Physical Security Management Policy for Wales Interiors

Document Classification	Confidential
Document Author	GRC Specialist
Document Owner	Facilities and Security Lead
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**
   Physical security plays a vital role in protecting Wales Interiors' infrastructure, assets, and employees. This policy sets out a robust physical security framework to prevent unauthorised access, theft, damage, or disruption of physical resources that support the confidentiality, integrity, and availability of our business operations and information systems.

2. **Purpose**
   The purpose of this policy is to establish and enforce consistent and comprehensive measures for:

   - Securing physical premises, infrastructure, and information assets.
   - Preventing unauthorised physical access to sensitive areas.
   - Ensuring appropriate monitoring, visitor control, and secure asset handling.
   - Enhancing resilience through integration of physical and cybersecurity practices.

   The implementation of this policy supports the organisation's security strategy and compliance requirements by mitigating physical threats and ensuring operational continuity.

3. **Scope**
   This policy applies to:
   - All employees, contractors, third-party personnel, visitors, and stakeholders who access Wales Interiors' premises.
   - All physical infrastructure, including offices, server rooms, storage areas, and access-controlled environments.
   - All physical assets such as computing devices, paper-based records, and physical access tools.

4. **Roles and Responsibilities**

Role	Responsibilities
HR	Maintain accurate records of workforce members; report joiners/leavers to the Facilities Lead.
CEO	Approve high-risk physical security exceptions and oversee security governance.
IT Manager	Ensure secure storage and physical protection of IT systems and media.
General IT	Secure computing devices, printers, and server hardware; enforce clean desk policy.
Facilities & Security Lead	Implement and monitor physical safeguards, control physical access systems, and manage surveillance and visitor logging.
All Users	Follow access protocols, wear identification badges, secure unattended areas, and report physical security incidents.

5. **Policy Alignment**

   5.1 Organisational Requirements
   - Establish a documented physical security program.
   - Conduct physical security risk assessments and penetration tests.
   - Integrate physical security measures with information security requirements.

   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
- Local health, safety, and building regulations

5.3 Standard Requirements (ISO/IEC 27002:2022)

- Clause 7.1 – Physical and Environmental Security
- Clause 7.2 – Secure Areas
- Clause 7.3 – Equipment Security

6. **Physical Security Safeguards**

Wales Interiors shall:

Control ID	Safeguard
PHY-01	Maintain a documented physical security program that outlines safeguards and procedures.
PHY-02	Implement mechanisms to monitor and detect violations of the physical security program.
PHY-03	Define procedures for the secure disposal of physical assets.
PHY-04	Enforce perimeter access controls, including locks, card readers, and entry alarms.
PHY-05	Implement visitor registration, identification, and escort procedures.
PHY-06	Apply internal access controls (e.g., key card zones, staff-only areas).
PHY-07	Securely manage physical access devices like keys, badges, or cards.
PHY-08	Visibly mark the classification level on critical hardware and devices.
PHY-09	Implement environmental controls such as fire suppression, HVAC, and flood prevention systems.
PHY-10	Restrict physical access to computing devices, especially servers and networking equipment.
PHY-11	Define and enforce policies for removing technology assets from premises.
PHY-12	Maintain a clean desk and secure unattended space protocols.
PHY-13	Secure peripheral technology assets (e.g., printers, copiers) against unauthorised access.
PHY-14	Maintain physical access logs for review and auditing.
PHY-15	Perform regular physical penetration tests to validate the effectiveness of physical controls.

7. Physical Security Measures

7.1 Access Control

- Access to office buildings, data rooms, and sensitive areas is controlled by key cards or locks.
- Only authorised personnel have access to specific areas based on job requirements.
- All staff must visibly display ID badges while on site.

7.2 Surveillance and Monitoring

- CCTV cameras are installed at entrances, exits, and sensitive areas and are retained for a minimum of 30 days.
- All visitor access is logged and subject to real-time monitoring.

7.3 Equipment Security

- Servers, network switches, and sensitive IT assets are kept in locked rooms with restricted access.
- Printers and multifunction devices must be positioned away from public view and logged for activity monitoring.
- Secure storage cabinets are used for backups and removable media.

7.4 Asset Disposal

- Obsolete equipment is disposed of via certified vendors with asset disposal certificates.
- Media containing sensitive data is physically destroyed or securely wiped before disposal.

7.5 Environmental Safeguards

- Smoke detectors, fire extinguishers, and temperature controls are in place in critical rooms.
- Electrical panels and backup power systems are tested periodically.

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 violations will be reviewed by the Facilities & Security Lead and HR, with involvement from the CEO where warranted.

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

7. 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.