Password Construction Standard for Wales Interiors

Document Classification	Confidential
Document Author	GRC Specialist
Document Owner	IT Manager
Reviewer	Compliance Officer
Approver	CEO
Version Number	1.0
Effective Date	2025-07-02
Next Review Date	2026-07-02

Document Control

Version Control

Version	Author	Reviewed By	Change Description	Owner	Date
1.0	GRC Specialist	Compliance Officer	Initial Draft	IT Manager	28/06/2025

Review Table

Periodical Review Rate	**Last review**	**Next Review**
Annually	28/06/2025	28/06/2026

Distribution List

Recipient	**Department**	**Role**	**Distribution Method**
IT Manager	Info Sec	Policy Owner	Email/Secure Portal
Compliance Officer	Info Sec	Oversight and Monitoring	Email/Secure Portal
HR Manager	Human Resources	Policy Communication	Email/Secure Portal

Document Approval

Approval	**Date**	**Signature**
CEO	**28/06/2025**	

1. **Introduction**
   The purpose of this policy is to establish a secure framework for the creation and management of passwords across Wales Interiors, thereby reducing the risk of unauthorised access and protecting sensitive information systems and data.

2. **Purpose**
   This standard outlines best practices for constructing strong and secure passwords to prevent unauthorised access to systems, services, and data within Wales Interiors.

3. **Scope**
   This policy applies to all employees, contractors, consultants, temporary staff, and third-party affiliates who access any systems or data owned or managed by Wales Interiors. It includes all types of accounts requiring authentication, such as:
   - User-level accounts
   - System-level accounts
   - Web applications
   - Email accounts
   - Remote access systems
   - Voicemail and telephone login credentials
   - Local administrative access (e.g., routers, servers, devices)

4. **Roles and Responsibilities**

Role	Responsibilities
Compliance Officer	Ensure adherence to password standards and conduct periodic checks.
IT Manager	Implement technical controls to enforce password requirements.
HR Manager	Ensure new joiners receive password guidance during onboarding.
All Users	Adhere to the password requirements outlined in this document.

5. **Policy Alignment**

   5.1 Organisational Requirements
   - Enforce strong password usage for all systems and applications.
   - Promote awareness on secure password management.
   - Maintain logs of failed login attempts and investigate anomalies.

   5.2 Regulatory Requirements
   Wales Interiors must comply with applicable data protection regulations, including:
   - ISO/IEC 27001 & ISO/IEC 27002:2022
   - UK GDPR and Data Protection Act 2018
   - NCSC Password Guidance

   5.3 Standard Requirements (ISO/IEC 27002:2022)
   - Clause 8.2: Authentication Information
   - Clause 8.3: Secure Authentication

6. **Safeguards**
   - Passwords must be a minimum of 16 characters.

- Use passphrases comprising multiple unrelated words (e.g., "block-curious-sunny-leaves").
- Avoid predictable patterns, such as birthdates or common dictionary words.
- Password reuse across systems is strictly prohibited.
- Multi-factor authentication (MFA) must be enabled where technically feasible.
- Passwords must be changed immediately if a compromise is suspected.
- Periodic password cracking or guessing tests may be conducted by InfoSec.

7. Learning from Incidents

- All password-related incidents (e.g., account lockouts, phishing attempts) must be logged.
- A post-incident review must be completed within 7 days.
- Reports should include root cause, affected systems, user impact, and remedial actions.

8. Enforcement and Sanctions

Failure to comply with this policy may result in disciplinary action. Sanctions may include:

- Mandatory training
- Written warnings
- Suspension of access privileges
- Termination of employment or contract
- Legal consequences if the breach involves unlawful activity

10. Review Cycle

This policy is reviewed annually or upon:

- Detection of recurring password-related incidents
- Updates to applicable standards or regulations
- Implementation of new authentication technologies

Next Review Date: 2026-03-20

11. Approval

Approved by: CEO
Date: 04/07/2025
Sign: John Doe
This policy is effective immediately upon approval and must be adhered to by all relevant personnel to maintain the security and integrity of the organisation’s information systems.