Data Classification 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 defines the approach Wales Interiors takes to classify and manage its information assets, ensuring that data accessed by employees at the office or remotely is handled securely and in accordance with regulatory and organisational requirements.

2. **Purpose**
   The purpose of this policy is to establish a standardised framework for classifying data based on its sensitivity, value, and criticality to Wales Interiors. This ensures that corporate and customer data is appropriately protected from unauthorised access, alteration, or loss.

3. **Scope**
   This policy applies to all employees, contractors, and third parties who access, process, store, or transmit Wales Interiors' information in any form (digital, physical, or cloud-based), including systems such as Microsoft 365, Google Drive, and the Enterprise Resource Planning (ERP) platform.

4. **Roles and Responsibilities**

Role	Responsibility
IT Manager	Supports classification, implements security controls, and maintains records.
Information Security	Provides guidance, audits compliance, and reviews the classification scheme.
Compliance Officer	Ensures adherence to applicable laws and regulations.

5. **Policy Alignment**

5.1 Organisational Requirements

- Data classification shall be based on business criticality and potential impact of loss.
- An approval framework must be in place for assigning classification levels.
- The classification framework must be integrated into data governance and protection strategies.
- Senior management is responsible for enforcing classification standards and allocating resources for compliance.

5.2 Regulatory Requirements

- Wales Interiors must comply with applicable data protection regulations, including:
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- NIST SP 800-53 (where applicable)
- Data Protection Act 2018

Regular audits must ensure that data classification practices align with these standards.

5.3 Standard Requirements (ISO/IEC 27002:2022)

- Clause 5.12 – Classification of Information
- Clause 5.13 – Labelling of Information
- Clause 5.14 – Handling of Assets

6. **Control Measures following ISO/IEC 27002:2022**

6.1 Organisational Controls

6.1.1 Classification and Labelling

- Information assets must be reviewed and classified by designated data owners.
- Classification labels (Restricted, Confidential, Public) must be clearly marked on documents or digital files.

- The classification level must be documented in the organisation's Data Classification Register.

6.1.2 Handling Procedures

- Each classification level has specific storage, transmission, and disposal procedures.
- Confidential or Restricted data must be encrypted in transit and at rest.
- Disposal of physical Restricted data must be done via cross-cut shredders or secure bins.

6.2 Technological Controls

6.2.1 Access Controls

- Access must be granted on a need-to-know basis.
- Restricted data must be accessible only to authorised personnel with multifactor authentication.
- Access privileges must be reviewed every six months.

6.2.2 Data Protection Technologies

- Use of encryption, data loss prevention (DLP), and endpoint protection for Confidential and Restricted data.
- Audit logging for access to sensitive data.
- Automatic expiration or deletion policies for temporary or outdated sensitive records.

6.3 Physical Controls

- Restricted and Confidential information stored physically must be kept in locked cabinets in secure areas with controlled access.
- Server rooms and physical archives must be protected with entry logs, CCTV, and badge-based access.
- Unauthorised devices (e.g., USBs, mobile phones) must be restricted in secure areas.

6.4 People Controls

- All staff must undergo mandatory data handling and classification training during onboarding and annually thereafter.
- Roles and responsibilities for information protection are defined in employment contracts and job descriptions.
- Employees must sign confidentiality agreements and acknowledge their understanding of this policy.

7. Data Classification Procedure

I. Identify the Data Asset

- The IT Manager identifies the data. Typical data assets include design files, client contracts, and financial records.

II. Check for Predefined Restricted Data

- If the data matches any of the types listed in *Appendix A*, it must be classified as **Restricted** (High impact).

III. Assess Security Objectives

- Evaluate the potential impact on **Confidentiality**, **Integrity**, and **Availability** using the guide in Section 6.
- Use the highest of the three to determine the **overall impact level**.

IV. Assign Classification Label

Overall Impact Level	Classification Label
High	Restricted

Overall Impact Level	Classification Label
Moderate	Confidential
Low	Public

V. **Record the Classification**
- Document the classification in the official **Data Classification Register** (electronic or paper).

VI. **Apply Security Controls**
- Appropriate security controls (e.g., encryption, access restrictions) must be applied based on the classification label.

VII. **Review and Reclassify**
- Reassess classification annually or upon significant changes in data usage or business context.

8. **Classification Examples**
- **Client Contracts**

Category	Description
Information Type	Client contractual agreements, including terms, NDAs, and pricing
Confidentiality	High - Exposure could breach confidentiality agreements.
Integrity	High – Contract alterations can cause legal/financial impact.
Availability	Moderate – Required for reference, but not urgently
Overall	High
Label	Restricted

- **Design Files**

Category	Description
Information Type	Proprietary design documents, blueprints, and technical assets
Confidentiality	Moderate – IP and client data exposure risks
Integrity	Moderate – Alteration may affect project outcomes.
Availability	Moderate – Required during project execution
Overall	Moderate
Label	Confidential

9. **Impact Level Determination Guide**

Use the following guide to assess the potential impact on the organisation:

Security Objective	Low	Moderate	High
Confidentiality	Limited adverse effect	Serious adverse effects	Severe or catastrophic effects
Integrity	Limited adverse effect	Serious adverse effects	Severe or catastrophic effects
Availability	Limited adverse effect	Serious adverse effects	Severe or catastrophic effects

10. **Classification Labels Summary**

Classification	Description
Restricted	High-impact data requiring the strongest protection (e.g., passwords, PII, PCI).
Confidential	Sensitive data that could cause harm if exposed (e.g., internal financials).
Public	Low-impact data approved for public distribution (e.g., press releases).

11. **Appendix A:**

I. Data Types Classified as “Restricted”

Authentication Information

- Passwords
- Shared secrets
- Private cryptographic keys
- Authentication hash tables

Payment Card Information (PCI)

- Credit card number plus:
  - Cardholder name
  - Expiration date
  - CVV2/CVC2/CID
  - PIN or PIN block
  - Magnetic stripe content

Personally Identifiable Information (PII)

- First name or initial and last name, combined with:
  - Driver’s license number
  - Financial account + password/security code
  - National Insurance number
  - Passport number
  - Home address
  - Email address
  - Phone number

II. Data Types Classified as “Confidential”

These are sensitive but not highly restricted. Their unauthorised access could harm the company, but not cause catastrophic damage. The following includes, but is not limited to;

- Employee Performance Reviews
- Internal Financial Reports (Quarterly summaries) (Not shared externally)
- Design Drafts for Upcoming Projects
- Vendor Agreements (without sensitive financial details)
- Client Project Timelines

III. Data Types Classified as “Public”

These are intended to be shared publicly or have no adverse impact if disclosed. The following includes, but is not limited to;

- Marketing Brochures
- Published Project Portfolios
- Job Postings
- Company Contact Information
- Non-sensitive Blog Content or Newsletters

12. **Exceptions**

Exceptions to this policy must:

- Be formally documented and approved by the Information Security Manager.
- Include justification, risk assessment, and compensating controls.
- Be reviewed quarterly for relevance and effectiveness.

13. **Enforcement and Sanctions**
    - Violations of this policy may lead to disciplinary action, including termination and legal penalties.
    - Any non-compliance must be reported to the IT Security team.
    - Wales Interiors reserves the right to audit data classification practices without notice.

14. **Review Cycle**
    This policy shall be reviewed annually or in response to significant changes in business operations, regulatory requirements, or risk assessments.
    Next Review Date: 2026-07-02

15. **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.