

Applies to: All Employees and Contractors

Approved by: Lead Custodian

## Purpose

To ensure that privacy and security of our computer systems are maintained by using strong password standards.

## Scope (please delete/add the items that do not apply in your clinic)

1. All clinic electronic information system users are assigned a unique identifier (user ID) that restricts access to systems that may contain sensitive personal information and health information required for the employee to carry out their job duties (e.g., windows login).
	1. Access to electronic systems are password protected.
	2. Access to phone voicemail is password protected.
	3. Access to iPhone/tablets devices are password protected.
	4. Access to the wireless network is password protected.
2. All remote access sessions are password protected.
3. All clinic user-level passwords must be changed every 90 days.
4. All system-level passwords (e.g., Windows Administrator, application administration accounts, etc.) must be changed on at least an annual basis.
5. All clinic-issued mobile devices must be password protected with a minimum six digit PIN.
6. All clinic employees must follow appropriate use guidelines including (these are the ones that are suggested:
	1. Passwords are to be kept confidential at all times and should not be written down or posted publicly or shared with other staff except for security purposes. Do not reveal a password in email, chat, or other electronic communication.
	2. Do not reveal a password on questionnaires or security forms.
	3. Always decline the use of the "remember password" feature of applications (e.g., Outlook, internet browsers, etc.).
	4. If an account or password compromise is suspected, report the incident to your manager or clinic lead physician immediately and follow the breach management policy.
7. All monitors used to display identifying health information will time out after a short period of inactivity and require the entry of a password to reactivate the screen.
	1. Selected time-out periods must reflect the level of risk of exposure of workstations (set to lock after one hour of inactivity for local computers and 30 minutes for remote access sessions)

Passwords must be:

(these are suggested ‘best practice’ password guidelines that you may wish to implement in your clinic)

* Minimum length of 8 characters
* Cannot contain user’s name
* Must contain an alpha-upper case, alpha-lower case, numeric, special character
* Only valid for 90 days
* New passwords must be unique (e.g. never used before)
* Maximum of 5 invalid attempts before account lockout

Suggestions:

* It is strongly suggested to use long passphrases (up to 64 characters with no spaces)
* All users with administration privileges should enable multi-factor authentication

|  |  |
| --- | --- |
| Group | Example |
| Lowercase letters | a, b, c, ... |
| Uppercase letters | A, B, C, ... |
| Numerals | 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Non-alphanumeric (symbols) | ( ) ` ~ ! @ # $ % ^ & \* - + = | \ { } [ ] : ; " ' < > , . ? /  |