Information Security Policy

2024.1

June 2024

Table of contents

1. Introduction to Quantium

The Quantium Group (Quantium) is an international group of companies with our head office based in Australia, and with offices in India, New Zealand, South Africa, United Kingdom and USA. The nature of our business, the type of work we do, our business partners and the types of clients we work for are outlined on our website: www.quantium.com. Our core business is to assist our clients to better understand their customers and suppliers.

2. The Quantium view

What it is …
Information security encompasses a set of policies and standards issued by Quantium to ensure the confidentiality, integrity, and availability of information.

What it means …
Everyone associated with Quantium, regardless of their capacity, must comply with the requirements set out in our information security policies and standards as established and maintained in accordance with our Information Security Management System (ISMS).

Who it applies to …
All employees, agency personnel and contracted labour globally.

3. Information security policy

2.1 Policy statement

This Policy seeks to ensure that the confidentiality, integrity, and availability of information is maintained by implementing information security best practice to minimise the impact of threats to Quantium, our clients and our business partners.

2.2 Policy overview

This Policy reinforces the importance of information security to Quantium and sets out the information security policies and standards which are at the core of our Information Security Management System (ISMS). The purpose of our information security policy is to ensure that all information owned by Quantium or held in our custody:

- Can be used with confidence.
- Is accurate and complete; and
- Is adequately protected from misuse, unauthorised disclosure, damage or loss.

4. Information Security Management System (ISMS)

The ISMS sets out Quantium's information security principles, objectives, and requirements which have shaped the development of our policies and standards. The ISMS facilitates continuous improvement of Quantium's information security capability and resilience to emerging and evolving security threats by adopting a risk-based approach.

Quantium's information security culture is driven by a holistic approach which integrates people, processes, and technology requirements into all information security policies. Employees are empowered to understand information security risk and incorporate information security into their everyday working practices and to ensure protection is proportional to the value of the information being managed.

Quantium's ISMS has been implemented by following the International Standard for Information Security, ISO/IEC 27001. The Standard defines the requirements (controls) for an ISMS based on internationally recognised best practice.

3.1 Charter, guiding principles and scope

Charter

To establish and evolve security practices that will enable Quantium to secure its information and system assets while maintaining a positive culture that promotes innovation. Should a conflict occur, cultural and operational activities, including security practices, will be taken into consideration to inform the risk-based decision-making process.

Guiding principles

Security is the responsibility of every Quantium employee, and every employee plays a part in developing and maintaining a culture of security.

a. Security will be prioritised; should a cultural or operational issue clash with this principle, exceptions may be approved by the Group Executive
b. Quantium will use technology wherever possible to address current and future risks
c. Practices implemented will be designed to meet or exceed the security expectations our customers and data partners have of us
d. Industry-standard controls that identify and mitigate information security risks to levels consistent with our risk appetite will be implemented.

Scope

The ISMS encompasses all Quantium systems whether on-prem or cloud based that are accessed locally or remotely (globally) by Quantium employees, contractors, partners and clients. A full description of the ISMS scope can be found in the context and scope of the organisation document.

3.2 Information security objectives

- To ensure an effective control environment, which considers the requirements of ISO 27001, the needs of external parties and Quantium's expectations of its employees in relation to information security, is in place, effectively communicated to the business and subject to ongoing development

- To ensure all employees have a proper awareness and appreciation of their responsibility for information security and are aware that a failure to comply with information security policies will be viewed as a disciplinary matter, which may include action up to and including termination of employment.
- To measure the success of, and identify opportunities for improvement in, the ISMS through the phased rollout of metrics for all implemented controls where technically and operationally practical; and
- To proactively identify, assess and appropriately treat information security risks.

Information security objectives will be set by the Information Security Committee and will be reviewed annually to coincide with financial year planning activities. The aim of aligning information security objectives and budgetary planning is to ensure that adequate funding is allocated to address any identified security gaps and required enhancements.

Objectives are set by the Information Security Committee based upon a clear understanding of business requirements and informed by the current risks, security incident reviews and the views of relevant interested parties. Each business unit is responsible for responding to the overarching objectives set by the Information Security Committee and documenting details of how those objectives will be achieved by that business unit. Each objective will be evaluated and monitored by the Information Security Committee as part of the management review process to ensure those objectives remain valid.

Any amendments to the information security objectives set by the Information Security Committee will be approved at a Group Executive management level before being implemented.

The following properties underpin the decision-making process for the setting of information security objectives by the Information Security Committee.

Property	Description
Confidentiality	Information is not made available or disclosed to unauthorised individuals or third parties.
Integrity	Information is accurate and complete.
Availability	Information is accessible and usable upon demand by authorised individuals, entities, or processes
Authenticity	The identity of a subject or resource is the identity claimed.
Accountability	The ability to map a given activity or event back to the responsible party.

3.3 Business context and interested parties

Business context

Quantium has developed a track record of innovation in data science, combining the best of human and artificial intelligence to power possibilities for individuals, organisations and society. Quantium works with iconic brands in over 20 countries, partnering on their greatest challenges and unlocking ground-breaking opportunities. Quantium implements renowned data handling techniques, without which customers cannot fully realise the strategic and commercial value of their data. The detailed business (organisational) description can be found in the context and scope of the organisation document.

Interested parties

Interested parties are stakeholders such as individuals and organisations that are influenced by Quantium's information security activities, or individuals and organisations that impact our information security activities. In this context, Quantium's clients, data partners, and statutory agencies such as the Office of the Australian Information Commissioner (OAIC) are considered interested parties. Interested parties can be found in the context and scope of the organisation document.

3.4 Information security requirements and communication

The ISMS framework (described in section 3.6) establishes the requirements (controls) for information security within Quantium and requires that all ISMS activity is focussed on the fulfillment of those requirements. Statutory, regulatory and contractual obligations have also been documented and absorbed into the planning process. Specific requirements about the security of new or changed systems and services are addressed as part of the system development lifecycle (e.g. during the planning, design, build, test and operational phases). It is an essential objective of the ISMS that the controls implemented are driven by information security objectives. Such controls will be regularly communicated to all employees through staff onboarding, awareness campaigns, training, education, meetings, and forums. Information security and communication requirements are detailed in the ISMS communications plan.

3.5 Management commitment and continual improvement

Quantium's commitment in relation to the ISMS is to:

a. Achieve and maintain ISO/IEC 27001 certification.
b. Continually improve the effectiveness of the ISMS.
c. Enhance current processes that align with good practice as defined within ISO/IEC 27002 and related standards.
d. Define, implement and monitor information security control metrics to measure control effectiveness and efficiency.
e. Obtain suggestions for enhancements from various sources including employees, clients, partners, suppliers, compliance reports and risk assessments.

3.7 ISMS risk, compliance and audit

In the interests of adopting a risk-based approach to protect Quantium's assets of value and to improve the maturity of the ISMS, a "three lines of defence model" has been implemented. This model is a concise and practical way to strengthen communications on risk management, assurance and control by clarifying essential roles and responsibilities regarding governance functions such as compliance and audit in addition to day-to-day operational activities. The three lines of defence are set out below:

First line of defence – risk identification

Quantium business units are responsible for day-to-day risk management activities ensuring operational risks are identified and addressed in line with Quantium's operational risk management practices. Also, and in the interests of continuous improvement, operational teams are subject to ongoing control assurance (compliance) testing.

Second line of defence – risk assessment

Quantium's Risk and Compliance team conduct activities designed to identify, assess and manage risks. Examples include, but are not limited to, risk workshops, security control deficiencies analysis and post-security incident reviews. The team also validates the first line of defence and reports Quantium's risk position to the Risk and Audit Committee.

Third line of defence – risk monitoring

At this level, independent audits are conducted to validate the effectiveness of the first and second lines of defence. Further details can be found in the Procedure for internal audits of the ISMS document.

3.8 Adherence to policy

The requirements of this Policy and the ISMS framework must be complied with. Failure by an employee to comply with these requirements may result in disciplinary action being taken, up to and including termination of employment.

5. Document management

Owner	Adam Driussi - Chief Executive Officer	Authoriser	Kyle Evans - Group Executive, Technology & Delivery
ISMS reference	Information Security Policy (external)	Next review date	June 2025

END OF DOCUMENT