element	Document Reference: 115732

Information Security Management System Policy

Issue No: Issue 1	Issue Date:03/09/2025	Effective Date: 28/9/2025	Review Date: 28/9/2027
Author: Andrew Kavanagh Head of Group Management Systems	**Technical Approval:** Stewart Welton Head of Security, EMEAA		**Operational Approval:** Dan Kent Vice President, Operational Development

1.0 SCOPE AND FIELD OF APPLICATION

The purpose of this Information Security Policy is to protect the confidentiality, integrity, and availability of all information assets owned, managed, or processed by Element Materials Technology. This policy establishes the framework for an Information Security Management System (ISMS) in conformance with ISO/IEC 27001:2022, ensuring the protection of sensitive data, compliance with legal and regulatory requirements, and the mitigation of information security risks.

This policy applies at location that conform to ISO27001:2022 to the following:

- All employees, contractors, vendors, and third parties who access or manage Element Materials Technology's information assets.
- All information assets, including physical and digital data, IT systems, networks, applications, and processes, whether stored, processed, or transmitted within or outside the organisation.
- All facilities, equipment, and services used to support Element Materials Technology's operations.

2.0 NORMATIVE REFERENCES

2.1 ISO/IEC 27001:2022

3.0 POLICY

Element Materials Technology is committed to maintaining the security of its information assets through the information Security Management System (ISMS) and we are committed to:

- Protecting the confidentiality, integrity, and availability of information.
- Compliance with all applicable legal, regulatory, and contractual obligations.
- Ensuring the confidentiality of sensitive information, restricting access to authorised individuals only.
- Ensuring the integrity of information by preventing unauthorised modification or corruption.
- Maintaining the availability of information and systems to support business operations.
- Promoting a culture of information security awareness across the organisation.
- Minimising security incidents and their impact through proactive risk management.
- Continually improve the ISMS to adapt to evolving threats and organisational changes.