RWS Group

ISMS Policy

Table of Contents

Scope

RWS is the world's leading provider of technology-enabled language, content management and intellectual property services. We help our customers to connect with people globally by communicating business critical content at scale, and enabling the protection and realization of their ideas and innovations.

Our customers place their trust in RWS every day. We have a responsibility to manage and protect the information and assets of our customers in exactly the same way we protect our own. RWS Executives, Management and the Security Governance, Risk and Compliance team take this responsibility very seriously and are fully committed to maintaining and improving the Information Security Management System (ISMS) as part of RWS' business strategy.

This ISMS policy details the approach RWS Holdings plc, its affiliates and its subsidiaries ("RWS") takes and applies to all RWS employees, contractors and vendors with access to RWS systems, facilities or information in any form whilst supporting global operations in any capacity. It is the responsibility of each person to whom this policy applies to remain fully conversant with the latest versions of this and other RWS information security and privacy policies and processes applicable to their role.

RWS' ISMS consists of the people, processes and technologies required to ensure an effective and appropriate risk-based approach to the selection, implementation, monitoring and management of the security, privacy and business continuity controls necessary to support business aims. The ISMS is designed to protect information and assets from threats and vulnerabilities, whether internal or external, deliberate or accidental. The Top Management Sponsor and owner of this policy is the Chief Technology and Information Officer.

Policy

All employees and contractors shall contribute to the protection of RWS and customer information, assets and personnel by:

- Protecting facilities, resources and information from unauthorized access
- Handling information and assets in accordance with Group and Divisional policies and practices to protect their confidentiality, integrity and availability
- Complying with regulatory and legislative requirements
- Producing, testing and maintaining business continuity plans
- Undertaking information security awareness and training relevant to their role

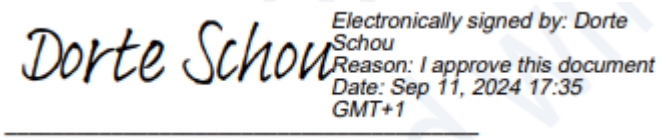
- Reporting as soon as possible actual or suspected security incidents to ensure they can be appropriately investigated
- Monitoring the performance of security controls regularly to ensure continued effectiveness and timely identification of weaknesses
- Reviewing policies and processes regularly to ensure their relevance and their continued support to business aims

Each of these objectives is governed and implemented according to one or more Information Security and Privacy Policies. All RWS Information Security and Privacy Policies are available via the RWS Group Intranet.

It is the individual responsibility of all RWS employees and contractors to comply with the security and privacy policies and processes. Managers are responsible for ensuring the implementation of policies within their business areas. Deliberate or persistent failure to comply with RWS policies may result in administrative or disciplinary action being taken.

Policy Review

You can access this Policy by visiting the RWS Hub and navigating to the Group Policies section. This Policy will be reviewed regularly and updated as required to ensure it remains effective and aligned with our organizational goals. If there are any material changes to the Policy, it will be relaunched through the RWS Hub for review by all Colleagues or by training or email communication, depending on the level modification to the Policy.



D Schou
Chief Technology and Information Officer

Document History

Author	Date	Detail	Version
Security	27/05/2021	Approved	1.0
Security	04/09/2023	Approved	2.0
Security	10/09/2024	Approved	3.0