### Remote Working Security Policy 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 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**
   As remote working becomes an essential part of modern business operations, Wales Interior is committed to ensuring that its information and systems remain secure. This policy outlines the necessary controls and responsibilities for securely accessing company data and resources while working remotely.

2. **Purpose**
   This policy defines the security requirements for employees and third parties accessing Wales Interiors' information and IT systems remotely.

3. **Scope**
   This policy applies to all employees, contractors, and third parties who access Wales Interiors' systems, data, or services remotely.

4. **Roles and Responsibilities**

| Role | Responsibilities |
|---|---|
| **Department Head** | Ensure team compliance, provide necessary tools and training, and support secure remote work practices. |
| **IT Manager** | Oversee policy enforcement, conduct audits, update guidelines, and lead security awareness efforts. |
| **IT Team** | Maintain secure remote access (e.g., VPNs), update and protect devices, and monitor for security incidents. |
| **All Users** | Must comply with this policy, use only authorised tools, safeguard devices, and report security incidents promptly. |

5. **Policy Alignment**

**5.1 Organisational Requirements**

- Maintain a documented physical security and remote access program.
- Regularly assess physical and remote security risks.
- Integrate physical and cyber controls across business functions.

**5.2 Regulatory Requirements**

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

- ISO/IEC 27001 & ISO/IEC 27002:2022
- UK Data Protection Act 2018 & GDPR
- Applicable health and safety laws

**5.3 Standard Requirements (ISO/IEC 27002:2022)**

- Clause 6.2: Teleworking
- Clause 5.10: Acceptable Use of Information
- Clause 8.1: User Endpoint Devices

6. **Remote Work Security Controls**

| Control ID | Safeguard |
|---|---|
| RW-01 | All remote access must use secure VPNs with MFA. |
| RW-02 | Company-approved devices must be encrypted and regularly updated. |
| RW-03 | Public Wi-Fi must be avoided unless a VPN is used. |
| RW-04 | Confidential data must not be stored locally unless authorised. |

| Control ID | Safeguard |
|---|---|
| RW-05 | Screens must be locked when unattended. |
| RW-06 | Use of personal devices (BYOD) must be approved and monitored. |
| RW-07 | Remote workers must report incidents within 24 hours. |
| RW-08 | Physical access to devices must be restricted at home or other remote sites. |
| RW-09 | Only company-approved cloud platforms may be used for storing and sharing files. |
| RW-10 | Data backups must be automatic and secure, where applicable. |
| RW-11 | Monitoring activities must be performed by the organisation through the IT Team |

## 7. Remote Work Environment Guidelines

### 7.1 Device Security

- Company devices must have anti-malware, firewalls, and full-disk encryption enabled.
- Regular patching and software updates must be enforced by IT.

### 7.2 Secure Network Use

- Only trusted, password-protected Wi-Fi should be used.
- VPN must always be active during remote sessions.

### 7.3 User Behaviour

- Maintain clear desk principles in home environments.
- Refrain from printing or storing physical copies of confidential materials.

### 7.4 Incident Response

- Any security concern must be immediately reported to the IT security team via the incident reporting channel.

## 9. Enforcement and Sanctions

Non-compliance with this policy will result in:

- **First Offence:** Mandatory training on physical security procedures and a written warning.
- **Second Offence:** Temporary suspension of facility access privileges.
- **Third Offence or Severe Breach:** Termination of employment or contractual relationship.
- **Criminal Activity:** Escalation to law enforcement following applicable laws.

All infractions are investigated by IT and HR, with escalation to the CEO as necessary.

## 10. Review Cycle

This policy is reviewed annually or upon:

- Significant physical or organisational changes.
- Changes to legal or regulatory requirements.
- Physical security incidents or control failures.

**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.