**Cybersecurity Templates**

**Password Guidelines Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Password Guidelines Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[Password Guidelines Policy 3](#_Toc206632340)

[1. Purpose 3](#_Toc206632341)

[2. Scope 3](#_Toc206632342)

[3. Roles & Responsibilities 3](#_Toc206632343)

[4. Password Requirements 3](#_Toc206632344)

[5. Password Change Policy 3](#_Toc206632345)

[6. Protection & Storage 3](#_Toc206632346)

[7. Account Security Controls 4](#_Toc206632347)

[8. Developer Guidelines 4](#_Toc206632348)

[8. Compliance & Enforcement 4](#_Toc206632349)

[9. Exceptions 4](#_Toc206632350)

[11. Review & Maintenance 4](#_Toc206632351)

[12. Quick Checklist for Users 4](#_Toc206632352)

# Password Guidelines Policy

## Purpose

To ensure secure password practices that protect the organisation’s systems, data, and users from unauthorized access and cyber threats.

## Scope

This policy applies to:

* All employees, contractors, vendors, and third parties with access to organisational systems.
* All IT systems, applications, mobile devices, and cloud services require authentication.

## Roles & Responsibilities

Users: Follow password rules and report compromises immediately.

IT Department: Enforce password controls, reset procedures, and compliance monitoring.

Managers: Ensure staff follow policy and report violations.

## Password Requirements

* Length: Minimum [12] characters; admin/service accounts: [16+] characters.
* Complexity: Must include at least 3 of 4: uppercase, lowercase, numbers, special characters.
* Restrictions: Must not contain names, birthdays, dictionary words, or common patterns (e.g., 12345, qwerty).
* Unique per system — no reuse across work/personal accounts.
* Must not reuse last [5] passwords.
* Passphrases encouraged; must follow the same complexity rules.

## Password Change Policy

* Default/vendor passwords must be changed on first use.
* User-level passwords: changed every [180 days].
* Admin/system-level: changed every [90 days].
* Immediate change required if compromise is suspected.

## Protection & Storage

* Passwords must not be written down, shared, or emailed.
* Do not use 'Remember Password' in browsers.
* Only approved password managers may be used.
* Encrypted storage required if system-based password files exist.

## Account Security Controls

* Lockout after [5] failed login attempts (auto-unlock after [30 min] or admin reset).
* Disable accounts inactive for [90 days].
* Enforce session timeouts after [15 min] inactivity.

## 8. Developer Guidelines

* Applications must not store or transmit passwords in cleartext.
* Authentication must be per-user, not shared accounts.
* Password reset functions must enforce verification and temporary secure codes.

## Compliance & Enforcement

IT Security may run password audits/testing.

Violations may lead to disciplinary action, including termination.

## Exceptions

Exceptions require documented approval by [CISO/IT Manager].

Risks must be assessed before approval of exceptions.

## 11. Review & Maintenance

This document is reviewed annually or in response to major security incidents.

The IT Security department maintains version control.

## 12. Quick Checklist for Users

* Use strong, unique passwords.
* Change passwords regularly.
* Never share or write down passwords.
* Report suspected compromise immediately.
* Use MFA wherever possible.