**Incident Management 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 is critical to maintaining information security. This policy outlines the responsibilities and processes for identifying, reporting, responding to, and learning from information security incidents.

2. **Purpose**
   To ensure that all information security incidents are consistently identified, reported, managed, and reviewed to protect the confidentiality, integrity, and availability of Wales Interiors' systems and data.

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.

4. **Roles and Responsibilities**

| Role | Responsibilities |
|---|---|
| **Compliance Officer** | Ensure regulatory and policy compliance and maintain incident logs. |
| **IT Manager** | Coordinate incident response, manage root cause analysis, and oversee post-incident reviews. |
| **Department Heads** | Report incidents and ensure staff follow response procedures. |
| **All Users** | Promptly report incidents and assist in investigations. |

5. **Policy Alignment**

**5.1 Organisational Requirements**

- Ensure a consistent and repeatable incident response process.
- Maintain secure logs of all incident activity.
- Conduct root cause analysis and implement remediation actions.

**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
- Other applicable legal and contractual obligations

**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

6. **Incident Classification and Reporting**

**6.1 Incident Definition**

An information security incident includes but is not limited to:

- Data loss or theft
- Unauthorised data access
- Malware infections or system compromise
- Denial of service attacks
- Misuse of information or systems

6.2 **Reporting Requirements**

- Report all incidents immediately to the IT Manager or via the secure incident reporting platform.

- Provide the following information:

    - Reporter's name and contact details
    - Type of incident and data/equipment involved
    - Time, date, and location
    - Impact or suspected risk

## 7. Incident Handling and Response

| Stage | Action |
|---|---|
| Identification | Recognise and log suspected incidents. |
| Containment | Limit exposure and isolate affected systems. |
| Eradication | Remove the cause and prevent reoccurrence. |
| Recovery | Restore services and confirm system integrity. |
| Lessons Learned | Conduct post-incident reviews and update controls. |

## 8. Learning from Incidents

- All incidents must be documented.
- Post-incident reviews must be conducted within 7 days.
- Trends and recurring vulnerabilities must be addressed.
- Reports must include incident type, impact, response time, and cost.

## 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.