quantium

Information security policy

August 2021

Table of contents

Information security policy

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

1. The Quantium view

What it is?

Information security encompasses a set of policies and standards to ensure the confidentiality, integrity and availability of information.

What it means?

Everyone associated with Quantium must comply with the requirements set out in our information security policies and standards, as maintained in accordance with our Information Security Management System (ISMS).

Who it applies to?

All employees, agency personnel and contracted labour globally.

2. Information security policy

2.1 Policy statement

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

2.2 Policy overview

Quantium will ensure that all information we own or hold:

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

3. Information Security Management System (ISMS)

Quantium's ISMS sets out Quantium's information security principles, objectives and requirements and facilitates continuous improvement of our capability and resilience to emerging and evolving security threats.

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 risks and incorporate information security into their everyday working practices.

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 culture that promotes innovation.

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;

b. Quantium will use technology wherever possible to address current and future risks

c. Practices implemented will be designed in consideration of 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 Quantium ISMS encompasses all Quantium systems that are accessed locally or remotely (globally) by Quantium employees, contractors, partners and clients.

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.

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

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.

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.

3.4 Information security requirements and communication

The ISMS framework 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.

3.5 Management commitment and continual improvement

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

a. 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 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. 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 Management 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.

4. Document management

Owner	Adam Driussi - Chief Executive Officer
Authoriser	Kyle Evans - Group Executive, Product & Technology
Reference	Information security policy (External)
Next review date	June 2022

END OF DOCUMENT