Clear Desk and Clear Screen 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**
   Wales Interiors recognises that effective incident management and maintaining secure work environments are critical to maintaining information security. This policy outlines the responsibilities and processes for identifying, reporting, responding to, and learning from information security incidents. It also defines the standards for clear desk and clear screen practices to protect both physical and digital information assets.

2. **Purpose**
   To ensure that:
   - All information security incidents are consistently identified, reported, managed, and reviewed.
   - Users are aware of their responsibilities for securing both electronic and paper-based information.
   - The confidentiality, integrity, and availability of Wales Interiors' systems and data are maintained.
   - Prevent theft, unauthorised access, or damage.
   - Comply with data protection laws.

3. **Scope**
   This policy applies to all employees, contractors, and third parties who access, process, or manage information systems, data, or services on behalf of Wales Interiors. It includes remote and office-based users.

4. **Roles and Responsibilities**

Role	Responsibilities
Department Head	Ensure teams follow policy requirements.
IT Manager	Coordinate incident response and oversee policy adherence.
Compliance Officer	Monitor compliance and maintain audit logs.
All Users	Adhere to clear desk and screen protocols and report incidents.

5. **Policy Alignment**

5.1 Organisational Requirements

- Implement a repeatable incident response and clear desk/screen control.
- Ensure secure handling and storage of both paper and digital records.
- Maintain logs and training documentation.

4.2 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

4.3 Standard Requirements (ISO/IEC 27002:2022)

- Clause 5.24: Information Security Incident Management
- Clause 5.25: Learning from Information Security Incidents
- Clause 6.5: Responsibilities and Procedures
- Clause 7.7: Clear Desk and Clear Screen Policy

6. Clear Desk and Clear Screen Policy

6.1 Requirements

6.1.1 Clear Desk

- Desks must be paper-free at the end of the day.
- Documents must be locked when leaving desks unattended.
- Sensitive prints must be collected immediately.
- Unauthorised document visibility must be avoided.

6.1.2 Clear Screen

- Screens must be locked when unattended.
- Log off or shut down at day's end.
- Mobile devices must be PIN-protected, auto-lock after 2 minutes, and stored securely.

6.2 Equipment Security

- Storage devices (e.g., USBs) must be locked away.
- Keys must not be left unattended.
- Shred confidential paper waste.
- Use the printer's "locked print" feature.

6.3 Exceptions

Any policy exceptions must be approved by the IT Manager and documented with:

- Nature and justification of exception
- Associated risks
- Approver details

7. Training

- All staff receive clear desk/screen and incident management training during induction.
- Refresher sessions are provided regularly.
- Role-based training ensures ongoing compliance.

8. Enforcement and Sanctions

- This policy forms part of employees' contractual obligations.
- Breaches may result in disciplinary action up to termination.
- Compliance will be audited regularly by the Compliance Officer.

9. 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.