Information Security Policy

Web Manuals shall establish and maintain effective Information Security Management System (ISMS) based on the principles, requirements, and controls of the ISO/IEC 27001:2022 standard and industry best practices.

The ISMS shall strive to fulfill the company's commitment to:

- Ensuring the confidentiality, integrity, and availability of information assets;
- Complying with relevant legal, regulatory, contractual requirements and ethical conduct;
- Continually improving the effectiveness of the ISMS; and
- Fostering a culture of awareness and responsibility for information security.

Applicability

The policy applies to all business units, employees, contractors, third-party service providers, and any other individuals and entities with access to Web Manuals information assets.

Information Classification

All information assets shall be classified based on sensitivity and criticality, to which access controls are implemented accordingly.

Access Controls

Access to information assets shall be restricted based on the Principle of Least Privilege. User access shall be reviewed regularly, and access rights revoked promptly when access is no longer needed.

Application Security and Privacy

Secure application coding and hosting practices shall be observed during the software development lifecycle. Regular security assessments shall be conducted, and vulnerabilities shall be addressed promptly. The development of the Web Manuals suite shall follow Private by Design and Private by Default principles, ensuring the greatest amount of protection for personal data stored in applicable systems.

Physical Security

Physical access to Web Manuals offices shall be restricted and monitored. Security and safety measures shall be implemented to prevent unauthorized access, damage, or theft. Physical security shall be a selection criteria for hosting providers.

Device Security

All company devices shall be secured and safeguarded against cyber threats, unauthorized access, and inadvertent damage and loss.

Information Security Training

All employees and relevant contractors shall undergo appropriate information security training. There shall be regular awareness programs to educate employees about the latest security threats and best practices.

Incident Management

Incident management shall be established to detect, respond to, and recover from security incidents. Incidents shall be reported promptly, response plan documented, and lessons learned used to improve the response process.

Business Continuity

Business continuity and disaster recovery plans shall be developed, tested, and maintained to ensure availability of critical systems and data in the event of disruptions.

Compliance

Web Manuals shall adhere to all applicable legal, regulatory, and contractual requirements related to information security. Regular compliance assessments and monitoring shall be conducted.

Risk Management

Risk management shall be established to identify, assess, and control information security risks. Risk controls and treatments plans shall be developed and implemented to appropriately respond to identified risks.

Monitoring and Audit

Information security controls shall be monitored regularly to ensure organizational compliance, and identify and respond to any deficiencies. Internal audit, management review, and other feedback mechanisms shall be used as tools to assess the effectiveness of the ISMS and identify opportunities for improvement.

Documentation and Communication

Policies, processes, procedures, and records required for ISO 27001 compliance shall be documented, maintained, and regularly reviewed for accuracy and relevance. Effective channels of communication shall be established to disseminate information and documentation and relevant updates to all stakeholders.

Enforcement

The Web Manuals Management System is based on the Principle of Collective Responsibility, meaning that the responsibility for information security rests with the organizational units and personnel performing the actual work. Nonetheless, violations of this Information Security Policy may result in disciplinary action, including but not limited to reprimands, dismissal, and legal action as appropriate.

Review and Approval

This Information Security Policy has been reviewed and approved by Martin Lidgard, CEO, and is effective from December 12, 2023.

DIGITALLY EXECUTED BY MEANS OF PUBLISHING

Martin Lidgard
CEO