ARQIVA

Information Security Policy

SYI-PY-001

v5.3

ARQIVA

Purpose

This policy sets out Arqiva's commitment to Information Security and provides a high-level overview of how Information Security is managed across the organisation.

Scope

This policy applies to all Arqiva's information assets, data, systems, and the individuals who use them, including employees, temporary employees, contractors, service providers, business partners and any other external parties.

Policy Statement and Our Commitment

Arqiva is committed to protecting the confidentiality, integrity, and availability of the information assets entrusted to us by our customers, partners, employees, and stakeholders. Safeguarding information is essential to maintaining trust, supporting operational excellence, and achieving our strategic objectives.

To ensure we consistently identify, manage, and mitigate information security risks in line with our corporate risk appetite, Arqiva commits to:

- Protecting all information assets against unauthorised access, disclosure, alteration, or loss.
- Preserving the accuracy, reliability, and completeness of information.
- Ensuring information and systems remain available to authorised users when required.
- Maintaining controls that meet all relevant legal, regulatory, and contractual requirements.
- Ensuring everyone who accesses Arqiva information or systems understands their responsibilities and follows defined best-practice security behaviours.
- Ensuring all actual or suspected information security incidents are promptly reported, documented, and investigated.

Arqiva works closely with customers and suppliers to establish and maintain secure working practices and engages with government, regulators, and industry bodies to exchange threat intelligence and strengthen our collective security posture.

Any third party that stores, processes, or transmits Arqiva information assets must comply with this policy, in many cases supported by additional regulatory or licensing obligations.

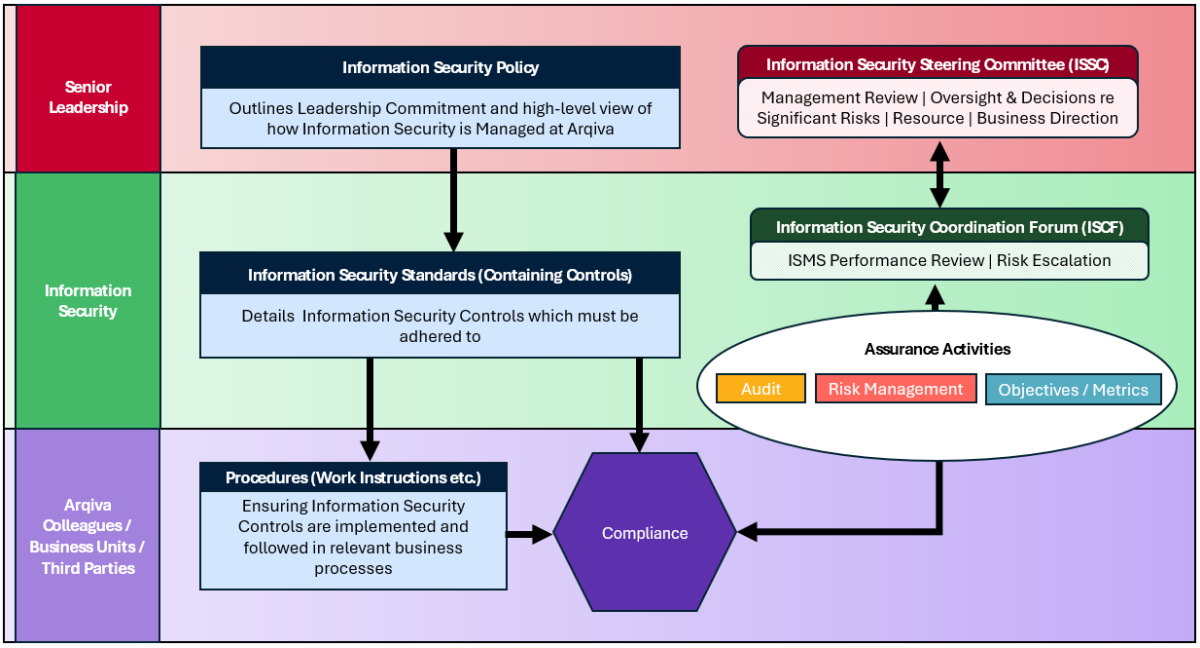
Recognising the evolving nature of the information security landscape, Arqiva remains committed to continuously improving its Information Security Management System (ISMS), so it remains effective, adaptive, and aligned with emerging threats, technological developments, and changes in business operations.

By embedding security into everything we do, we help ensure a secure and resilient future for Arqiva and our partners.

How Information Security Is Managed at Arqiva

Arqiva manages information security through a structured Information Security Management System (ISMS). As illustrated in the diagram below, our ISMS is built on the following core elements:

- **Information Security Policies**: This document, along with supporting policies across key security domains, sets out Arqiva's commitment to information security and provide a high-level overview of how information security is governed and managed across the organisation.
- **Information Security Standards**: These standards define the specific controls and requirements that must be followed. These controls and requirements are also communicated to their audience through targeted communications and training activities.
- **Assurance Activities**: These include risk management, audit, and the tracking of objectives and metrics, alongside other validation activities. These measures give the Information Security Team clear insight into the effectiveness of our controls and the level of organisational compliance.
- **Information Security Coordination Forum**: This group provides a dedicated forum for reviewing assurance findings, discussing new or emerging issues and threats, and escalating any significant risks to the Information Security Steering Committee.
- **Information Security Steering Committee**: The Steering Committee makes decisions on major information security risks, reviews the performance of the ISMS, ensures appropriate resourcing aligned to our risk appetite, and provides strategic direction for the business.



Arqiva is recognised as a leader in secure service delivery, and our certification to ISO/IEC 27001:2022 reflects our commitment to maintaining and continually improving our ISMS.

Responsibility and Authority

The CEO and Senior Leadership Team are responsible for:

- Ensuring this policy is communicated, understood, and effectively implemented across the organisation.
- Providing the necessary resources, governance, and processes to support the Information Security Management System (ISMS).
- Reviewing and approving the Information Security Policy at least biennially (every 2 years).
- Overseeing the management of significant information security risks.

ARQIVA

Information Security teams are responsible for:

- Maintaining and operating Arqiva's Information Security Management System (ISMS).
- Developing, updating, and communicating security policies, standards, and controls.
- Monitoring compliance and escalating significant security risks or incidents.
- Providing expert guidance and leading information security incident response activities.

All staff, and anyone granted access to Arqiva technology or information, are responsible for:

- Reading and complying with this policy and all relevant information security standards, controls, and procedures.
- Using Arqiva systems responsibly and completing required security training.
- Applying secure behaviours in their daily work and promptly reporting any suspected or actual security incidents.
- Protecting Arqiva information in all working environments, including on-site, remote, or when representing the organisation externally.
- Handling Arqiva information in accordance with classification and handling rules (as defined in the information security standards) and consistently acting with due care, integrity, and respect for its sensitivity.

Review

The CEO of Arqiva will review the Information Security Policy at least biennially (every 2 years) to ensure its continued applicability and effectiveness.

Shuja Khan Date: 28/08/2026

Chief Executive Office