WARD & BURKE

Stradbally East
Kilcolgan
Co. Galway

Tel | +353 (0)91 340 100
Email | info@wardandburke.com
Web | www.wardandburke.com

INFORMATION SECURITY POLICY

Signed |  Padraig Burke [Director]
Dated | 21st July 2023

Ward and Burke is committed to maintaining the highest standards of information security to safeguard our valuable assets, ensure the confidentiality, integrity, and availability of information, and protect the interests of our clients, partners, employees, and stakeholders. This Information Security Policy outlines our commitment to ISO 27001 standards and serves as the foundation for our Information Security Management System (ISMS).

Our commitment to information security reflects our dedication to maintaining the trust of our clients, partners, and stakeholders. By adhering to this policy, we ensure the ongoing protection of our information assets and the sustainability of our business operations.

Scope

This policy applies to all employees, contractors, third-party vendors, and stakeholders who access, process, store, or manage company information assets. It encompasses all aspects of information processing, storage, transmission, and disposal within our organisation.

Information Security Objectives

Our information security objectives are set, reviewed and monitored regularly. The ISMS and the objectives are designed to:

a. Ensure the confidentiality, integrity, and availability of information assets.
b. Identify and assess information security risks regularly.
c. Implement appropriate controls to mitigate identified risks.
d. Continuously improve our information security management system.
e. Foster a culture of security awareness and responsibility among all personnel.

Information Security Responsibilities

Top Management: Our leadership is committed to providing the necessary resources, support, and direction to maintain an effective ISMS that complies with ISO 27001.
Information Security Management Team: The appointed ISMT is responsible for overseeing the implementation, maintenance, and continuous improvement of the ISMS. The ISMS lead is a member of the Top Management team.
Employees: All personnel are responsible for adhering to security policies, reporting security incidents, and actively participating in security awareness and training initiatives.

Risk Assessment and Treatment

We undertake a systematic approach to identifying, assessing, and managing information security risks in accordance with ISO 27001. This includes:

a. Identifying information assets and associated risks.
b. Evaluating the impact and likelihood of identified risks.
c. Implementing controls to mitigate or reduce risks to an acceptable level.
d. Regularly reviewing and updating risk assessments as necessary.

Information Security Controls

We implement a comprehensive set of information security controls based on ISO 27001 Annex A, customised to our organisation's needs, and added to as deemed appropriate.

Compliance and Auditing

We commit to conducting regular internal audits and reviews of our ISMS to ensure compliance with ISO 27001 requirements. We also engage in external audits to validate our information security practices and seek certification as evidence of our commitment.

Incident Response

In the event of a security incident or breach, we have established procedures to effectively respond, mitigate, and recover. This includes reporting incidents promptly, assessing impact, notifying relevant stakeholders, and implementing corrective actions.

Security Awareness and Training

We recognise that information security is a shared responsibility. All personnel receive appropriate training and awareness programs to ensure they understand their roles in safeguarding information assets and adhering to security policies.

Continuous Improvement

We are dedicated to continually improving our ISMS based on regular reviews, lessons learned from incidents, and changes in the threat landscape. We encourage all employees to provide feedback and suggestions to enhance our information security practices.