# EXHIBIT 2 – SECURITY POLICY

This Security Policy outlines the minimum security and data privacy obligations that RWS shall meet when processing Client Content, which may include Personal Data (together, "Client Content"), in connection with the provision of Services under the Master Relationship Agreement ("MRA" or "Agreement"). These obligations are in addition to, and do not limit, any other obligations set forth in the Agreement.

All capitalised terms not defined in this Security Policy shall have the meanings ascribed to them in the Agreement or the applicable Data Processing Agreement ("DPA").

## 1. LIABILITY

RWS expressly accepts responsibility for ensuring that the obligations set out in this Security Policy are fulfilled when processing Client Content, whether directly or indirectly through its Sub-Processors and/or third-party contractors (collectively referred to as "RWS" for the purposes of this Policy).

## 2. BINDING POLICIES AND PROCEDURES

2.1 RWS shall maintain documented and binding security and privacy policies and procedures ("Security Documentation") that comply with applicable Data Protection Laws and incorporate the requirements set out in this Security Policy. RWS shall ensure that such documentation is regularly reviewed and kept up to date.

2.2 The Security Documentation shall clearly define the physical, technical, and organisational measures implemented by RWS to protect Client Content against unauthorised access, acquisition, use, disclosure, or destruction. Upon request, RWS shall provide the Client with evidence that the Security Documentation is in place and current.

## 3. INFORMATION SECURITY PROGRAM

RWS shall implement and maintain an information security program, supported by a suite of policies and an organisational structure aligned with industry best practices. The program shall define clear roles and responsibilities and include the appointment of a senior management representative responsible for overseeing its implementation and ongoing maintenance. The representative shall have the authority to allocate resources and make decisions necessary to ensure the security of Client Content processed under the Agreement and shall report directly to RWS senior management. RWS shall regularly review and update the information security program to address emerging threats, vulnerabilities, and applicable regulatory requirements.

## 4. RISK MANAGEMENT

RWS shall conduct periodic, independent security risk assessments to identify the criticality of information assets, assess threats, evaluate potential risks, and implement appropriate risk treatment plans. RWS shall apply technical and organisational measures to mitigate identified risks, ensuring a level of security appropriate to the nature and severity of the risk.

## 5. INVENTORY

RWS shall maintain an inventory of media, servers, and equipment containing Client Content to ensure traceability and accountability. This inventory shall include records of the return or secure destruction of Client Content in accordance with applicable data retention and disposal policies.

## 6. PERSONNEL

RWS shall require all personnel to sign a non-disclosure or confidentiality agreement that outlines their responsibilities for protecting Client Content and the consequences of non-compliance. RWS shall provide annual training and awareness programs on information security and data protection

to all personnel, ensuring they understand their obligations and are equipped to handle Client Content securely.

## 7. USER AUTHENTICATION

Access to RWS systems shall be strictly conditional upon the proper implementation and adherence to authentication procedures, in accordance with an approved Identity and Access Management (IAM) policy. Each user shall be assigned a unique login account, and authentication shall be enforced through secure mechanisms to prevent unauthorised access.

## 8. ACCESS MANAGEMENT

RWS shall enforce password policies that comply with applicable regulatory requirements, industry standards, and recognised best practices. Passwords shall be changed at least every 180 days, must not be reused, disclosed to others, or written down. Users shall be required to change any password assigned automatically or by an administrator. Systems shall enforce account lockout mechanisms to limit the number of failed login attempts and prevent unauthorised access.

## 9. ACCESS PRIVILEGES

Access privileges shall be granted based on predefined roles aligned with job responsibilities and the principle of least privilege. RWS shall ensure that access to Client Content is restricted on a need-to-know basis. Outdated or unnecessary access rights shall be promptly revoked, and access permissions shall be reviewed at least annually. RWS shall implement separation of duties controls to ensure that personnel with privileged access do not simultaneously have access to other sensitive systems or data beyond their role requirements.

## 10. ENCRYPTION, HASHING AND SIGNING

10.1 RWS shall use recognised, secure cryptographic algorithms, libraries, and software to protect Client Content. All secrets and cryptographic keys shall be securely stored and managed in accordance with industry best practices.

10.2 Client Content shall be protected equally, regardless of classification, both in transit outside of RWS's network and at rest. This includes, but is not limited to:

- Use of strong encryption algorithms, such as Advanced Encryption Standard (AES), to prevent unauthorised access;
- Secure generation, storage, rotation, and destruction of encryption keys, ensuring sufficient key length and randomness to prevent brute-force attacks;
- Secure transmission of Client Content using protocols such as Transport Layer Security (TLS);
- Encryption of Client Content at rest using secure algorithms and key management practices;
- Compliance of encryption methodologies with applicable laws and regulations;
- Encryption of Client Content prior to transmission to authorised external parties, with secrets (e.g., decryption keys) transmitted separately via a different communication channel to ensure confidentiality.

## 11. LOGGING

RWS shall maintain appropriate audit trails and system access logs for all Information Systems processing Client Content. Logs shall be protected against tampering and monitored by trained security personnel to detect anomalies and support incident investigation and compliance requirements.

## 12. PHYSICAL AND ENVIRONMENTAL SECURITY

RWS shall implement physical and environmental security measures to prevent unauthorised physical access, damage, or interference to Client Content and supporting infrastructure. These measures shall include, but are not limited to:

- Physical access controls to restrict access to authorised personnel only, including mechanisms such as locked doors, access cards, biometric systems, and security guards;
- Environmental controls to mitigate risks from fire, flooding, temperature fluctuations, and power outages, including fire suppression systems, water detection, HVAC systems, and backup power supplies;
- Asset management controls to track and manage equipment, hardware, and software that store or process Client Content, including inventory systems, asset tagging, and regular inspections;
- Secure work areas with restricted access, surveillance, and physical safeguards to prevent unauthorised access or theft;
- Documented physical security policies and procedures aligned with industry standards, covering access control, environmental protection, asset management, and incident response;
- Monitoring and testing of physical security controls through regular inspections and audits;
- Secure destruction of sensitive materials, including the use of P-4 rated shredders (or higher) for hard copy records, and physical destruction of decommissioned hard drives and storage media;
- Physical access restrictions and monitoring at data centre facilities, which may include multi-zone security, mantraps, perimeter deterrents (e.g., fencing, guarded gates), biometric access, CCTV, and secure cages;
- Protection of equipment and media used to process Client Content from physical and environmental threats, including secure storage when not in use;
- Secure storage of hard copy records containing Client Content in filing systems that support retrieval, amendment, and destruction in accordance with data subject rights;
- Use of locked containers or equivalent secure transport mechanisms for moving hard copy records, and secure destruction of such records when no longer required.

## 13. PATCH MANAGEMENT

13.1 RWS shall ensure that only licensed software is used in the provision of services and that such software complies with applicable security standards. RWS shall maintain a documented patch management process and schedule covering all infrastructure, systems, and application components used to deliver services. This process shall include the timely deployment of updates and upgrades in accordance with industry best practices.

13.2 When a vulnerability is identified and a vendor patch is available, RWS shall obtain the patch from the relevant vendor and apply it in accordance with its current vulnerability and security patch management policies and procedures. Patches shall only be deployed after appropriate testing to confirm their stability and compatibility with RWS systems. RWS shall ensure that vulnerability patches, antivirus, and anti-malware protections are applied and kept up to date, and shall not knowingly or intentionally introduce any malicious code into RWS or Client systems.

## 14. SECURITY INCIDENT RESPONSE

RWS shall implement and maintain an incident response framework to ensure the timely identification, management, and resolution of security incidents. This shall include:

- Procedures for identifying and reporting security incidents, supported by security monitoring tools, employee awareness training, and clearly defined communication channels;
- A process for categorising and prioritising incidents based on severity and potential impact on the confidentiality, integrity, and availability of data and systems;
- Documented response procedures, including escalation paths and the involvement of incident response teams, tailored to different types of incidents;
- Root cause analysis and post-incident reviews to prevent recurrence of similar incidents;

- Maintenance of accurate and detailed records of all security incidents, including actions taken, for audit, compliance, and reporting purposes.

RWS shall notify the Client without undue delay, and in any event within 72 hours of becoming aware of a security incident that impacts the Client, including any Personal Data Incident. Notification shall be sent to the Client's designated contact email address.

## 15. ENDPOINT SECURITY

Client Content shall only be stored on RWS-owned equipment and assets where necessary to fulfil a defined business purpose. RWS shall implement appropriate endpoint security measures to protect against unauthorised access to Client Content and other sensitive information. These measures shall include, at a minimum:

- Installation and maintenance of anti-malware software on all endpoint devices, with up-to-date virus definitions;
- Automatic session lockout after a predefined period of inactivity;
- Activation of host-based firewall protection on all endpoint devices;
- Regular application of security patches and software updates to protect against known vulnerabilities;
- Full-disk encryption on all endpoint devices to protect data in the event of loss or theft;
- Access controls to ensure only authorised personnel can access endpoint devices and any Client Content stored on them;
- Regular backups and data synchronisation to ensure data availability and integrity;
- Ongoing employee training on endpoint security best practices, including adherence to RWS's security policies, phishing awareness, malware identification, and incident reporting procedures.

## 16. REMOVABLE MEDIA

16.1 RWS shall not use removable media (including USB drives, external hard drives, flash drives, CDs, DVDs, tapes, or other portable storage devices) to store Client Content under any circumstances.

16.2 Regardless of media type, RWS shall ensure that Client Content is protected against unauthorised access, loss, or destruction using industry-recognised security controls and in accordance with the terms of this agreement.

## 17. NETWORK SECURITY

17.1 RWS shall implement appropriate network security controls to ensure the confidentiality, integrity, and availability of systems and data. Network flows shall be restricted to what is strictly necessary, and secure remote access shall be enforced through the use of Virtual Private Networks (VPNs). Wireless networks (Wi-Fi) shall be secured using WPA3 or equivalent encryption protocols, and shall include secure identification, authentication, and encryption mechanisms. Peer-to-peer networking shall be disabled, and the use of insecure public Wi-Fi shall be prohibited.

17.2 RWS shall implement industry-standard network access controls to prevent unauthorised access to systems and data. These controls may include firewalls, intrusion detection and prevention systems (IDPS), extended detection and response (XDR), and other appropriate technologies. RWS shall regularly monitor and test network security controls to ensure they are functioning effectively.

## 18. BUSINESS CONTINUITY AND DISASTER RECOVERY

18.1 RWS shall maintain a business continuity management system aligned with ISO 22301, including a documented business continuity policy, strategy, and program. This program shall include a

business continuity plan covering the services provided by RWS, which shall be reviewed and tested periodically to ensure effectiveness.

18.2 RWS shall perform regular backups of critical systems and data, ensure that backup media is encrypted and securely stored, and implement appropriate protections during transport. Business continuity and disaster recovery procedures shall be tested regularly to ensure that Client Content can be restored in the event of a disruption. Where RWS utilises data centres to support its services, both primary and backup data centres shall be in place. These data centres may be operated by RWS or by approved third-party providers.

## 19. DISPOSAL

19.1 In the event that client data is archived, RWS shall implement appropriate access controls for archived data to ensure that only authorised personnel can access such data. Expired archives shall be securely destroyed in accordance with RWS's data retention and disposal policies.

19.2 When disposing of or repurposing equipment, physical documents, files, or media containing Client Content, RWS shall implement appropriate measures to prevent unauthorised recovery of the data. Such measures may include secure deletion, reformatting, degaussing, or restoring devices to their original configuration.

## 20. SUB-PROCESSORS AND THIRD-PARTY PROVIDERS

RWS shall implement appropriate controls to prevent unauthorised access to Client Content by sub-processors and third-party providers ("Third Parties"). These controls shall include:

- Conducting security risk assessments of Third Parties and approving their use based on their ability to meet RWS's security requirements for processing Client Content;
- Regularly monitoring Third Parties to ensure ongoing compliance with applicable security requirements;
- Implementing data flow controls to ensure Client Content is only shared with vetted and approved Third Parties;
- Requiring Third Parties to report any security incidents or data breaches involving Client Content to RWS in a timely manner;
- Including termination rights in contracts with Third Parties in the event of non-compliance with security obligations;
- Incorporating specific data privacy and security clauses in Third Party contracts, including provisions for the return or secure destruction of Client Content.

## 21. SECURE SOFTWARE DEVELOPMENT

21.1 Where applicable, RWS shall develop secure applications for the Client and maintain a secure software development lifecycle (SDLC) aligned with ISO/IEC 27001 standards. Applications and websites developed and/or maintained by RWS shall be designed and tested to ensure that passwords and Personal Data are not transmitted via URL query strings or other insecure mechanisms.

21.2 RWS shall implement input validation controls to ensure that user input conforms to expected formats and does not introduce security vulnerabilities.

21.3 RWS shall ensure logical separation between development and production environments.

21.4 RWS shall not promote software to production without first addressing all discovered vulnerabilities classified as critical or high risk, in accordance with industry-standard vulnerability scoring systems (e.g., CVSS).

## 22. SECURITY TESTING

RWS shall implement appropriate measures to discover and address vulnerabilities in RWS systems, applications and network, including but not limited:

- Conduct regular vulnerability scanning of RWSs' systems, applications and networks to identify potential security vulnerabilities, testing should be performed for OWASP Top 10+ vulnerabilities using industry recognized tools.
- Establish a patch management process to ensure that security patches and updates are promptly applied to address known vulnerabilities;
- Conduct risk assessments to identify potential vulnerabilities and prioritize their remediation based on the level of risk they pose to Client Content; If applicable, ensure that Third Parties used by RWS for services such as cloud computing or network monitoring also address vulnerabilities in their systems and networks.
- RWS shall engage independent Third Parties to conduct penetration testing on its web applications to identify security vulnerabilities. These tests will be performed at a minimum prior to each major release of the web application. RWS shall mitigate identified vulnerabilities according to defined security policy expectations and, upon request, provide the Client with executive summary reports of the third-party penetration testing.

## 23. INDEPENDENT VALIDATION OF CONTROLS

23.1 RWS commits to maintaining an independent security certification, such as ISO/IEC 27001 or SOC 2 Type II, at the time of contract signature. These certifications shall be made available to the Client for review upon request. Such certifications or attestations shall be maintained throughout the term of the contract.

23.2 RWS shall respond promptly to reasonable requests from the Client for information about, or copies of, these certifications and attestations, including any updates or successor certifications that may apply.