# CLINITALK Password Protection Policy

**Change control**

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer | Date | Comments | Version |
| N.BoeckxP.Salmon | 25/9/23 | Password protection policy review | 1.0 |
| P.Salmon N.Boeckx | 1/4/24 | Password protection policy review | 1.0 |
| N.BoeckxP.Salmon | 11/04/2025 | Password protection policy review | 1.0 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Next review date: April 2026

Contents

[CLINITALK Password Protection Policy 1](#_Toc146707846)

[1. Overview 1](#_Toc146707847)

[2. Purpose 1](#_Toc146707848)

[3. Scope 2](#_Toc146707849)

[4. Policy 2](#_Toc146707850)

[4.1 Password Creation 2](#_Toc146707851)

[4.2 Password Change 2](#_Toc146707852)

[4.3 Password Protection 2](#_Toc146707853)

[4.4 Application Development 2](#_Toc146707854)

[4.5 Multi-Factor Authentication 3](#_Toc146707855)

[5. Password construction guidelines 3](#_Toc146707856)

[6. Protections against brute force password attacks 3](#_Toc146707857)

[7. Password and Account Compromise Response Policy 3](#_Toc146707858)

# 1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of our resources. All staff, including contractors and vendors with access to Clinitalk systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

# 2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

# 3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system or network that resides at any Clinitalk place of work or stores any non-public Clinitalk information.

# 4. Policy

## 4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines* as described in section 5 below.

4.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.3 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

## 4.2 Password Change

4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

### 4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and co-workers.
All passwords are to be treated as sensitive, confidential Clinitalk information.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in “password managers” authorised by Clinitalk.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

### 4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

## 4.5 Multi-Factor Authentication

4.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

# 5. Password construction guidelines

Passwords used in Clinitalk applications should:

* Be at least 8 characters long.
* Not be a recognisable word.
* Contain at least 1 uppercase letter
* Contain at least 1 lowercase letter
* Contain at least 1 number
* Contain at least 1 special (non alpha-numeric) character

# 6. Protections against brute force password attacks

Protecting against brute force password guessing is crucial for securing our user accounts and systems.

We implement the following strategies to defend against brute force attacks:

* Account Lockout
	+ After 3 repeated unsuccessful login attempts a lock is applied to the user's account to prevent attackers from repeatedly guessing passwords.
* Strong Passwords
* Password expiration
* Monitoring to detect multiple failed login attempts
* Password hashing
* Regular software updates

# 7. Password and Account Compromise Response Policy

Policy Statement:

This policy outlines the steps and procedures to be followed when a password or account is suspected or confirmed to be compromised. The objective is to minimise the impact of security incidents and protect the integrity and confidentiality of our business data.

1. Detection and Initial Assessment:

 - Detection may occur through automated monitoring systems, reports from users, or suspicious activity alerts.

- Upon detection the Security Incident Response Team (SIRT) responsible for initial assessment will be Pete Salmon and Nicholas Boeckx.

 - Establish clear criteria for what constitutes a potential compromise.

2. Isolation and Containment:

 - Immediately isolate the compromised account or system to prevent further unauthorised access.

 - Change the compromised password if necessary to lock out the attacker.

3. Notification:

 - Notify the account holder if their account is confirmed to be compromised. Provide clear instructions on what they should do next, such as resetting their password.

 - Encourage users to report suspicious activity promptly.

4. Investigation:

 - Conduct a thorough investigation to determine the extent of the compromise, how it occurred, and what information or systems may have been accessed.

 - Identify any vulnerabilities or weaknesses in our security that led to the compromise.

5. Password Reset and Account Recovery:

 - If a password was compromised, initiate a password reset process for the affected account.

 - Implement a strong authentication method for account recovery to ensure that the legitimate account holder can regain access securely.

6. Forensic Analysis (if necessary):

 - In cases of severe breaches, consider performing a forensic analysis to gather evidence for potential legal actions and to identify the full scope of the incident.

7. Remediation and Mitigation:

 - Address any identified vulnerabilities or weaknesses in our security systems and practices.

 - Implement improvements to prevent similar incidents in the future, such as enhancing password policies, implementing multi-factor authentication (MFA), or enhancing employee training.

8. Communication:

 - Communicate the incident and actions taken to relevant stakeholders, such as IT staff, affected users, management, and, if necessary, legal and regulatory authorities.

 - Maintain transparency while respecting privacy and confidentiality.

9. Documentation:

 - Maintain detailed records of the incident, including timelines, actions taken, and findings from the investigation.

 - Document lessons learned and update security policies and procedures accordingly.

10. Review and Continuous Improvement:

 - Conduct a post-incident review to assess the effectiveness of the response and identify areas for improvement.

 - Continuously monitor for any signs of recurring incidents and adjust security measures accordingly.

11. Legal and Regulatory Compliance:

 - Ensure that our response process aligns with any legal and regulatory requirements for data breach notifications or reporting.

12. Employee Training and Awareness:

 - Regularly educate and train employees on security best practices and how to recognise and report potential compromises.

**Policy Compliance:**

All employees and relevant stakeholders are required to comply with this policy. Non-compliance may result in disciplinary actions.

**Policy Review:**

This policy will be reviewed annually or as needed to ensure its effectiveness and relevance.