Group Policy: Information Security

Synthomer produces high-performance, highly specialised chemical products and solutions that bind the modern world together through the broadest range of everyday applications.

Synthomer relies on many categories of information to be able to develop, produce, market and sell our innovative products across the globe. We have an unwavering commitment to provide secure, reliable and accurate information across all facets of the business and protect the data utilizing industry best practices.

The Chief Executive Officer, assisted by the Executive Team, has overall responsibility for implementation of this policy throughout the business. The security of Synthomer's information assets is the responsibility on all management, users, and providers of IT information and services.

Our Information Security Program is built on Synthomer's core commitments. We will:

Comply ▶ Adhere to all applicable laws, regulations, and industry standards concerning information security. Compliance is monitored through regular assessments and policy reviews to ensure alignment with evolving security requirements.

Manage ▶ Actively manage security by employing robust risk management, conducting regular security reviews and maintaining policies that define expectations.

Appoint ▶ Designate key IT personnel to oversee our security program. This includes a Security Steering Committee to lead and the security teams that enforce policies.

Involve ▶ Encourage all employees to follow security standards to help keep Synthomer secure as a shared responsibility. Cross-functional collaboration ensures security considerations are embedded into all aspects of business operations.

Train ▶ Equip employees with the knowledge and behaviours needed to protect company assets. Training covers many topics around cybersecurity and data responsibility.

Expect ▶ Set clear expectations for security compliance and behaviour. Employees, contractors, and third parties must adhere to our security policies, procedures and follow assigned training. Security requirements are integrated into contracts, and service agreements to reinforce accountability.

Report ► Encourage employees to report security concerns, suspicious activity, and policy violations. A structured response process ensures prompt investigation and resolution of security incidents, minimizing impact and preventing recurrence.

Learn & Share ► Continuously refine our security practices by learning from incidents, security research, and industry trends. Lessons learned are documented and shared across teams to improve resilience. Participation in industry forums and collaboration with peers enhance our security knowledge base.

Audit ► Regularly use audit to validate our security controls and ensure compliance with policies and regulations. Periodic control reviews are conducted to ensure compliance to policy. Audit findings drive continuous improvement initiatives, addressing vulnerabilities and reinforcing best practices.

Our Information Security Program is a comprehensive framework designed to protect our organization and stakeholders from security threats. By adhering to our key commitments, we foster a security-first culture that safeguards our data, maintains trust, and upholds compliance requirements. Security is a shared responsibility, and through diligence and collaboration, we ensure the integrity, confidentiality, and availability of our information assets.

M. Wil

Peter Hill
Chair of Synthomer
Synthomer plc
March 2025

Michael Willome
Chief Executive Officer
Synthomer plc
March 2025