WSR MEDICAL SOLUTIONS LTD	Date: June 2025	POLICY	REF. No:	ISSUE
Approved By: Paul Dixon (Managing Director)	Review: June 2026	Information Security Policy	POL-16	No.1

1. Purpose and Scope

- The purpose of this policy is to protect WSR's information assets from all threats, whether internal or external, deliberate or accidental.
- This policy applies to all employees, contractors, systems, data, cloud services (e.g. Odoo, Microsoft 365), and physical locations operated or managed by WSR.

2. Information Security Objectives

- Ensure confidentiality of sensitive and personal data.
- Maintain integrity of all company data, including customer records.
- Guarantee availability of information systems through appropriate access, backup, and continuity planning.

3. Roles and Responsibilities

- The Managing Director holds overall accountability for information security.
- Day-to-day operations are supported by Smart IT (external IT provider) and designated internal roles (e.g. Compliance Officer).
- All staff are responsible for adhering to this policy and reporting security incidents.

4. Asset Management

- All physical and digital assets must be identified and tracked in an asset register. **[DF8 Asset Register]**

5. Access Control

- Access to systems and data is granted on a least privilege basis. **[POL 15 Access Control Policy]**
- Multi-Factor Authentication (MFA) is required for all key systems including Microsoft 365 and Odoo. **[POL 13 MFA Policy]**
- Access is revoked immediately upon termination or role change. **[POL 15 Access Control Policy]**
- Password Policy must be followed. . **[POL 14 Password Policy]**
-

6. Physical and Environmental Security

- Server and networking equipment must be kept in secure areas with restricted access.
- Visitors must be signed in and accompanied at all times.

7. Cloud and IT System Security

- WSR uses certified UK-based cloud services (e.g. Smart IT and Odoo) with encryption in transit and at rest.
- Penetration testing is conducted regularly under the Cyber Essentials programme.
- Updates and patches are managed by the IT provider to maintain secure systems.

8. Data Handling & Classification

- Data must be handled according to its classification and in line with GDPR principles.
- Secure transmission methods (e.g. encrypted email) must be used for confidential or sensitive data.
- Sensitive data must be securely deleted when no longer required.

9. Backup and Business Continuity

- Information must be stored on the Odoo system which is managed and maintained with secure backups
- Backup restoration is tested periodically by Smart IT.
- A Business Continuity Plan and Disaster Recovery Plan must be maintained and reviewed annually.

10. Incident Management

- All employees must report suspected breaches immediately to their manager or the DPO.
- Incidents must be logged, investigated, and remediated according to internal procedures.
- Serious incidents must be reported to the ICO within 72 hours if they involve personal data.

WSR MEDICAL SOLUTIONS LTD	Date: June 2025	POLICY	REF. No:	ISSUE
Approved By: Paul Dixon (Managing Director)	Review: June 2026	Information Security Policy	POL-16	No.1

11. User Awareness and Training

- All employees receive GDPR and information security training annually.
- Refresher training and awareness campaigns are provided based on risk and role.
- Phishing awareness and acceptable use policies are reinforced regularly.

12. Third-Party and Supplier Security

- All processors must be subject to due diligence and have GDPR-compliant contracts.
- A list of authorised processors is maintained and reviewed annually (e.g. Smart IT, CubeHR, Mirion**). [ROPA Document}**
- Suppliers must accept WSR's data protection and information security expectations.
- Suppliers Must go through:
    - A402 – Legitimate Interest Assessment
    - A403 – Processor Due Diligence
    - Entered onto ROPA

13. Monitoring and Audit

- Systems are monitored for suspicious activity and access anomalies.
- Audits of IT systems and policies are conducted periodically or after incidents.
- Access logs and system changes are retained for security review.

14. Policy Review and Maintenance

- This policy is reviewed annually or upon significant changes to business operations or legal requirements.
- Reviews are led by the Managing Director and Compliance Officer with input from IT support.

15. Compliance

- WSR complies with the UK GDPR, Data Protection Act 2018, and relevant ISO standards (e.g. ISO 9001, ISO 27001 where applicable).
- Failure to comply with this policy may result in disciplinary action.