Identity Management and Access Control Policy for Wales Interiors

Document Classification	Confidential
Document Author	GRC Specialist
Document Owner	Information Technology 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 and Classifier	Email/Secure Portal
Compliance Officer	Info Sec	Monitoring and Compliance	Email/Secure Portal
CEO	Other Department	Strategic Overview and Policy Alignment	Email/Secure Portal

Document Approval

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

1. **Introduction**
   This policy outlines the approach of Wales Interiors to managing digital identities and access privileges across its information systems. Identity and access controls are fundamental to preventing unauthorised access, data breaches, and insider threats, and they support compliance with international standards and regulations.

2. **Purpose**
   The purpose of this policy is to establish a comprehensive framework for effectively managing and controlling user identities, access privileges, and authentication mechanisms within the organisation. It provides clear guidelines for:
   - Account creation, maintenance, and termination.
   - Enforcing authentication and access control standards.
   - Role-based access control and least privilege principles.
   - Regular identity reviews and password hygiene.

   By implementing these practices, Wales Interiors aims to ensure only authorised individuals have appropriate access, maintain data confidentiality and system integrity, and meet regulatory compliance obligations.

3. **Scope**
   This policy applies to:
   - All employees, contractors, third-party service providers, and other stakeholders.
   - All systems, applications, data sources, and network resources requiring authentication.
   - All user accounts, credentials, identity providers (IDPs), and access control mechanisms.

4. **Roles and Responsibilities**

Role	Responsibility
HR	Maintain workforce records in HRIS and notify the IT Manager of new hires, terminations, and role changes.
CEO	Approve access to sensitive systems and third-party integrations where applicable.
IT Manager	Oversee identity management operations, ensure policy enforcement, and conduct regular access reviews.
IT Team	Provision and deprovision user accounts, enforce password and MFA policies, and monitor access logs.
All Users	Use systems responsibly, protect login credentials, follow access control procedures, and report anomalies.

5. **Policy Alignment**

4.1 Organisational Requirements

- The purpose of this policy is to establish a comprehensive framework for effectively managing and controlling user identities, access privileges, and authentication mechanisms within the organisation. It provides clear guidelines for:
- Account creation, maintenance, and termination.
- Enforcing authentication and access control standards.
- Role-based access control and least privilege principles.
- Regular identity reviews and password hygiene.
- By implementing these practices, Wales Interiors aims to ensure only authorised individuals have appropriate access, maintain data confidentiality and system integrity, and meet regulatory compliance obligations.

4.2 Regulatory Requirements

Wales Interiors must comply with applicable data protection regulations, including:

- ISO/IEC 27001 & ISO/IEC 27002:2022
- GDPR and the UK Data Protection Act 2018
- PCI-DSS (where applicable)
- NIST SP 800-63 & NIST Cybersecurity Framework (CSF)

4.3 Standard Requirements (ISO/IEC 27002:2022)

- Clause 5.16 – Identity Management
- Clause 5.17 – Authentication Information
- Clause 5.18 – Access Rights

6. Identity Management & Access Control Safeguards

Wales Interiors shall:

Control ID	Safeguard
ID-01	Maintain an HR program to manage workforce members formally.
ID-02	Maintain an HRIS to track the employment status of each user.
ID-03	Require background screening of all workforce members.
ID-04	Ensure workforce members accept the terms and conditions of employment.
ID-05	Enforce the return of physical assets upon termination.
ID-06	Enforce the return of information assets upon termination.
ID-07	Enforce return or revocation of authentication credentials upon exit.
ID-08	Maintain an inventory of approved Identity Providers (IDPs).
ID-09	Minimise the number of IDPs and adopt Single Sign-On (SSO) solutions.
ID-10	Maintain an inventory of authorised user accounts per IDP.
ID-11	Establish configuration benchmarks for all authorised IDPs.
ID-12	Prohibit account sharing in IDP configuration.
ID-13	Prohibit concurrent login sessions across IDPs.
ID-14	Restrict account name reuse within defined timeframes.
ID-15	Conduct regular identity reviews of all IDPs.
ID-16	Auto-provision user accounts via integration with HRIS.
ID-17	Auto-deprovision accounts upon HRIS status change to inactive.
ID-18	Enforce strong password policies in all IDPs.

Control ID	Safeguard
ID-19	Lock accounts after a defined failed login attempts.
ID-20	Store passwords as encrypted, salted hashes.
ID-21	Only transmit passwords over encrypted channels.
ID-22	Enforce secure password provisioning via the help desk.
ID-23	Mandate Multi-Factor Authentication (MFA) across all IDPs.
ID-24	Auto-disable dormant accounts or apply expiration dates.
ID-25	Log successful and failed login attempts.
ID-26	Log attempts to access deactivated accounts.
ID-27	Log user behaviour analytics (UBA) events for anomaly detection.

7. Identity Lifecycle Management

6.1 Provisioning

- Access is provisioned based on job function using Role-Based Access Control (RBAC).
- The IAM system integrates with the HR system to trigger provisioning workflows.
- All new accounts must be approved by the IT Manager.

6.2 Authentication

- All users must authenticate using MFA where supported.
- Passwords must follow complexity, length, and history requirements as per policy.
- Temporary credentials must be time-limited and monitored.

6.3 Access Reviews

- Quarterly access reviews must be conducted by the IT Manager.
- Privileged accounts (e.g., administrators) must be reviewed monthly.
- Dormant accounts are deactivated after 30 days of inactivity.

6.4 Deprovisioning

- Access is immediately revoked upon termination or change of role.
- Deprovisioning is automated through integration with the HR system and IT systems and reviewed within 48 hours by the IT Manager.
- Terminated credentials are removed from IDPs, VPN, email, and ERP systems by the IT Team.

8. Access Control Guidelines

Access Type	Policy Guideline
General User Access	Provisioned based on business role via RBAC.
Administrative Access	Limited to named individuals; subject to logging and review.
Third-Party Access	Requires NDA, contract, and time-limited accounts.
Emergency Access	Logged and granted under break-glass procedures with post-access review.

9. Enforcement and Sanctions

Non-compliance with this policy will result in:

- **First Violation**: Mandatory refresher training and written warning.
- **Second Violation**: Temporary suspension of access privileges.
- **Third Violation or Severe Breach**: Termination of employment or contract.
- **Illegal Acts**: Legal prosecution under relevant laws and regulations.

All incidents are reviewed by HR and the Information Security Governance Committee.

10. Review Cycle

This policy is reviewed annually or upon:

- Changes in business operations or organisational structure.
- Updates to regulatory or legal requirements.
- Major incidents or audit findings related to access control.

Next Review Date: 2026-03-20

8. **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.