Information Security Policy
SYI-PY-001

Arqiva enables a switched-on world to flow. Arqiva is at the heart of broadcast and utilities in the UK and abroad. Everything Arqiva creates is aimed at meeting the needs and expectations of our customers and will be compliant with customer, statutory, regulatory, internal and industry safety and quality requirements.

Policy Statement

Information security provides a vital component in ensuring the confidentiality, integrity and availability of information and data and is embedded in the products and services we deliver to our customers, suppliers, and staff. We are recognised as an industry leader for the provision of secure services, and our continued commitment and delivery is recognised through the certification to and continual improvement of ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection as the framework for information security.

To provide all of our stakeholders with the assurance that Arqiva identifies and manages its information security risks (both business and technical) within the corporate risk appetite, Arqiva will:

- protect information assets and data against unauthorised access;
- maintain the accuracy and completeness of information assets and data;
- make information assets and systems available to all authorised users as and when required.

Arqiva will implement information security controls to:

- meet applicable legal, regulatory, and contractual requirements;
- ensure that all individuals using Arqiva's information assets, data and systems comply with defined best practice and are made aware of their information security responsibilities;
- ensure that all breaches of information security, actual or suspected, are reported, documented and fully investigated.

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. The scope includes information or data that is stored on devices or systems, processed by business applications, transmitted across networks, printed out or written down, sent by post, stored on removable media, or spoken in conversation.

In a connected world, none of us can work in isolation. Arqiva will work with its customers and suppliers to define and implement secure working arrangements. Arqiva maintains close relationships with government, government agencies, a regulators and other organisations to share information security knowledge and threat intelligence.

Any downstream business partners that store, process or transmit Arqiva information assets must adhere to and implement this policy. In some cases this is a regulatory requirement or requirement for licensing.

Arqiva recognises that the information security landscape is constantly evolving and changing. Arqiva is committed to the continual improvement of its Information Security Management System (ISMS) and other information security frameworks, updating them as required in response to emerging threats, technological advancements, and changes in Arqiva's business processes, threat and risk profiles identified through internal or external sources.

By working together and embedding security into our DNA, we can all help create a secure future for Arqiva and our business partners.

Responsibility and Authority

It is the responsibility of the Chairman and CEO of Arqiva and management teams at all levels throughout the business, to ensure the communication, understanding and implementation of this policy by providing the necessary platforms, processes, procedures, resources and training to ensure that all the employees can deliver products and services to our customers consistently through capable, compliant and controlled processes.

It is the responsibility of all staff and others granted use of and/or access to Arqiva technology resources.to voice concerns regarding the ability to meet customer requirements and comply with:

- the requirements of this policy
- all parts of our Information Security Management System

Together we shall meet these commitments through:

- clearly documented plans
- documented guidance
- awareness raising and education campaigns
- control reviews and risk assessments
- your individual support

To that end, employees should promptly report:

- Any questions or concerns about interpreting this policy or its application to their jobs;
- Any concerns involving a violation or possible violation of this policy, to their managers or the Information Security team.

Review

The CEO of Arqiva will review the Information Security Policy annually to ensure its continued applicability and effectiveness.

Shuja Khan **Date: 21/11/2024**

Chief Executive Officer