Third-Party Management 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 establishes a framework for assessing, onboarding, managing, and monitoring third-party entities who access, process, or store Wales Interiors' data or systems. It ensures third parties operate in a manner that upholds the organisation's security, privacy, and compliance obligations.

2. **Purpose**
   The purpose of this policy is to:
   - Define the lifecycle for engaging third-party vendors, suppliers, and partners.
   - Establish criteria for assessing risk before, during, and after third-party engagement.
   - Ensure third parties follow applicable security, privacy, and contractual controls.
   - Promote visibility and accountability of external entities interfacing with Wales Interiors.

3. **Scope**
   This policy applies to:
   - All third-party entities who access or manage Wales Interiors' systems, services, networks, or data.
   - Internal teams (e.g., Procurement, IT, Legal, and Compliance) involved in third-party evaluation and engagement.
   - All vendor relationships, including technology service providers, cloud vendors, consultants, and outsourced partners.

4. **Roles and Responsibilities**

Role	Responsibility
Procurement Team	Evaluate vendors' contractual and financial standing.
Legal Counsel	Draft and review contracts with security, privacy, and liability clauses.
Compliance Officer	Conduct third-party risk assessments and ensure ongoing compliance.
IT Manager	Review third-party technical integrations and ensure secure connectivity.
Business Owners	Own the relationship and validate vendor performance.
All Users	Report third-party security concerns to the Information Security team.

5. **Policy Alignment**

5.1 Organisational Requirements

- Third-party onboarding must follow a structured due diligence process.
- Risk-based assessments must be conducted before granting system or data access.
- Agreements must include security clauses (e.g., breach notification, audit rights).
- Ongoing monitoring is required for high-risk vendors.

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
- NIST SP 800-171 and Cyber Essentials (where applicable)
- Supplier assurance obligations as per client contracts

4.3 Standard Requirements (ISO/IEC 27002:2022)

- Clause 5.19 – Information Security in Supplier Relationships
- Clause 5.20 – Addressing Information Security in Supplier Agreements

- Clause 5.21 – Managing Supplier Service Delivery

6. **6. Third-Party Safeguards**

Wales Interiors shall:

Control ID	Safeguard
TP-01	Maintain a centralised third-party inventory with risk classification.
TP-02	Perform due diligence assessments prior to engagement.
TP-03	Require signed contracts with security, confidentiality, and audit clauses.
TP-04	Perform data protection impact assessments (DPIAs) when necessary.
TP-05	Enforce principle of least privilege for all third-party access.
TP-06	Require Multi-Factor Authentication (MFA) for third-party remote access.
TP-07	Monitor third-party activities through audit logs and alerts.
TP-08	Conduct annual reviews of critical third-party performance and security posture.
TP-09	Revoke access immediately upon contract termination or non-compliance.
TP-10	Ensure third parties are aware of and adhere to the organisation’s security policies.

7. **Third-Party Lifecycle Management**

7.1 Onboarding

- Complete due diligence and risk assessment.
- Define scope of access and system integration requirements.
- Obtain sign-off from IT, Legal, and Compliance.

7.2 Contracting

- Include clauses on security standards, incident reporting, data handling, and audit rights.
- Require NDAs and data protection agreements (DPA) where personal data is involved.

7.3 Monitoring

- Monitor performance, SLA compliance, and data usage.
- Periodically assess risks based on vendor classification.

7.4 Offboarding

- Ensure termination of access across all systems and applications.
- Retrieve or confirm secure deletion of data.
- Document lessons learned and update the vendor record.

8. Enforcement and Sanctions

Non-compliance with this policy may result in:

- Termination of third-party contracts.
- Removal of access privileges.
- Legal claims or penalties.
- Internal disciplinary action where employee negligence is involved.

10. Review Cycle

This policy is reviewed annually or upon:

- Changes in applicable legal or regulatory frameworks.
- Onboarding of new critical third parties.
- Security incidents involving third-party services.

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.