

**Hello,  
world.**

## **RWS Group**

ISMS Policy

**Author:** Russell Frith

**Approver:** Dorte Schou

**Version:** 4.0

**Issue Date:** 16/12/2025

**Next Review Date:** 16/12/2026

**Classification:** Public

**Retention Period:** Until superseded

# 1 Purpose and Strategic Alignment

At RWS, our ambition is to be the world's most trusted partner for global content solutions. Trust is foundational to our success – enabling growth, understanding, and confidence across every market, language, and surface. This Information Security Policy sets out our strategic commitment to protecting the confidentiality, integrity, and availability of information and assets – both our own and those entrusted to us by our clients and partners. It reflects our belief that security is not just a safeguard, but a strategic enabler of innovation, transformation, and global collaboration.

## 2 Scope

This policy applies to all RWS entities, affiliates, and subsidiaries (“RWS”), and to all employees, contractors, and vendors who access RWS systems, facilities, or information in any form. It governs the principles and practices of our Information Security Management System (ISMS), which is designed to support our business strategy through a risk-based, resilient, and continuously improving approach to security, privacy, and business continuity.

## 3 Information Security Objectives

The following objectives support the RWS strategic pillars of Generate, Transform, and Protect. They are reviewed annually, aligned with risk assessments, and monitored through key performance indicators (KPIs) maintained separately in the ISMS performance framework. RWS is committed to the continual improvement of the ISMS to ensure these objectives remain effective and relevant.

### 3.1 Secure Intelligent Content Generation

Safeguard Generative AI tools and enterprise publishing platforms to ensure the confidentiality, integrity, and availability of data and outputs, enabling secure, scalable production and distribution of intelligent content.

### 3.2 Embed Trust in Human-Centric Communication

Protect personal and sensitive data across Linguistic AI and localization services to guarantee confidentiality, integrity, and availability, delivering compliant and trusted communication in every end market.

### 3.3 Safeguard Innovation with Confidence

Secure the patent lifecycle to maintain the confidentiality, integrity, and availability of intellectual property, helping innovators protect ideas worldwide.

### 3.4 Foster a Security-Aware Culture

Promote cross-functional ownership of security through training, awareness, and collaboration, embedding confidentiality, integrity, and availability practices across all operations.

### 3.5 Ensure Operational Resilience

Implement and test business continuity and disaster recovery plans to preserve the confidentiality, integrity, and availability of critical content pipelines, localization services, and patent systems.

### 3.6 Drive Continual Improvement of the ISMS

Continuously monitor, assess, and enhance the ISMS to strengthen confidentiality, integrity, and availability controls in line with evolving risks and business needs.

## 4 Policy Principles

- **Risk-Based Approach** – Security decisions are driven by assessed risks and business impact.
- **Least Privilege & Need-to-Know** – Access is granted only to fulfil defined roles.
- **Defence-in-Depth** – Layered controls across people, processes, and technology.
- **Secure by Design** – Security is integrated from the start in systems, AI, and development.
- **Incident Response & Learning** – Incidents are reported promptly; lessons are applied.
- **Legal & Regulatory Compliance** – Full adherence to applicable laws, standards, and client obligations.

## 5 Leadership, Roles & Responsibilities

**The Chief Product & Technology Officer (CPTO):** Executive sponsor and owner of this ISMS policy; ensures ISMS objectives align with business strategy and approves ISMS objectives.

**RWS Leadership Team:**

- Ensure adequate resources for ISMS initiatives.
- Integrate ISMS requirements into business processes.
- Promote awareness and communication of ISMS requirements.

**SVP, Enterprise Technology Services:** Acts as the policy approver, providing formal authorization for this ISMS policy.

**The Senior Security Director:** Oversees ISMS implementation, monitoring, and continual improvement; reports performance, risks, and improvement opportunities to the CPTO and governance forums.

## The Security and Privacy Governance (SPG) Group:

- Provide strategic/business input to ISMS and Privacy Programme topics through expertise, insights, and guidance.
- Lead and ensure implementation of ISMS/Privacy Programme needs within their teams/functions.
- Provide support and advocacy for the ISMS/Privacy Programme.
- Contribute to setting agreed objectives and KPIs for effective ISMS monitoring.
- Conduct regular management reviews of ISMS performance.

**Managers:** Ensure security policy requirements are implemented and followed within their teams.

**Employees and Contractors:** Comply with security policy requirements and related security/privacy procedures.

**Third Parties:** Meet equivalent security standards through contractual obligations and regular risk assessments.

All employees and contractors must comply with this policy and related security and privacy procedures. Managers are responsible for ensuring compliance within their teams. Third-party vendors and partners must meet equivalent security standards through contractual obligations and regular risk assessments.

## 6 Policy Review

This Policy is available on the Group's SharePoint. If there are amendments to the applicable legislation or regulatory requirements, the Policy will be amended to reflect these. There will be an annual review by the person responsible for the Policy to ensure the document is fit for purpose and remains effective. Any changes will be communicated by email or by way of team briefings or training, depending on the complexity of the amendment.

*Dorte Schou*

Electronically signed by: Dorte Schou  
Reason: I approve this document  
Date: Dec 17, 2025 08:37:03 GMT

SVP, Enterprise Technology Services

## Document History

Name	Date	Detail	Version
Ed Parkins	20/05/2021	Document creation	0.1 draft
Shane Clarke	21/05/2021	Reviewed, no amendments	0.1 draft
Carla Matthews	22/05/2021	Reviewed, amendments made	0.2 draft
Azad Ootam	27/05/2021	Reviewed, approved	1.0
Russell Frith	02/09/2022	Policy Review. Updated IS executive sponsor to CIO.	1.1
Terry Doyle	02/09/2022	Approved	1.1
Russell Frith	22/08/2023	Policy review. Updated SGRC team reference.	2.0
Terry Doyle	04/09/2023	Approved	2.0
Russell Frith	10/09/2024	Updated Exec sponsor references.	3.0
Dorte Schou	10/09/2024	Approved	3.0
Russell Frith	08/12/2025	Policy rewrite, alignment to strategic goals	4.0
Dorte Schou	16/12/2025	Approved	4.0



## **About us**

RWS is a content solutions company, powered by technology and human expertise. We grow the value of ideas, data and content by making sure organizations are understood. Everywhere.

Our proprietary technology, 45+ AI patents and human experts help organizations bring ideas to market faster, build deeper relationships across borders and cultures, and enter new markets with confidence – growing their business and connecting them to a world of opportunities.

It's why over 80 of the world's top 100 brands trust RWS to drive innovation, inform decisions and shape brand experiences.

With 60+ global locations, across five continents, our teams work with businesses across almost all industries. Innovating since 1958, RWS is headquartered in the UK and publicly listed on AIM, the London Stock Exchange regulated market (RWS.L).

More information: [RWS.com](https://www.rws.com)

© 2025 All rights reserved. Information contained herein is deemed confidential and the proprietary information of RWS Group\*.

\*RWS Group shall mean RWS Holdings plc for and on behalf of its affiliates and subsidiaries.