Global Information Security Policy

1. Purpose

This Global Information Security Policy sets out Infineum's commitment to protecting the confidentiality, integrity and availability of its information assets and constitutes the foundation of Infineum's Information Security Management System (ISMS), aligned with ISO/IEC 27001:2022.

This policy is published to provide customers, partners, regulators and other stakeholders with transparent evidence of Infineum's commitment to information security.

2. Scope

This policy applies, as appropriate to the nature of the activity, risk and contractual relationship, to:

- All Infineum employees, contractors, consultants, temporary staff and any other party acting on behalf of Infineum.
- All information assets owned, processed, stored or transmitted by Infineum, regardless of format, location or technology used.
- All Infineum facilities, business systems, networks, applications and cloud environments globally.
- Third-party suppliers, service providers and business partners who access, process, store or handle Infineum information.

The detailed ISMS scope is defined in the internal ISMS Scope Statement, which is maintained by the Information Security function and reviewed periodically.

3. Information Security Objectives

Infineum is committed to preserving the three core properties of information security and applying them through proportionate organisational, procedural and technical measures:

- *Confidentiality*: ensuring information is accessible only to authorised individuals, entities or processes.
- *Integrity*: safeguarding the accuracy, completeness and reliability of information and *processing* methods.
- Availability: ensuring authorised users can access information and associated assets when required to support business needs.

Measurable security objectives are established, monitored and reviewed at planned intervals, in alignment with Infineum's strategy, obligations and risk landscape.

4. Governance and Risk Management

Information security at Infineum is governed through defined roles, responsibilities and oversight arrangements. Executive Management supports the ISMS and promotes a risk-based approach to the protection of information assets.

Information security risks are identified, assessed, treated and monitored in accordance with Infineum's internal risk management processes. Controls are implemented and reviewed to ensure they remain appropriate to the sensitivity of the information, the criticality of supporting systems and the evolving threat landscape.

5. Legal, Regulatory and Contractual Compliance

Infineum is committed to complying with applicable legal, regulatory and contractual obligations relating to information security, cybersecurity and data protection, including, where relevant:

- The General Data Protection Regulation (GDPR) and applicable national data protection laws.
- Cybersecurity and network and information systems security requirements, including the EU NIS2 Directive and related national implementing legislation.
- Industry-specific regulatory requirements and recognized information security standards.
- Contractual obligations agreed with customers, partners, suppliers and service providers.

6. Awareness, Incident Management and Resilience

Infineum promotes information security awareness through communication, guidance and training appropriate to personnel roles and responsibilities.
Structured processes are in place to report, assess and manage information security events and incidents; actual or suspected incidents must be reported promptly.
Infineum also maintains business continuity and disaster recovery arrangements to support the resilience and availability of critical information systems and services.

7. Continuous Improvement

Infineum is committed to the continual improvement of its ISMS. Information security performance is monitored through planned reviews, internal audits, management review activities and the management of nonconformities, corrective actions and improvement opportunities.

8. Policy Governance

This policy is owned by the Chief Information Security Officer and approved by Infineum's Executive Management. It is reviewed periodically and updated as necessary to reflect changes in Infineum's business, risk profile, regulatory environment or information security objectives.

9. Contact

Questions regarding this policy or Infineum's Information Security programme should be directed to the Information Security Team: ciso@infineum.com