HARDIUM
Information Security

ISO 27001 principles, UK GDPR, NISR (where relevant) Aligned

Document Reference: HARD-IS-POL-001
Version: 1.0
Date: 12th DEC 2025
Owner: Director
Approved By: David Hardy, Founder & Director

Purpose

This policy sets out Hardium Ltd's approach to protecting information assets, ensuring confidentiality, integrity and availability of information used or generated in the delivery of nuclear and high-hazard engineering consultancy services.

Hardium recognises that effective information security underpins regulatory confidence, client trust and safe decision-making.

Scope

This policy applies to all Hardium personnel, associates, contractors and partner SMEs who access, process or manage information on behalf of Hardium, including:

- ✓ Client information
- ✓ Technical and safety documentation
- ✓ Commercial and contractual data
- ✓ Personal data
- ✓ Digital systems and devices

Information Security Principles

Hardium applies a risk-based and proportionate approach to information security, founded on the following principles:

- ✓ Confidentiality – information is accessible only to authorised persons
- ✓ Integrity – information is accurate, complete and protected from unauthorised change
- ✓ Availability – information is accessible when required for legitimate business purposes

Controls and Measures

Hardium implements appropriate controls including:

- ✓ Use of secure, UK-hosted cloud services (e.g. Microsoft 365)
- ✓ Multi-factor authentication for email and core systems
- ✓ Strong password management and device access controls
- ✓ Encryption of devices where practicable
- ✓ Controlled access based on role and need
- ✓ Secure handling and transfer of client information
- ✓ Regular backup of critical information

Hardium avoids unnecessary data replication and limits data access to what is required for delivery.

Incident Management

Any actual or suspected information security incident must be reported promptly to the Director.

Incidents will be assessed, contained, investigated and, where required, reported to affected parties or authorities in line with legal obligations.

Roles & Responsibilities

Founder & Director

- ✓ Overall accountability for information security
- ✓ Approval of this policy
- ✓ Incident oversight

All Personnel and Associates

- ✓ Comply with this policy
- ✓ Protect information under their control
- ✓ Report concerns or incidents promptly

Review

This policy is reviewed annually or following significant change, incident or regulatory development.

Approval

David Hardy
Founder & Director
Hardium Ltd