# INFORMATION SECURITY, CYBERSECURITY & PRIVACY PROTECTION POLICY

### Euler Information Security Statement

At Euler, we are dedicated to protecting the confidentiality, integrity, and availability of information while ensuring compliance with cybersecurity and data privacy requirements. This Information Security, Cybersecurity and Privacy Protection Policy is supported by a set of policies and procedures designed to systematically manage risks, enhance resilience against cyber threats, and safeguard personal data.

Our Information Security Management System (ISMS) integrates people, processes, and technology to mitigate information security risks, ensure business continuity, and ensure trust with stakeholders. Euler also prioritises cybersecurity measures to protect against unauthorised access, data breaches, and evolving cyber threats.

### Euler Information Security Objectives for 2025/26

- Information will be accessible only to authorised personnel, safeguarded against unauthorised access, and managed in compliance with privacy regulations (e.g., GDPR, UK Data Protection Act).
- Euler will implement threat intelligence, security monitoring, and vulnerability management to proactively detect and respond to cyber threats.
- Security-by-design principles will be applied to software and cloud environments to prevent vulnerabilities and enforce secure configurations.
- Business continuity and incident response plans will be maintained, tested, and improved to limit the impact of cyber incidents and data breaches.
- All staff will receive ongoing cybersecurity awareness training, and any suspected or actual security incidents will be reported, investigated, and mitigated.
- Euler will ensure compliance with ISO 27001:2022, cybersecurity frameworks, and privacy laws while adapting to evolving security threats.

### Euler Senior Management Team Shall:

- Take full accountability for the effectiveness of the ISMS, cybersecurity, and privacy protection efforts.
- Ensure compliance with all regulatory and legislative requirements, including ISO 27001:2022, GDPR, and other applicable security and privacy laws.
- Allocate and maintain necessary resources for the ISMS, ensuring that all personnel receive appropriate training, support, and guidance to uphold security standards.
- Foster a culture of security awareness by effectively communicating the importance of information security management and adherence to ISMS policies.
- Monitor and evaluate ISMS performance, ensuring that security objectives and intended outcomes are consistently met.
- Actively engage, direct, and empower employees to contribute to the ongoing effectiveness and resilience of the ISMS.
- Drive continuous improvement, regularly reviewing and enhancing ISMS policies, controls, and security measures to address emerging threats and business needs.

### Monitoring & Measuring:

This policy will be reviewed annually by the Senior Management Team and if deemed necessary it will be amended and re-issued.

Job Title: CEO
Name: Rob Jones
Dated**:** 25/02/2025
Signed Rob Jones

Euler.