Secure Configuration 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 is committed to maintaining the security, integrity, and availability of its information systems through a structured and standardised approach to configuration management. This policy establishes controls and procedures to ensure the secure and consistent configuration of all IT assets.

2. **Purpose**
   This policy defines the requirements and responsibilities for identifying, documenting, tracking, and maintaining secure configurations of the organisation's hardware, software, and network devices. Effective configuration management minimises the risk of unauthorised access, vulnerabilities, and system disruptions.

3. **Scope**
   Applies to all employees, contractors, and third parties managing or accessing Wales Interiors' IT infrastructure, including all hardware, software, network devices, and systems requiring secure and consistent configuration management.

4. **Roles and Responsibilities**

Role	Responsibilities
Department Head	Ensure team adherence to configuration standards and provide necessary support.
IT Manager	Oversee configuration management program, approve standards, and enforce compliance.
IT Team	Implement and maintain configuration baselines, enforce policies, and conduct audits.
All Users	Follow configuration policies, report anomalies, and not alter configurations without approval.

5. **Policy Alignment**

5.1 Organisational Requirements

- Maintain documented configuration baselines and standards.
- Implement change control processes for configuration updates.
- Conduct regular configuration audits and drift detection.
- Maintain version control and configuration backup processes.

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
- Industry-specific compliance requirements

4.3 Standard Requirements (ISO/IEC 27002:2022)

- Clause 8.1: Operational Procedures and Responsibilities
- Clause 8.3: Configuration Management
- Clause 12.1: Change Management

6. **Configuration Management Controls**

Control ID	Safeguard
CFG-01	Maintain a library of approved OS configuration benchmarks, ensuring secure baseline setups.
CFG-02	Disable unnecessary OS services based on approved benchmarks.
CFG-03	Public Wi-Fi must be avoided unless a VPN is used.
CFG-04	Remove or disable unnecessary scripting languages within OS environments.
CFG-05	Enable advanced logging for shells like PowerShell or BASH to monitor system activity.
CFG-06	Enforce cybersecurity features including DEP, ASLR, and UAC on all systems.
CFG-07	Disable autorun features on all operating systems.
CFG-08	Enable machine lock/screensaver after a predefined inactivity period.
CFG-09	Ensure secure boot processes (e.g., UEFI) verify OS integrity before loading.
CFG-10	Disable unnecessary wireless protocols and networks on endpoint devices.
CFG-11	Maintain a library of approved software application configuration benchmarks.
CFG-12	Implement configuration enforcement systems that apply approved OS and application settings.
CFG-13	Ensure that enforcement systems apply configurations regardless of device location (on-site or remote).

7. Configuration Management Procedures

- **Configuration Baselines:** Approved secure configurations must be documented, version-controlled, and maintained for all relevant systems.
- **Change Management:** All configuration changes require formal approval, testing, and documentation before deployment.
- **Configuration Drift Detection:** Regular automated and manual audits must be conducted to detect and remediate unauthorised changes.
- **Backup and Recovery:** Configuration files and baselines must be securely backed up and recoverable in the event of system failure.
- **Access Control:** Only authorised personnel shall have right to modify configurations, enforced by role-based access controls.

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.