Information Security Policy

Version	3.6
Document Status	Published
Classification	Public
Published Date	September 2026
Next Review Date	September 2027
Intended Audience	Quantexa Employees, Partner Organisations, Contractors, and Other Interested Parties
Document Owner	Head of Information Security

Contents

1. Background 2
2. Purpose 2
3. Scope 2
4. Definitions 3
5. Roles and Responsibilities 3
6. Information Security Policy 4
7. ISMS Scope 5
8. ISMS Objectives Overview 5
9. Regulatory Compliance 6
10. Violations and Enforcement 6
11. Referenced Documents 6
12. Revision and Approval Log 7
    - 12.1 Change History 7
    - 12.2 Approval History 7

1. Background

Information and systems are considered valuable Quantexa assets which all require protection against varying types of internal and external security risks. These risks have the potential to threaten the confidentiality, integrity, and availability of Quantexa assets. Quantexa is committed to promoting effective controls across the range of information, technical, personnel, and physical security to maintain the confidentiality of our and our clients' data. We will maintain and protect all the information we use or store in a manner consistent with our relevant professional, ethical, legal, regulatory, and contractual requirements.

Quantexa's Senior Leadership Team, represented by the Head of Information Security and the Risk Committee fully endorse and support all Information Security policies, standards, guidelines, processes, and procedures. These measures are strictly enforced across the organisation to support the continuous improvement of the Information Security Management System (ISMS).

Information security is at the core of our culture. We educate and regularly update our employees, so they understand our security expectations and recognize the evolving threats to the security of our information.

The ISMS is maintained through controls set out in our various policies, standards, guidelines, processes, and procedures, ensuring that Quantexa meets its obligations to its stakeholders and clients. These controls are continuously monitored, reviewed, and improved to align with security and business objectives while adhering to statutory and contractual requirements.

Quantexa operates an information security awareness and compliance programme through company inductions, training, and regular internal and external audits. All employees are encouraged to report potential security weaknesses, events, and/or incidents via the appropriate management/information security channels.

This policy will be reviewed annually, or within planned and agreed intervals, to determine whether it has achieved its intended outcome(s) over the past year, to review the objectives going forward and to identify opportunities for continual improvement.

2. Purpose

The purpose of this policy is to:

- Ensure full compliance with the requirements of ISO/IEC 27001;
- Protect information from unauthorised access;
- Maintain the confidentiality of information;
- Preserve the integrity of information by safeguarding it against unauthorised modification;
- Ensure the availability of information to authorised users as and when needed;
- Prevent unauthorised or accidental disclosure of information to unauthorised individuals;
- Outline Quantexa's commitment to safeguarding information assets and information systems;
- Ensure compliance with the cloud service-related requirements of ISO/IEC 27017; and
- Effectively manage risks associated with third-party cloud services.

3. Scope

This policy applies to all employees, including staff and contractors, as well as partner organisations that have access to Quantexa's information or technologies as part of employment contracts or contracted work agreements.



4. Definitions

Terms	Definitions
Confidentiality	The assurance that information is not accessible or disclosed to unauthorised individuals, entities, or processes.
Integrity	Safeguards that protect information from unauthorised modification, ensuring the accuracy and completeness of data.
Availability	Measures that ensure timely and reliable access to systems and data when needed.
Board of Directors (BoD)	An elected group of individuals that represent shareholders. The Board is a governing body that typically meets at regular intervals to set policies for corporate management and oversight.

5. Roles and Responsibilities

Role	Responsibilities
All Staff (Including third parties and partners, regardless of location)	• Comply with the requirements of this policy; • Support information security initiatives by promoting awareness of its importance and adhering to security requirements; • Identify and manage risks related to information security; and • Comply with the Security Behaviour Policy and fulfil any role-specific responsibilities.
Information Security Team	• Continuously improve and update the ISMS to ensure it accurately reflects the agreed scope; • Ensure that this policy, along with its principles and requirements, is consistently implemented, managed, and maintained; • Establish and align the Information Security Policy and objectives with Quantexa's strategic direction; • Integrate ISMS requirements into Quantexa's business processes; • Support information security initiatives that align with the organisation's needs; • Ensure adequate resources are available for the ISMS, in collaboration with the Risk Committee; • Guide and support staff in contributing to the effectiveness of the ISMS; and • Promote continual improvement in information security throughout the organisation.
Executive Committee (ExCo)	• Approve this policy and ensure full support for its implementation; and • Ensure the integration of the ISMS requirements into Quantexa's business processes.
Risk Committee and Chief Operating Officer (COO)	• Provide management oversight of the ISMS. • Review objectives for the ISMS performance monitoring. • Assist in establishing Quantexa's information security strategy and improvement programme. • Review risk assessments, approve mitigation and treatment strategies, or accept risks as appropriate.

	• Ensure security functions, and supporting departments, are adequately resourced with trained staff to meet security goals. • Provide oversight of key decisions that impact overall strategy or information security risk. • Serve as the point of escalation for significant security matters.
Business and IT Leadership	• Understand and implement relevant controls from this policy and associated ISMS documents within their business areas.
All Risks Owners and Department Managers	• Coordinate, monitor, and manage their department's individual risk requirements; and • Ensure the implementation, management, and maintenance of this policy and security principles within their business area.
External Parties	• Comply with the requirements of this policy; and • Understand the Information Security Policy, relevant ISMS documentation, and associated processes.

6. Information Security Policy

Under the instruction of the Senior Leadership Team, Quantexa is required to develop, implement, and maintain an ISMS that is compliant with, and independently certified to, the ISO/IEC 27001 and ISO/IEC 27017 standards. The ISMS is designed to:

- Provide assurance to the organisation, clients, and relevant stakeholders that the confidentiality, integrity, and availability of information are maintained appropriately;
- Manage information security risks to Quantexa and client data assets;
- Protects Quantexa's ability to meet contracted commitments by maintaining and testing business continuity plans to counteract disruptions and safeguard critical business processes from major failures or disasters;
- Establish and enforce policies, standards, guidelines, processes, and procedures that support this Information Security Policy, reviewed at least annually to ensure effectiveness in meeting business requirements for confidentiality, integrity and availability;
- Address business, legal, regulatory, and contractual security obligations;
- Promote security awareness across the organization, ensuring employees can recognize and meet contractual, legislative, and company-specific security responsibilities;
- Ensure that actual or suspected security incidents are reported promptly and acted upon effectively to minimise business impact;
- Demonstrate leadership and commitment from the Senior Leadership Team by supporting management in the development of policies, standards, guidelines, processes, and procedures; and
- Implements incident management and escalation procedures to ensure timely reporting, investigation, and review of security incidents for management action.

7. ISMS Scope

7.1 Scope Statement - ISMS

Quantexa operates an Information Security Management System which complies with requirements of ISO/IEC 27001:2023 and ISO/IEC 27017:2015 for the following scope:

"The people, processes, and technologies that handle, transmit, store and process digital information assets, which enable the deployment, support, development, and management of Decision Intelligence Powered Solutions. This is in accordance with Statement of Applicability version 4.0 dated 17/09/2025."

7.2 Scope Statement - Certificate

Quantexa operates an Information Security Management System which complies with requirements of ISO/IEC 27001:2023 and ISO/IEC 27017:2015 for the following scope:

"The management, development, deployment, and support of Decision Intelligence Powered Solutions. This is in accordance with Statement of Applicability version 4.0 dated 17/09/2025."

*Please note that the scope statement on the certificate has been refined in line with BSI external auditor requirements.

8. ISMS Objectives Overview

This policy is supported by the following high-level objectives:

Objective ID	High Level Objectives
1	Information Governance, Assurance and Reporting Establish and maintain compliance to information security best practice.
2	Enhanced Logging, Monitoring and Management
3	Enhanced Cyber Awareness
4	Business & Cyber Resilience Programme
5	Integrate, establish and maintain an Information Risk Management Framework
6	Organisation and Talent Management
7	Establish and maintain Supplier Assurance
8	Ensure the Confidentiality, Integrity and Availability of Quantexa information and systems for effective management of Quantexa information security management system

To support these objectives, Quantexa is committed to the continuous improvement of its ISMS by setting and reviewing specific ISMS objectives annually. These objectives evolve based on business needs, ensuring compliance with all applicable requirements and enhancing the ISMS's effectiveness.

9. Regulatory Compliance

Quantexa evaluates its compliance with legal and regulatory requirements on an annual basis. This involves reviewing existing and emerging legislation to ensure ongoing adherence. The evaluation is documented to identify applicable laws and regulations and to demonstrate how Quantexa meets these requirements.

Any changes in legislation or regulatory obligations are communicated to relevant personnel, including contractors, as necessary. Where required, additional training will be provided to ensure that all affected individuals understand and comply with these changes.

For clarity, Quantexa's compliance with data protection requirements includes adherence to the Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), and other applicable data privacy laws and regulations. This includes compliance with any guidance or codes of practice issued by regional Information Commissioner or Supervisory Authorities (SA).

10. Violations and Enforcement

We encourage the reporting of non-compliance or policy breaches to ensure transparency and drive improvement in our organisation's practices. Please use the procedures outlined in the Speak Up Policy for reporting. Individuals found in violation of this policy or other organisational policies may be subject to disciplinary action in line with applicable People Team policies, contractual obligations, and legal or regulatory requirements.

11. Referenced Documents

- ISO/IEC 27001 Certificate
- ISO/IEC 27017 Certificate
- ISO/IEC 27001 Standard
- ISO/IEC 27017 Standard
- ISMS Manual
- Security Behaviour Policy
- Statement of Applicability

12. Revision and Approval Log

12.1 Change History

Version	Date	Role	Revision Notes
3.2	March 2023	Information Security Analyst	Document review and updated to reflect ISO/IEC 27017.
3.3	September 2024	Senior GRC Analyst	Minor updates throughout to improve readability.
3.4	February 2025	Information Security Analyst	ISMS Objectives Overview updates.
3.5	September 2025	Information Security Analyst	Annual document review.
3.6	April 2026	Senior GRC Analyst	Updated ISMS Scope statements.

12.2 Approval History

Name and Role	Action (i.e., version approval, annual review)	Action Date
Chief Executive Officer	Version 3.2 approval.	March 2023
Chief Financial Officer	Version 3.2 approval.	March 2023
Chief Technology Officer	Version 3.2 approval.	March 2023
Chief Product Officer	Version 3.2 approval.	March 2023
Chief Architect	Version 3.2 approval.	March 2023
Head of Information Security	Annual review with no substantial changes.	September 2023
Senior GRC Analyst	Annual review with no substantial	September 2023

	changes.	
Head of Information Security	Version 3.3 approval.	October 2024
Head of Information Security	Version 3.4 approval.	February 2025
Head of Information Security	Version 3.5 approval.	October 2025
Head of Information Security	Version 3.6 approval.	April 2026
Senior GRC Analyst	Annual review with no substantial changes.	September 2026