RWS Group

ISMS Information Security Policy

Author: Russell Frith

Approver: Michelle Wilson

Version: 2.1

Issue Date: 19/10/2023

Next Review Date: 19/10/2024

Classification: Public

Retention Period: Until superseded

Table of Contents

1 Document history

Name	Date	Detail	Version
Ed Parkins	24/06/2021	Document Creation	0.1
ISSC	15/07/2021	Document Review	0.1
Azad Ootam	27/09/2021	Approved	1.0
Christopher Arbon	19/10/2022	Document review and repurposed with 2022 RWS policy template Minor updates to the following sections: Policy (4), Job title and description (8.3.1), Job description (8.3.2), Applicable Laws, Regulations and Standards (9), Training & Awareness (22).	2.0
Russell Frith	19/10/2022	Approved	2.0
Russell Frith	06/10/2023	Document Review and Minor amends including section: Policy (4) and wording throughout	2.1
Michelle Wilson	19/10/2023	Approved	2.1

2 Summary

The Group ISMS Information Security Policy addresses RWS' strategic security requirements and controls for IT Security, Information Security, Personnel Security and Physical Security. Detailed security requirements may be found in subordinate policies, processes and standards which comprise RWS' information security management system (ISMS). The Group ISMS Information Security Policy applies to all RWS

permanent and temporary employees, including contractors, freelancers and those employed by RWS' suppliers as set out in their relevant contracts, in all locations and operations. It is the responsibility of all RWS employees and contractors to be familiar with the organization's policies and to comply with their requirements and those of any supporting policies, processes, and standards.

3 Purpose

The Group ISMS Information Security Policy presents relevant and defining information about the objectives and functions of the RWS information security program and how all of RWS' security elements contribute to the global security posture. This document provides a high-level view of RWS' control environment which is implemented to minimize malicious or unintended risks to the confidentiality, integrity, and availability of RWS assets, including people, facilities, equipment, and information in all its forms. It is equally applicable to client assets under the control of RWS. This document provides guidance to everyone with logical or physical access to RWS or client information and facilities to assist them implementing good practice whilst carrying out their responsibilities.

4 Policy

The Group ISMS Information Security Policy is founded upon RWS' Information Security Management System (ISMS), which integrates the standards and guidelines established by the International Organization for Standardization (ISO) 27000 series, in addition to any supplementary RWS information security controls identified as suitable through feedback from stakeholders and comprehensive risk assessments.

5 Terms and Definitions

Information Security Management System (ISMS)	The policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information.It includes all elements used to manage and control information security risks.

Information security policy	Aggregate of directives, regulations, rules, and practices that prescribes howan organization manages, protects, and distributes information.
Personally identifiableinformation (PII)	Any information about an individual maintained by an organization, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other informationthat is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Sensitive PII	Information which, when disclosed, could result in harm to the individualwhose privacy has been breached. Such information includes biometric information, medical information, personally identifiable financial information, and unique identifiers such as passport or Social Security numbers.
Information security event	Identified occurrence of a system, service or network state indicating a possible breach of information security; policy or failure of controls; or apreviously unknown situation that may be security relevant.
Information security incident	A single – or series – of unwanted or unexpected information security eventsthat have significant probability of compromising business operations and threatening information security.
Fraud	A deliberate deception to secure unfair or unlawful gain.
Data breach	An information security incident which has been investigated and is reasonably suspected or confirmed to have resulted in the compromise of confidentiality, integrity, or availability of information whilst in the control ofRWS or its contracted third parties.

Cloud Client	An individual or entity that utilizes or subscribes to cloud-based services orresources.
Cloud Provider	A company that provides cloud-based platform, infrastructure, application,or storage services to other organizations and/or individuals, usually for a fee, otherwise known to clients “as a service.”

6 Organization of Information Security

Security responsibilities at RWS are delegated throughout the organization to appropriately support Group and Divisional business aims. Strategic policy and direction are set and monitored at Group level and is implemented through Divisional and functional policies and processes. The Chief Information Officer (CIO) is the executive sponsor for security and the RWS Information Security Program. The CIO is chairman of the Information Security Steering Committee (ISSC), which supports business aims by setting and monitoring RWS’ strategic security direction and providing oversight and governance of Group and Divisional security risk management.

Day-to-day oversight of RWS’ Information Security Program is performed by the Security Governance, Risk & Compliance team, which maintains the Group ISMS policies, provides information security advice, guidance, awareness, and governance, performs security audits, monitors the effectiveness of the ISMS, and oversees Divisional implementation of security risk management processes. The Security Governance, Risk & Compliance team consists of: The Security Governance, Risk & Compliance Manager; the Information Security Auditor, Information Security Engineer’s, and Security Sales Support analysts.

7 Information Security Management System

The RWS Information Security Management System (ISMS) comprises the people, processes and technologies employed at RWS regardless of whether they fall within an area of the organization which is in scope of the ISO27001 certification. Group Policies are used to define the high-level requirements of the ISMS, outlining the effects to be achieved to support RWS’ business aims. Group policies are ‘living documents’ and are subject to review annually or more frequently if necessary to ensure they continue to reflect good/best practice in the context of RWS. All employees are responsible for

ensuring they are aware of and comply with the latest RWS Group policies. Changes to Group security policies will be notified via the RWS Yammer feed. Supporting policies, processes and standards are used by Divisions and functions to specify how the requirements of the ISMS will be met at the operational level. Each Division and function are responsible for ensuring changes to their policies, processes and standards are notified to applicable employees.

7.1 Monitoring the ISMS

RWS operates in an environment where it must consistently comply with national and international laws and demonstrate an effective ISMS which complies with international security standards and client's requirements and expectations. Additionally, the ISMS must be flexible to support evolving business aims and adapt to the evolving threat landscape.

Therefore, RWS' ISMS must be kept under regular review to ensure that its policies and controls continue to support the business by addressing new threats; incorporating any statutory or regulatory requirements when applying and managing controls; identifying and managing consequential risks; and that any changes to the legal or regulatory environment are incorporated. RWS monitors the effectiveness of its ISMS by conducting tests against its infrastructure, for example penetration or vulnerability testing; by collecting information on policy compliance, such as endpoint encryption and AV status; by conducting audits across the ISMS by its internal teams; and by exercising its contingency and response plans.

The ISMS is controlled by the Information Security Steering Committee (ISSC). Membership of the ISSC includes several permanent members, which may change based on organizational requirements. Additionally, membership may be extended on an ad hoc basis to specialists where specific issues are to be discussed. Core membership of the ISSC includes:

- Chief Information Officer (Chair)
- Vice President Data & Analytics, Security and Quality Compliance
- Security Governance, Risk & Compliance Manager
- VP Cloud Operations
- Director Group IT
- Head of IT (Life Sciences)
- Head of IT (IP Services)
- Head of IT (Language Services & Technology)

- VP Product Development (Language Technology)
- Head of Development (Tridion)
- Head of Application Software Development
- VP Research & Development (Machine Translation)

The ISSC shall meet every four months, though extraordinary meetings may be called as required. The ISSC shall identify the controls most critical to supporting RWS' business aims and decide the appropriate KPI for each, along with the team responsible for implementing, monitoring, and reporting on control effectiveness. Effectiveness reports shall be produced at each meeting where the ISSC will consider the evolving threat environment and RWS' business aims to ensure control performance is adequately supporting the organization and that risks are appropriately addressed.

8 Roles and Responsibilities

8.1 Chief Information Officer (CIO)

The CIO is the executive sponsor for Information Security at RWS. The CIO provides Executive and Board level strategic direction for the information security program and chairs the ISSC. The CIO represents RWS' security and privacy concerns during strategic planning and investment control processes to ensure the RWS security strategy and roadmap supports organizational aims and is appropriately funded and resourced.

8.2 Information Security Steering Committee (ISSC)

The ISSC is responsible to the RWS Board and Executive management team for providing strategic direction and support for information security in accordance with RWS business requirements and relevant laws and regulations. Furthermore, it is responsible for establishing a management framework to initiate and control the effective implementation and operation of information security within the organization. Membership of the ISSC comprises the following roles:

8.2.1 Vice President (VP) Cloud Operations

The VP of Cloud Operations is responsible for the implementation of Group security policies in the Cloud Ops Division. This shall be achieved through the development, publication and distribution of Cloud Ops specific security policies, processes, procedures, and standards (as applicable) which support

Cloud Operations and RWS business aims. Security risks which could impact on the achievement of Cloud Operations or RWS goals shall be identified, analysed, managed, recorded, and reported in accordance with Group policy. VP Cloud Operations is a member of the ISSC and is responsible for generating KPI data to demonstrate the effectiveness of security controls within Cloud Operations and for presenting this information at meetings of the ISSC.

8.2.2 Heads of Research and Development

Heads of Research and Development (R&D) are responsible for the implementation of Group security policies in their functions. This shall be achieved through the development, publication and distribution of function specific security policies, processes, procedures, and standards (as applicable) to support functional and organizational aims. Security risks which could impact on the achievement of functional or organizational aims shall be identified, analysed, managed, recorded, and reported in accordance with Group policy. Heads of R&D functions are members of the ISSC and are responsible for reporting to the Committee the effectiveness of the security controls implemented in their function via agreed KPI, which are to be presented at ISSC meetings.

8.2.3 Divisional / Group Head of Information Technology

RWS' Divisional structure requires a head of IT in all RWS Divisions and the Group function. In addition to their IT responsibilities each head of IT is responsible for ensuring that the requirements of RWS' Group security policies are implemented within their area of responsibility and that appropriate security controls are identified, implemented, managed, and monitored to ensure their effectiveness. Heads of IT are required to present reports showing the performance of security controls in their area of responsibility against specific KPI at meetings of the ISSC. Additionally, IT heads are to ensure they maintain a register of their information security risks and ensure that owners are assigned and that appropriate mitigation activities are implemented and monitored.

8.3 Security Governance, Risk & Compliance Team

The Security Governance, Risk & Compliance Team reports to the Vice President Data & Analytics, Security & Quality Compliance. It supports the achievement of business aims by providing: SME advice and guidance on the selection and implementation of security controls; independent oversight of KPI data to monitor the effectiveness of the RWS ISMS; independent information security auditing of RWS Divisions and Functions; SME

support to new and existing client engagements; and SME support to the maintenance and expansion of RWS information security certifications to further business goals. The Security Governance, Risk & Compliance team consists of the following:

8.3.1 Security Governance, Risk & Compliance Manager

The Security Governance, Risk & Compliance Manager provides information security advice and guidance both to senior management and across all RWS Divisions. The Security Governance, Risk & Compliance Manager also owns RWS' Group information security policies; is responsible for ensuring they are aligned with business strategy and support its aims; and oversees the implementation of RWS' security strategy by Group and Divisional functions. Secretary of the ISSC, the Security Governance, Risk & Compliance Manager ensures meetings take place as required and that they support the implementation and maintenance of the ISMS by monitoring its performance and identifying opportunities to continually improve. The Security Governance, Risk & Compliance Manager provides oversight of the information security tasks required to maintain confidentiality, integrity and availability of RWS' systems and operations and exercises oversight of information security risk management across the Group. The Security Governance, Risk & Compliance Manager must hold or be working towards a Certified Information Security Manager (CISM) (or equivalent) qualification.

8.3.2 Security Engineer

The Security Engineer supports the Security Governance, Risk & Compliance Manager in the definition and implementation of the ISMS policies and procedures and the security activities of the RWS Information Security Program, and is primarily responsible for the operation of the RWS Group vulnerability management and security testing tools to identify weaknesses in RWS' public facing infrastructure and also to configure and perform vulnerability scans and facilitate independent penetration testing of RWS technology solutions in development as required to support business aims. In addition, the security engineer supports sales operations with client queries and auditing relative to information security, privacy, and associated compliance, and supports the RWS Business Continuity Manager by assisting and advising on the definition and implementation of physical security controls across the Group and by conducting and maintaining business impact assessments and reports on the preparedness of functions to deal with business interruptions. The Security Engineer shall hold or be working towards appropriate industry recognised security certifications.

8.3.3 Information Security Auditor

The Information Security Auditor is responsible for validation of the implementation and effectiveness of RWS' information security policies and procedures through auditing of RWS' systems, operations, and supply chain. The Information Security Auditor must hold or be working towards a recognized auditor qualification such as the International Register of Certificated Auditors (IRCA) Auditor or ISACA Certified Information Security Auditor (CISA).

8.3.4 Security Sales Support Analyst

The Security Sales Support Analyst assists RWS sales and client accounts teams by coordinating specialist security, business continuity and privacy input to client and prospect requests for information, requests for proposal, reviews of contractual security clauses and client security assessments. Additionally, the Security Sales Support Analyst is responsible for producing monthly reports detailing the number of client requests dealt with and tracking client security requirements which is used to inform RWS' roadmap of security priorities.

8.4 Group Data Privacy Officer

The Group Data Privacy Officer is responsible for defining RWS' stance in privacy law adoption and the privacy law framework for RWS. The Global Data Privacy Officer is also responsible for maintenance of privacy related policy information in the ISMS. The Group Data Privacy Officer must hold or be working towards a Certified Information Privacy Professional – European Union (CIPP-EU) and Certified Information Privacy Professional – United States (CIPP-US) certification and shall attend training and conferences to keep knowledge up to date.

8.5 All RWS Employees

All RWS employees are individually accountable and responsible for information security by maintaining an awareness of and following RWS' information security policies and profiles, reporting all suspected and actual security incidents when discovered and attending annual an updated information security training.

9 Applicable Laws, Regulations and Standards adopted by RWS

RWS uses the following security frameworks and standards for defining security within the ISMS:

- **ISO/IEC 27001** – specifies a management system that is intended to bring information security under management control and defines specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.
- **ISO/IEC 27002** - provides best practice recommendations on information security controls for use by those responsible for initiating, implementing, or maintaining the ISMS. Information security is defined within the standard in the context Confidentiality, Integrity, and Availability (CIA).
- **ISO/IEC 27017** - a code of practice for information security controls based on ISO/IEC 27002 specifically for cloud services. ISO 27017 provides additional information security controls implementation advice beyond that provided in ISO/IEC 27002, focusing on the protection of the information in the cloud services.
- **ISO/IEC 27018** - a code of practice for the protection of personal data in the cloud basedon ISO/IEC 27002 specifically for cloud services. ISO 27018 provides additional information security controls implementation advice beyond that provided in ISO/IEC 27002, applicable to public cloud Personally Identifiable Information (PII).
- **HITRUST CSF** - a certifiable framework that provides organizations with a comprehensive approach to regulatory compliance and risk management. Primarily targeted at highly regulated sectors such as healthcare and life sciences but more recently adapted to suit other sectors such as financial services.
- **NIST CSF** – Set forth by the National Institute of Standards and Technology (NIST) under the United States Commerce Department, NIST CSF is a cybersecurity framework consistingof standards, guidelines, and best practices to manage cybersecurity-related risk.

The RWS legal team is responsible for identifying and reviewing changes to laws and regulations applicable to RWS and shall maintain a register of such laws and regulations.

10 Security Risk Management

RWS' information security strategy supports business aims by identifying, prioritizing, and managing its security risks. Operational teams throughout the organization are responsible for identifying, assessing, and managing their risks in accordance with RWS' Group Security Risk Management Policy. Security and privacy risks are addressed through the application of appropriate security controls and associated risk treatment plans and the acceptance and management of residual risks. The security risk management process is overseen by the Security Governance, Risk & Compliance Manager and security risk oversight and governance is exercised by the ISSC.

11 Logical Access Control

Access to RWS' systems and information must be controlled to protect their confidentiality, integrity, and availability. Accordingly, access is restricted to those with a 'need to know' and is reviewed periodically to ensure appropriate access is maintained. Access credentials must meet specific minimum requirements, depending on the subject system, to reduce the risk of unauthorized access. Further guidance can be found in the Group Logical Access Control Policy.

12 Business Continuity

RWS has a global presence and offers several SaaS products and localization services to its clients. The implementation of the RWS Group Business Continuity Policy ensures preparations are made to identify risks which may affect RWS' ability to operate during an incident and recover quickly in the aftermath. All RWS employees must ensure they understand the business continuity process and their place in it. Business continuity plans and processes must be regularly reviewed and tested to ensure effectiveness.

13 Information Classification, Handling and Retention

Information assets created, stored, and used within RWS have value, which must be identified by the asset owner or creator to allow the appropriate security controls to be

applied. Additionally, information processed for clients in RWS SaaS products must be classified according to its value to the client.

All employees are required to protect information according to the data classification assigned to it. Access to all classified information is based on the Need-to-Know principle. Although people might be authorized to access information, they shall only access data when strictly required.

Further information classification, handling and retention information may be found in the RWS Group Classification and Handling Policy.

14 Security Incident Management

A risk-based approach to security focused on supporting business aims, such as that implemented by RWS, results in the likelihood that a security incident will occur at some point. Therefore, all RWS employees must ensure they know how to identify and report a security incident and must be fully familiar with their involvement in the incident management process. RWS' security incident management processes must be in place and tested.

RWS' security incident management process follows a four-stage approach focused on: Preparation; Detection & Analysis; Containment; Eradication & Recovery; and Post-Incident Activity. This supports RWS' business continuity policies and processes. Further details can be found in the RWS Group Information Security Incident Management Policy.

15 Physical Security

Information and assets at RWS facilities must be protected in accordance with their value or classification. RWS' Group Physical Security Policy defines the baseline security requirements for RWS facilities, and guidelines for the identification, assessment and management of physical security risks and the implementation of designated security access areas within the facility.

RWS' Group Physical Security Policy should be consulted for further information on physical security.

16 Data Privacy

RWS employees handle a variety of Personal information both for other RWS employees and for clients. In some cases, this personal information may fall into the category of sensitive information such as healthcare data, which requires increased levels of protection. In all circumstances, personal information and sensitive personal information must be processed and stored in accordance with RWS' policies and any local legislation.

RWS' Data Privacy Officer maintains a Privacy Legislation Framework to meet regulatory requirements for data privacy. The Privacy Legislation Framework covers relevant privacy legislation for RWS as a data controller and / or data processor.

Further data privacy information may be found in the RWS Group Privacy Policy.

16.1 Privacy Impact Assessment

The implementation of RWS' Privacy Legislation Framework supports privacy by design. Part of privacy by design is the execution of a Privacy Impact Assessment to ensure proper protection of personal data.

17 IT Systems Management

IT Systems includes all physical and virtual IT systems used by RWS in RWS' IT infrastructure or SaaS products. RWS' requirements for IT system installation and maintenance can be found in its Group IT System Policy.

18 Client owned IT systems

Client owned IT Systems (for example an on-premises installation of an RWS product) are managed and maintained by the client, this responsibility includes information security. In case RWS employees are required to access such systems, client's security requirements apply.

19 Cryptography

RWS uses cryptography to protect physical and logical assets. Cryptographic solutions must be employed correctly for them to be effective and cryptographic keys must be managed to ensure their availability. RWS' requirements for cryptography are contained in several Group policies, such as the Group Classification and Handling Policy and the Group Secure Software Development Lifecycle Policy. Further cryptography information may be found in the Group Cryptographic Controls Policy.

20 Supplier Management

RWS' supply chain constitutes a risk due to the reliance on a third party implementing appropriate controls to protect services and information. RWS' supplier on-boarding process must include an information security assessment which varies in detail depending on the goods or services to be provided, or the level of physical or logical access provided to the supplier. Additionally, appropriate 'Right to audit' clauses must be contained in all supplier contracts which allow RWS to carry out periodic assessments of the effectiveness of a supplier's controls. Supplier contracts must also include a set of minimum expected security requirements for protecting RWS assets and information and an obligation for the supplier to inform RWS upon learning of a security incident or breach which affects RWS assets or information.

Further details can be found in the Group Supplier Security Management Policy.

21 Secure Software Development

Application source code and algorithms developed by RWS are considered Intellectual property. Secure development of software such as applications is essential to protect both the software itself and any information contained within it or accessible through it. It is therefore essential that security risks must be identified and managed at each stage of the software development lifecycle. Such controls are documented by teams holding such information.

Further secure software development information may be found in the RWS Group Secure Software Development Lifecycle Policy.

22 Training and Awareness

Information security training is provided to all RWS employees, contractors, and suppliers, through a variety of media. The Security Governance, Risk & Compliance team is responsible for the content of the 'in house' training delivered within RWS and approves any externally provided training for specific roles. Completion of mandatory security training modules is monitored and reported to the ISSC for follow-up action as necessary.

- New hires are enrolled in the Atlas Learning Zone and are required to undertake information security training within their first month of employment.
- Line managers are responsible for ensuring their teams are aware of and comply with any applicable security requirements.
- Annual Information Security and Privacy training is provided through several e-learning modules.
- Think Security bulletins are distributed to all employees on a regular basis.
- Some specialists, such as software developers, are required to undertake specific training delivered through the MyLX portal.
- Other information security training courses are available to all employees.

23 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 by way of the "Regulatory and compliance update," team briefings or training, depending on the complexity of the amendment.