DSB SECURITY POLICY

1 GENERAL

1.1 This DSB Security Policy (the "**Security Policy**") sets out the security standards and processes that will apply to the DSB Services that the DSB will provide to the User.

1.2 This Security Policy forms part of the Agreement agreed between the User and the DSB. Defined terms shall have the same meaning as set out in the Main Terms and as otherwise set out herein.

2 SECURITY MEASURES

2.1 The DSB shall apply the following security standards and processes to the DSB Service.

Standard / Process	Details
ISO27001/2 Accreditation	As part of an ongoing commitment to compliance and security, Rackspace (formerly Datapipe) maintains SOC 1, SOC 2, ISO 27001, FedRAMP, FISMA, PCI, and HITRUST compliance and security standards. The DSB has reviewed all aspects of ISO27001 standard adherence with a recommendation to move forward with certification approved by TAC and for confirmation by the DSB board.
Acceptable Usage Policy	The Acceptable Use Policy sets out the restrictions applicable to using the DSB Service, as amended by the DSB from time to time.
	Detailed rules of engagement documents have been created for both FIX and ReST APIs (as described in the Subscription Management and Connectivity Policy) for the OTC ISIN Services and UPI Services respectively and are available for public download from the DSB website for OTC ISIN and UPI.
	FIX API users are also required to complete the DSB's FIX client certification process successfully. The certification document is available for public download from the DSB website.
Information Security Policy	The DSB maintains an information security policy aligned with external information security standards and will be reviewed annually. The DSB maintains an Information Security FAQ on its website where updates and specifics can be found to assist Users.
	The information security policy is currently published or communicated to all third-party employees and contractors.
IT Standards, Processes and Procedures	The DSB will maintain the standards and procedures supporting its IT processes and functions that are reviewed and, if required, updated annually.
	When a significant change occurs, the continuing suitability, adequacy, and effectiveness of the IT processes and procedures shall also be reviewed.
Process Governance	The DSB protects and secures its data managed through an information security program that is overseen centrally by the DSB management team representing: • Senior firm management • Senior business unit management • Information security officers.

Standard / Process	Details
	The DSB: • Approves, maintains, consistently applies and enforces compliance with the policies, program plans, procedures and controls supporting the information security governance program. • Maintains clear lines of reporting, responsibility, accountability, communication of expectations and the delegation of appropriate authority supporting decisions. • Manages the effect of security issues on the firm, business lines and related processes. Oversee risk mitigation activities to address issues. • Maintains risk measurement definitions and criteria, establish acceptable levels of information security risks. • Requires that data with similar criticality and sensitivity characteristics are protected consistently throughout the DSB. • Coordinates information with physical security.
	The DSB, with regards to the information security governance program, is responsible and held accountable for the following: • Central oversight and coordination • Assignment of responsibility • Risk assessment and measurement • Monitoring and testing • Reporting • Acceptable residual risk • Risk acceptance.
	The DSB reviews the information security program, considering the results of internal and external assessments, reviews and audits.
	The DSB has a Chief Information Security Officer (CISO) who performs risk management functions.
	The Chief Information Security Officer: • Reports directly to the board or to senior program management. • Has sufficient independence to perform their assigned tasks. • Has the authority to respond to a security event where confidentiality, integrity, availability or accountability of an information system is compromised. • Has the capacity to order emergency actions to protect the DSB and its customers from an imminent loss of information or value. • Holds a sufficient organisational position to enable them to perform their assigned tasks.
	The DSB will undertake an independent evaluation of its control environment relative to the services provided to its Users.
Asset Inventory	The DSB maintains an inventory of assets (both hardware and software) that includes ownership, classification and criticality of each asset, covering all IT systems which access, store or process User data (**Asset Inventory**).
	The Asset Inventory records asset owner, information classification, applied to that asset and physical location of the asset.
Pre-Employment Screening	Pre-employment screening (PES) is completed before authorising access to User information or User systems and includes minimum background checks such as criminal, professional qualifications, identification, solvency and proof of address.

Standard / Process	Details
InfoSec Training	The DSB provides an active IT security awareness training program (**IT Security Awareness Training**) that includes as a baseline: • The DSB's information security program • Using IT resources • Information management • Local and remote access • Internet safety • Physical security and backups • Computer security review. Each employee shall perform the IT Security Awareness Training annually. The DSB's global IT security manager reviews and updates the associated training material periodically. The status of the security training is continuously followed-up by the management. Customised training materials can be created, and the training status is tracked. The employees must state and sign that they have read the IT Security Awareness Training, understood it, and agreed to behave accordingly.
	Project-specific data privacy awareness training (**Data Privacy Awareness Training**) can be created for the project staff, containing User-specific data privacy or other requirements. The DSB has an active Data Privacy Awareness Training program that includes as a baseline: • Reporting • PII & Sensitive Data • Data Privacy Laws • Social Media Risks • Email Scams • Password Policy Each of the DSB's employees shall perform the Data Privacy Awareness Training annually. The DSB's global IT security manager reviews and updates the training material periodically. The status of the security training is continuously followed-up by the management.
Employment Policy	The DSB maintains a joiners, movers and leavers policy and supporting processes and procedures for all employees.
	All employees and contingent staff are screened before being onboarded in accordance with relevant internal policies, laws, regulations and ethics and proportional to the business requirements, the classification of the information to be accessed and the risk resulting from their failure to perform their role/function in an acceptable manner.
	All employees and contingent staff are required to sign terms and agreements of confidentiality, non-disclosure, acceptable use and/or code of conduct/ethics.
	All employees and contingent staff receive awareness training and updates related to Information Security, including privacy, and other organisational policies and procedures relevant to their job functions at least annually. Additionally, there is a process to track compliance to the organisation's awareness training exercises.
	The DSB maintains a disciplinary process for non-compliance with information security policies.
End of Service	The DSB ensures that access to User information or User IT systems is removed on or before the last day of service and that the DSB owned devices that can store, or access User information are returned.

Standard / Process	Details
Physical Security	The DSB maintains a policy, standard, and procedures supporting physical security, including physical access to the building, access control processes, and emergency procedures.
	All personnel entering the premises are forced to enter through a controlled entry point monitored by a receptionist or security guard. They are required to provide a unique method of verification of identification, i.e., driver's license, business card, supplier identification tag. Physical access rights to secure areas are appropriately modified to reflect changes in responsibility, including transfer and termination.
	Access authorisation procedures are in place to cover granting, removing, and reviewing access, including retrieving access keys/IDs. The procedures apply to all persons (e.g., employees and suppliers) requiring access to the premises.
	Physical access to the site or building includes: • Staffed reception area controls physical access to the site or building (staffed 24 X 7). • All facility entrance points, main perimeter walls, and exit points are monitored 24 X 7 via either security staff or CCTV coverage. • Logging and monitoring procedures exist, covering access control usage that indicates who entered the facility (employee and visitor) and when, as well as CCTV playbacks. • CCTV monitors entrances to loading and delivery areas. • Restricted to authorised personnel only by key card access.
	Visitors are required to be escorted by a responsible employee. Visitors include friends, maintenance specialists, computer suppliers, consultants (unless long term, special guest access is provided), maintenance personnel, and external auditors.
	The building management company authorises building access to third parties such as tenants, suppliers, service providers, i.e., cleaners and maintenance personnel.
	Policies, processes and procedures are in place to ensure that access to information storage facilities is restricted to authorised individuals and ensures that access to information storage facilities is recorded and monitored. Role-based access control mechanism is in place, which restricts access to sensitive data only to authorised persons. Roles and access are regularly reviewed. The employees must sign a confidentiality/non-disclosure agreement.
	All fire doors on the security perimeter of the building have been fitted with alarms that are regularly monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards. In addition, the fire alarms operate accordance with the local fire code in a failsafe manner.
	All power and telecommunications lines into the building are installed underground, and they are segregated from telecommunications cables to prevent interference.
	Controls are in place to restrict access to patch panels and cable rooms.
	An expert has conducted a risk assessment to evaluate if the building may be at risk from terrorist activity. A safe area exists where building occupants can retreat during a terrorist incident.

Standard / Process	Details
	An expert has conducted a risk assessment to evaluate how the building may be at risk from fire, earthquake, flood, explosion, civil unrest or any other type of natural or manufactured disaster.
IT System Maintenance	IT systems are maintained in accordance with the manufacturers' recommended service intervals and specifications.
User Information Disposal	Procedures are in place to delete User information from IT systems such that the information cannot be retrieved when IT systems are required to be disposed of or reused. Storage devices containing sensitive information are physically destroyed or securely overwritten rather than using the standard delete function to make the original information non-retrievable. The physically destroyed pieces of equipment are recorded in an inventory file. All equipment containing storage media items must be checked to ensure that any sensitive data and licensed software have been removed or overwritten before disposal. Damaged storage devices containing sensitive data will require a risk assessment to determine if the items should be destroyed, repaired or discarded.
	The DSB maintains processes and procedures for the secure disposal of User information, including paper-based secure disposal and any supporting storage media (i.e., hard drives etc.). This includes the secure transport and storage of User information before destruction.
User Info: Operational Procedures	The DSB maintains operational procedures for all IT systems used to access, manage, store or process User information or access to User IT systems. This includes: • Technical vulnerability and patch management. • Network management. • A regular check of compliance with security implementation standards.
	There is no User access to the network or systems that store, process and transmit User data.
	Information systems are regularly checked for compliance with security implementation standards.
	The DSB manages the software download and installation process on systems that store, host and/or process User data in the following way: • Secure software download and installation procedures are documented. • Require approval to download and install the software. • Prohibit users from downloading and installing unapproved software. • Monitor the environment to identify new and legacy unapproved software download/installations.
Virus Protection	The DSB maintains an anti-virus/malware policy (and user awareness procedures) which covers workstations, services, mobile devices for the detection, prevention, containment and recovery to protect against malware.
Info and Software	The DSB maintains a backup and recovery policy, standards and procedures for how systems, applications and data backups are performed - including scheduling, testing and recovery.

Standard / Process	Details
Backup / Recovery	Backup copies of information and software are taken and tested regularly in accordance with the agreed backup policy. They are stored in one of the DSB locations, and the recoverability of data and software is periodically verified.
	Backup copies of data containing User information are encrypted.
User Access	The DSB maintains an access management policy, standard(s), and procedures that cover authentication, password management, entitlements and segregation of duties around this application.
	The DSB ensure segregation of duties to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. This includes separating duties between individuals who request access, authorise access, enable access, and verify access.
	The process for provisioning and de-provisioning user accounts includes: • Change requests are reviewed for appropriateness and approved. • Access rights appropriately modified to reflect changes in responsibility, including transfer and termination. • Reports or other authorisation lists of user access rights are reviewed annually. • Remote access is only granted to the DSB from their office locations. • Each User is uniquely identified with a user ID at the platform and network level. • Special privileges allow security account set-up and administration limited to a segregated security administration function.
	Processes are implemented to ensure all violations and/or unauthorised activities are monitored/reviewed and addressed promptly by the proper management level - as per the 27001 framework. Additionally, logs are created to identify users or attempted use and modification or attempted modification of critical systems components, including files, registry entries, configurations, network and server security settings/parameters, and audit logs.
Network Management / Access	An up-to-date topology (a network diagram) is documented and maintained with sufficient detail to manage the IT network and its security. Controls are in place to limit disclosure of information about the IT network and topologies to external parties.
	All IT networks used to provide a service to the group (and accessed from an external connection) are monitored for malicious activity.
	The network is managed and controlled, protected from threats, and maintain security for the IT systems using the network, including User information in transit within the IT network.
Password Security	The following restrictions are placed on passwords: • A complex password containing eight (8) or more characters with at least three of the following: upper case letters, lower case letters, numbers and special characters. • Passwords with the following characteristics: easily guessed words (Password), sequences (1234), duplicative characters (mmmm), personal facts (DOB) are prohibited. • Passwords are changed with the first login.
	Controls are in place to prevent password sharing and are governed by a defined Password Policy
	Two Factor Authentication is in place to monitor and restrict internal access.

Standard / Process	Details
External / Remote Network Access	The IT networks used to manage the platform are strictly controlled and have no access to portable media, the Internet, or email of any kind and are subject to the following additional restrictions: • These networks can only be accessed from the DSB office networks and secure remote access networks on remote control protocols. • Network traffic is restricted to defined entry points, and VPN traffic is controlled to the expected source IP. • Where necessary, virtual workstations are provided in data centres and allocated to unique individual users, monitored by login activity. • Additionally, client-server login/access is audited. • All firewall activity is logged.
	Remote access connectivity to User-related data is required for employees or any other third party (e.g., suppliers) via an encrypted VPN into a management server. This access requires authorisation and is audited.
	Remote access requests reviewed for appropriateness, approved, and only granted to the DSB from their office locations. Remote access is appropriately modified to reflect changes in responsibility, including transfer and termination.
	System logging and monitoring are performed on remote user activities once within the environment.
Network Segregation	Segregation is maintained between the IT network used to provide service to the User, the network used to provide services to other customers, and the networks used by other parts of the third-party Supplier's IT network. Firewalls are used for DMZ (Internet-facing systems).
	The network architecture segregates pre-production and production environments.
Firewalls	Access to firewalls and the rule sets they contain is limited to authorised users.
	Firewall rules are reviewed as part of the external security testing programme. Typically, rules are disabled for a fortnight before being deleted. Additionally, all firewall configurations for legacy customers are removed.
Other Technology	Wireless technology is not used to transmit User Information or access User IT systems.
	VoIP technology is not used to access User Information or User IT systems.
Intrusion Detection and Prevention	Intrusion detection and prevention controls are implemented to protect against unauthorised attacks or change. They are configured: • to alert when unauthorised and suspicious activity is detected • analyse suspected intrusions; and • identify and respond to new attacks.
Audit Logs	The DSB retains all login and event log activities from the monitoring and logging services. These are stored in centralised cloud storage location.
Personally Identifiable Information (PII)	A log of the PII data accessed by users is retained. Protection is enforced by using the third-party services inbuilt operations. In addition, the logging facilities and log information are protected against tampering and unauthorised access to PII.
User Activity Monitoring	The DSB records all login and access attempts across all infrastructure locations.

Standard / Process	Details
	Only those individuals whose role requires them to manage/maintain logging and monitoring services have administrative access.
Data Leakage Policy	The DSB has controls in place to prevent data leakage through removable storage devices. Accepted use is only permission to encrypt devices before saving data onto the device.
Environment Segregation	Development, test, and operational facilities are segregated to reduce the risks of unauthorised access or changes to the operational IT systems.
Change Management Process	The DSB maintains a documented change management process that covers: • Network Changes • Application Software Changes • Database Changes • Physical Environment Changes, (**Change Management Process**).
	The Change Management Process has appropriate controls in place to manage changes to the environment, including the following: • Clearly identified roles and responsibilities. • Impact or risk analysis of the change request. • Testing before implementation of change. • Authorisation and approval. • Post-installation validation. • A 'recover position' so that IT systems can recover from failed changes or unexpected results. • Backout or recovery plans.
Patch Management	The DSB's patch management procedures related to User relevant systems include the following: • Process for determining if vendors have released new patches and hotfixes • The timeframe in which patches are installed once the vendor has released it • If patches are tested before installing them on a production system
Technical Standards	Technical workflows are in place for applying emergency fixes to IT systems used to provide services to the User.
Release Management	The DSB maintains a release management process that requires that releases are subject to change and version control.
Capacity Management	The DSB maintains capacity management processes to ensure that IT systems monitor, tune, and provide projections of future capacity requirements to ensure system performance.
	The capacity management process takes into account the following before new applications, systems, upgrades/updates and new versions are pushed into the production environment: • Performance and capacity requirements to ensure adequate capacity and system resources to deliver the required system performance. • Error recovery and contingency plans. • Preparation and testing of routing operation procedures. • Agreed onset of security controls. • Effective manual procedures. • Analysis outlining the potential impact of the change on existing systems and the organisation's overall security. • Training in the operation or use of the new system.
Acceptance Criteria	The DSB has acceptance criteria that must be met for new IT systems, upgrades and new versions.

Standard / Process	Details
Monitoring InfoSec Events	The DSB maintains policies, processes and procedures to monitor Information Security events. These policies include: • Reporting of incident requirements and processes. • Reporting of security weakness. • Process of evidence collection, analysis and remediation of an incident. • Post-mortems and resulting actions are taken. • The capture of unauthorised access and unsuccessful access attempt. • The creation, modification and use of privileged user accounts. • The monitoring of support and development staff activity in production environments. • Unauthorised devices cannot be connected to the network without being approved. • Alerts from network gateways and firewalls. • Alerts from intrusion detection and prevention systems.
	As part of the 27001 accreditation to the vendors and the DSB. There are processes in place to baseline and monitor system activities, exceptions and information security events which include the following: • Audit logs include relevant event details such as user IDs, dates, times and details of an event, changes to system configuration, files, protocols, etc. • Monitoring system use includes details for authorised access, privileged operations such as privileged accounts, unauthorised access attempts, system alerts or failures and changes to or attempts to change system security settings and controls. • Protection of logging and monitoring systems against tampering and unauthorised access.
Privileged user activity logs	Privileged user activity logs are independently reviewed by users whose activity is not included in the logs.
Logging	The DSB logs faults, analyses them and takes any required action.
Remote Devices	The DSB maintains a policy on and restricts personal devices on the network that could access User information or User IT systems.
Open Source Software	The DSB uses the below list of Open Source software and maintains the appropriate patch management of these to ensure application governance: • NGINX • Tomcat • Kafka • Solr • Zookeeper • JAVA • Mongo DB • Cordra
Source Code	The DSB restricts access to program source code to prevent the introduction of unauthorised functionality and to avoid unintentional changes.
Penetration Testing	The DSB performs regular network vulnerability scanning in each office. The scanning includes checking external IPs to analyse network vulnerabilities, identifying the open ports, which software listens to these ports, checking the software is vulnerable, security settings, etc.). Intrusion detection and monitoring services are used for network audits. The output of the scanning is provided to the Office of the CISO for review. It contains the vulnerabilities, their description and recommendation for the fix. The issues are

Standard / Process	Details
	registered and tracked. The scans are repeated until all issues are fixed.
Incident Reporting Process	The DSB maintains defined, implemented and maintained information security incident reporting processes that include: • A defined escalation process to the User (In the event of loss of User data) within one business day. • Investigate and remediate service disruptions caused by system or human error, such as failure to run a nightly batch job per service requirements. • Responses to information security-related incidents are prioritised, tracked, escalated and resolved.
Internal Audit	The DSB conducts internal audits at planned intervals to determine whether the control objectives, controls, processes and procedures: • Conform to the requirements of their information security management framework and relevant legislation or regulations; • Conform to the contractual information security requirements; • Are effectively implemented and maintained; and • Perform as expected.
Building / Hardware Protection	The IT systems and data centres used for the DSB are designed to:- protect IT systems from natural and manufactured hazards;- provide lockable server racks for IT systems;- segregate power cables from communications cables to prevent interference;- manage the temperature and humidity of IT systems in accordance with equipment manufacturer recommendations;- provide layered security zoning within the building;- protect the physical security perimeter from unauthorised access, damage, and threats; -provide resilience; and- detect unauthorised access.
Power Supplies etc.	All power supplies, temperature and humidity equipment used in the DSB data centres use: • uninterruptible power supplies (UPS) with a battery capacity to perform a controlled shutdown; • resilience to maintain service during maintenance; • surge protection equipment; • backup electricity generators; and • emergency lighting.
	The DSB data centres emergency equipment, including fire alarms, uninterruptible power supplies, backup electricity generators, emergency lighting and temperature and humidity equipment, are serviced and tested in accordance with manufacturer recommendations.
Monitoring	The DSB employs monitoring for IT systems in real-time.
BCP and DR	Please refer to the DSB Disaster Recovery and Business Continuity Policy which contains full details of the disaster recovery and business continuity policies and procedures.
External Party Details	The datacentres are AWS located in: • AWS EU West region, Republic of Ireland; and • AWS US East region, N. Virginia.
	Etrading Software Ltd is the management services partner.
	Rackspace (formerly Datapipe) is the service provision partner.
	The DSB data is encrypted to at least 128bit AES encryption during transmission to any external party.

Standard / Process	Details
External Party Management	All external parties have signed data confidentiality and a non-disclosure agreement.