# Information Security Policy

BS ISO/IEC 27001:2013 & BS ISO/IEC 27017:2015

Date: March 2023
Version: 3.2
PUBLIC

# 1 Contents

# 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.

The Quantexa Board of Directors (BoD) and the Senior Management team, represented by the Head of Information Security and the Information Security Steering Group (ISSG), fully endorse all information security policies and standards, and expects them to be adhered to. Prescribed controls will be implemented consistently throughout the organisation supporting the continuous review and improvement of the Information Security Management System (ISMS).

Information security is at the core of our culture. We ensure that we educate our people and regularly refresh their knowledge, so they all have a clear understanding of our expectations and hold an appreciation of the changing nature of the threats to the security of our information.

The ISMS is achieved using controls set out within the various policies, standards, guidelines, processes, and procedures. Conforming with these controls is critical in ensuring that Quantexa meets all its obligations to its stakeholders and clients.

These controls are continually monitored, reviewed, and improved upon to ensure that security and business objectives are met. This is operated in conjunction with other business management processes and incorporates the applicable statutory and contractual requirements.

Quantexa operates a programme of information security awareness and compliance through company inductions, training, internal and external audits.

All employees are empowered to identify any potential security weaknesses, events and/or incidents and report through the appropriate management/information security channels.

The policy will be reviewed annually by the Head of Information Security, 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 all of the requirements detailed within ISO/IEC 27001 are met;
- Ensure information is protected against unauthorised access;
- Ensure Confidentiality of information is maintained;
- Ensure information is not disclosed to unauthorised persons through deliberate or careless action;
- Ensure the Integrity of information through protection from unauthorised modification;
- Ensure Availability of information to authorised users when needed;
- Outline Quantexa's commitment to safeguarding information assets and information systems;

- Ensure compliance with the cloud service-related requirements outlined in ISO/IEC 27017 are successfully monitored and met; and
- Ensure any risks associated with third-party cloud services used are effectively managed.

# 3. Scope

This policy applies to all employees (e.g., staff, contractors) and partner organisations who have access to Quantexa information and technologies as part of any employment contracts or contracted scope of works.

# 4. Definitions

| Terms | Definitions |
|---|---|
| **Confidentiality** | The property that information is not made available or disclosed to unauthorised individuals, entities, or processes. |
| **Integrity** | Measures are in place to protect information from unauthorised modification. These measures provide assurance in the accuracy and completeness of data. |
| **Availability** | Measures are in place to protect timely and uninterrupted access to systems and its data. |
| **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 and regardless of location)** | • Comply with the requirements of this policy;<br>• Support all information security initiatives by communicating the importance of effective information security to others, and conforming to the information security requirements;<br>• Identify and manage risk which is at the core of information security; and<br>• Comply with the Security Behaviour Policy and understanding any role-specific responsibilities. |
| **Information Security Team** | • The continual improvement and updates to the ISMS so that it accurately reflects the agreed scope;<br>• Ensure that this document and information security principles and requirements contained within are continuously implemented, managed, and maintained;<br>• Ensure that the Information Security Policy and the information security objectives are established and are commensurate with the strategic direction of Quantexa;<br>• Ensure the integration of the ISMS requirements into |

| | |
|---|---|
| | Quantexa's business processes;<br>• Demonstrate ongoing commitment through supporting the information security initiatives that are commensurate to the organisation;<br>• Ensure that the resources needed for the ISMS are available in conjunction with the ISSG;<br>• Direct and support persons to contribute to the effectiveness of the ISMS; and<br>• Promote continual information security improvement within and around the organisation. |
| **Senior Management and Board of Directors** | • Approve this policy and ensuring full support for its implementation; and<br>• Ensure the integration of the ISMS requirements into Quantexa's business processes. |
| **Information Security Steering Group** | • Provide management oversight of the ISMS;<br>• Define metrics and KPIs needed to monitor the ISMS in line with our ISMS Performance Monitoring Standard;<br>• Define the Quantexa security strategy and improvement programme and align business and IT departments to support the implementation of Information Security Policy and the ISMS documents;<br>• Review risk assessments, agreeing mitigation and treatment strategies or accepting risk if deemed fit for the business;<br>• Ensure the security functions, and supporting departments are appropriately resourced with adequately skilled and trained staff to deliver upon this strategy and any required risk treatments;<br>• Take key decisions that affect the overall strategy or information security risk; and<br>• Act as the point of escalation for security matters. |
| **Business and IT Leadership** | • Understand and implement any relevant controls within their business area which stem from this policy and all relevant flow down policies within our ISMS. |
| **All Risks Owners and Department Managers** | • The overall coordination, monitoring, and management of their individual risk requirements; and<br>• Ensuring that this document and information security principles are implemented, managed, and maintained within their business area. |
| **External Parties** | • Comply with the requirements of this policy; and<br>• Have a clear understanding of the Information Security Policy and relevant ISMS documentation and its associated processes. |

# 6. Information Security Policy

Under the instruction of Senior Management and the Board of Directors, it is a mandated requirement to develop, implement and maintain an ISMS and the implementation of an organisation wide ISMS that is compliant and independently certified to the ISO/IEC 27001 and ISO/IEC 27017 standard that:

- Provides assurance within the organisation and to our clients, and other relevant stakeholders that the availability, integrity, and confidentiality of their information will be maintained appropriately;
- Manages information security risks to Quantexa and client data assets;
- Protects Quantexa's ongoing ability to meet contracted commitments through appropriate business continuity plans which should be maintained and tested to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of disasters;
- Contains policies, standards, guidelines, processes, and procedures to support this Information Security Policy which will be reviewed at least annually to ensure they are effective. Business requirements for the confidentiality, integrity and availability of information and information systems will be met and managed through these policies;
- Considers business and legal or regulatory requirements, and contractual security obligations;
- Maintains security awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities;
- Reports and acts effectively upon actual or suspected security incidents to minimise any business impact;
- Senior Management and the Board of Directors demonstrate leadership and commitment to the ISMS by supporting the management layer in providing direction and guidance in the form of policies, standards, guidelines, processes, and procedures; and
- Implements incident management and escalation procedures for reporting and investigation of security incidents for management review and action.

# 7. ISMS Scope

The current certified scope is:

*"The Quantexa Information Security Management System (ISMS) covers people, processes and technology that handle, transmit or store Quantexa's physical and digital information assets across the Quantexa offices regardless of the individual's location. The ISMS covers internal and externally contracted personnel who have access to Quantexa's information and systems, the development and the support of the Entity Resolution and Network Analytics software products for our customers to deploy within their own infrastructure and within Quantexa's own cloud infrastructure."*

# 8. ISMS Objectives Overview

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

- Implementation of an ISMS that is compliant and independently certified to the ISO/IEC 27001 and aligns and meets the requirements detailed within ISO/IEC 27017 Standard (Cloud Services);
- Implementation of an information security risk assessment process that assesses the business impact likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented;
- Development and implementation of a business continuity plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters;

- Defined security-controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information;
- Provide information security awareness guidance and training for all employees on an ongoing basis;
- Implement and manage a supplier assessment and management programme that is commensurate to supply chain risk profile;
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for ISMS management review and action.

In support of these high-level objectives, Quantexa will continually improve the activities by establishing specific ISMS objectives which are subject to change based on business requirements. These are set annually and reviewed on a regular basis. We are committed to complying with all applicable requirements in relation to information and continually improving the effectiveness of the ISMS.

# 9. Regulatory Compliance

Quantexa evaluates its compliance with legal and regulatory requirements on an annual basis. This involves a review of current and any new legislation. The evaluation will be documented to identify and demonstrate applicability of how Quantexa complies with current regulations and laws. Any changes to our legislative requirements will be communicated and any other persons who may be affected, e.g., contractors and where required, additional training will be provided for anyone affected by the changes.

To provide further clarity, compliance with various data protection requirements such as Data Protection Legislation means the Data Protection Act 2018, the EU General Data Protection Regulation and applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the in-region information commissioner or supervisory authority (SA).

# 10. Violations and Enforcement

Any person found to have violated this policy and other policies within the ISMS may be subject to disciplinary action, up to and including termination of employment. Non-compliance with or breach of this policy will be reported to the violator's line manager and/or mentor and the Information Security team.

# 11. Referenced Documents

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

# 12. Document Control

| | | | |
|---|---|---|---|
| **Author** | | | |
| **Role** | Head of Information Security | | |
| **Version** | 3.2 | | |
| **Creation Date** | July 2021 | | |
| **Next Review** | September 2023 | | |
| **Classification** | Public | | |
| **Revision notes** | Document review and update to reflect ISO/IEC 27017. | | |
| **Approvals** | | | |
| **Name** | **Role** | **Date** | |
| | Chief Executive Officer | March 2023 | |
| | Chief Financial Officer | March 2023 | |
| | Chief Technology Officer | March 2023 | |
| | Chief Product Officer | March 2023 | |
| | Chief Architect | March 2023 | |
| **Annual Review and Approval** | | | |
| **Name** | **Role** | **Revision Notes** | **Date of Approval** |
| | Senior GRC Analyst | Annual review with no substantial changes. | September 2022 |
| | Head of Information Security | Annual review with no substantial changes. | September 2022 |