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 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 of the Agreement 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 Datapipe maintains SOC 1, SOC 2, ISO 27001, FedRAMP, FISMA, PCI, and HITRUST compliance and security standards.
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 and are available for public download from https://github.com/ANNA-DSB/.
	FIX API users are also required to be complete successfully the DSB's FIX Client Certification process. The certification document is available for public download from https://github.com/ANNA-DSB/FIX/tree/master/docs.
Information Security Policy Document	The DSB maintains an Information Security Policy document that is aligned with external information security standards and will be reviewed annually.
	The Information Security Policy is currently published or communicated to all Third-Party employees and contractors.
Processes and Procedures	The DSB will maintain the standards and procedures in support of its IT processes and functions that is reviewed and, if required, updated annually.
	When significant change occurs, the continuing suitability, adequacy, and effectiveness of the processes and procedures are also reviewed.
Process Governance	The Derivatives Service Bureau (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

© DSB 2018

	The DSB: - Approve, maintain, consistently apply and enforce compliance with the policies, program plans, procedures and controls supporting the information security governance program. - Maintain clear lines of reporting, responsibility, accountability, communication of expectations and the delegation of appropriate authority supporting decisions. - Manage the effect of security issues on the firm, business lines and related processes. Oversee risk mitigation activities to address issues. - Maintain risk measurement definitions and criteria, establish acceptable levels of information security risks. - Require that data with similar criticality and sensitivity characteristics be protected consistently throughout the DSB - Coordinate information with physical security.
Process Governance	The DSB with regards to the information security governance program are 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 an information security risk officer who performs risk management functions.
	The information security officer: - Reports directly to the board or to senior program management - Have sufficient independence to perform their assigned tasks - Have the authority to respond to a security event where confidentiality, integrity, availability or accountability of an information system is compromised - Have capacity to order emergency actions to protect The DSB and its customers from an imminent loss of information or value - Hold 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 clients.
Client Information Disposal	The DSB maintains processes and procedures for the secure disposal of client Information - including paper based secure disposal and the disposal of any supporting storage media (i.e. Hard drives etc.).
	This includes provision for the secure transport and storage of client information prior to destruction.
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 client data.
	The Asset Inventory records asset owner, information classification applied to that asset and physical location of the asset.
Pre-Employment Screening (PES)	Pre-Employment Screening (PES) is completed prior to authorising access to Client information or Client systems and includes: Minimum background checks such as Criminal, Professional Qualifications, Identification, Solvency, proof of address.

Info Sec Training	The DSB provides an active IT Security Awareness Training program that includes as a baseline: - DSB Information Security Program - Using IT Resources - Information Management - Local and Remote Access - Internet Safety - Physical Security and Backups - Computer Security Review Each employee has to perform the IT Security Awareness training annually. The training material is reviewed and updated periodically by the Global IT Security Manager. The status of the security training is continuously followed-up by the management. Customized training materials can be created and the status of the training is tracked. The employees must state and sign that they have read the IT Security Awareness Training, understood it and agree to behave according to this.
	Project specific Data Privacy Awareness training can be created for the project staff, containing client specific data privacy or other requirements. The DSB has an active IT Security Awareness Training Program as a baseline: - The DSB Information Security Program - Using IT Resources - Information Management - Local and Remote Access - Internet Safety - Physical Security and Backups - Computer Security Review Each employee has to perform the IT Security Awareness training annually. The training material is reviewed and updated periodically by the Global IT Security Manager. 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 prior to being on-boarded in accordance with relevant internal polices, 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.
Employment Policy	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 as it relates to Information Security, including privacy, and other organizational policies and procedures relevant for their job functions at least annually. Additionally, there is a process to track compliance to the organization'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 client information or client IT systems is removed on or before the last day of service and that the DSB owned devices that can store or access Client information are returned.
Physical Security	The DSB maintains a policy, standard and procedures in support of physical security which include physical access to the building, access control processes and emergency procedures

Physical Security	All personnel entering the premises are forced to enter through a controlled entry point that is monitored by a receptionist or security guard and they are required to provide some 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 authorization procedures are in place to cover granting, removing and reviewing of access, including the retrieval of access keys/ID's, and do the procedures apply to all persons (e.g., employees and suppliers) requiring access to the premises.
	Physical access to the site or building includes: - Manned reception area to control physical access to the site or building (manned 24/7). - All entrance points, main perimeter walls and exit points to the facility 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. - Entrances to loading and delivery areas monitored by CCTV. - Restricted to authorised personnel only by key card access.
	Visitors are required to be escorted by a responsible employee. Visitors include friends, repairmen, computer suppliers, consultants (unless long term, in which case special guest access is provided), maintenance personnel, and external auditors.
	Building access is authorised by the building management company 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 authorized persons. Roles and access are regularly reviewed. The employees have to sign a confidentiality / non-disclosure agreement.
	All fire doors on the security perimeter of the building have been fitted with alarms which 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 in 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.
	A risk assessment has been conducted by an expert to evaluate if the building may be at risk from terrorist activity. A safe area exists where building occupants can retreat to during a terrorist incident.
	A risk assessment has been conducted by an expert to evaluate how the building may be at risk from fire, earthquake, flood, explosion, civil unrest or any other type of natural or man-made disaster.
IT System Maintenance	IT systems are maintained in accordance with the manufacturers recommended service intervals and specifications.

Client Information Disposal	Procedures are in place to delete Client 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 items of equipment containing storage media must be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive data will require a risk assessment to determine if the items should be destroyed, repaired or discarded.
Client Info: Operational Procedures	The DSB maintains operational procedures for all IT systems which are used to access, manage, store or process client information or access to client IT systems. This includes: - technical vulnerability and patch management. - network management. - regular check of compliance with security implementation standards
	There is no user access to the network or systems that store, process and transmit client 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 Client data in the following way: - Secure software download and installation procedures are documented - Require an approval to download and install 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 Backup / Recovery	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.
	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 Client information are encrypted
User Access	The DSB maintains an Access Management policy, standard(s), and procedures which cover Authentication, Password Management, Entitlements and Segregation of duties around this application.
	The DSB ensures that there is segregation of duties to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. This includes the separation of duties between individuals who request access, authorize access, enable access, and verify access.

User Access	The process for provisioning and deprovisioning 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 authorization lists of user access rights are reviewed on an annual basis. - 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 unauthorized activities are monitored/reviewed and addressed in a timely manner by the proper level of management - as per 27001 framework. Additionally, logs are created to identify use 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 of the network (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 Client 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 logon
	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.
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. - These networks are only able to be accessed from The DSB office networks and secure remote access networks on remote control protocols (RDP). - Network traffic restricted to defined entry points and VPN traffic is controlled to the expected source IP. - Where necessary virtual workstations are provided in DSB data centres and are allocated to unique individual users, with login activity is monitored. - Additionally, client server login/access is audited. - All firewall activity is logged.
	Remote access connectivity to client 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 is 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 is performed on remote user activities once within the environment.

Network Segregation	Segregation is maintained between the IT network used to provide service to the Client and 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 configuration for legacy customers are removed.
Other Technology	Wireless technology is not used to transmit Client Information or access Client IT systems.
	VoIP technology is not used to access Client Information or Client IT systems
Intrusion Detection and Prevention	Intrusion detection and prevention controls are implemented to protect against unauthorised attack or change. They are configured: - to alert when unauthorised and suspicious activity is detected - analyse suspected intrusions - identify and respond to new attacks
Audit Logs	The DSB retains all login activity and event log activity in Tripwire and Alert Logic's repositories. These repositories are backed up to encrypted tape and held offsite, and can be restored for analysis.
Personally Identifiable Information (PII)	A log of the PII data accessed by users are retained and is able to offer Varonis file access auditing on file shares. In addition, the logging facilities and log information are protected against tampering and unauthorised access to PII.
User Activity Monitoring	The DSB records all attempts to access server and network nodes, including failed and valid logins, and this data is analysed in Alert Logic Additionally, all server, network and firewall nodes are configured to log to two read-only log facilities in region These read-only logs are then ingested and analysed by Alert Logic.
	Only those individuals whose role requires them to manage/maintain syslog, Tripwire and Alert Logic services have administrative access.
Data Leakage Policy	The DSB has controls in place to prevent data leakage through the use of removable storage devices. Accepted use is only permissioned to encrypted devices before saving data onto the device.
Environment Segregation	Development, test, and operational facilities are segregated in order 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
	The Change Management Process has applicable controls in place to manage changes to the environment. - Clearly identified roles and responsibilities - Impact or risk analysis of the change request - Testing prior to 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 client relevant systems include the following: - Process for determining if new patches and hotfixes have been released by vendors - Timeframe in which patches are installed once it has been released by the vendor - If patches are tested before installing them on production system
Technical Standards	Technical workflows are in place for applying emergency fixes to IT systems used to provide services to the Client
Release Management	The DSB maintains a release management process which requires that releases are subject to change and version control.
Capacity Management	The DSB maintains capacity management processes to ensure that IT systems are able to monitor, tune, and provide projections of future capacity requirements to ensure the required system performance
	The capacity management process takes into account the following before new applications, systems, upgrades/updates and new versions are pushed into production environment: - Performance and capacity requirements to ensure availability of adequate capacity and system resources to deliver the required system performance. - Error Recovery and Contingency Plans - Preparation and testing of routing operation procedures - Agreed set of security controls - Effective Manual Procedures - Analysis outlining the potential impact of the change on existing systems and the overall security of the organization - Training in the operation or use of the new system
Acceptance Criteria	The DSB has Acceptance criteria in place for new IT systems, upgrades and new versions
Monitoring Info Sec Events	The DSB maintains policies, processes and procedures to monitor Information Security events. These policies include: - Reporting of incident requirements and process - Reporting of security weakness - Process of evidence collection, analysis and remediation of an incident - Post-mortems and resulting actions 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 on 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
Monitoring Info Sec Events	As part of the 27001 accreditation to the vendors and therefore the DSB. There are processes in place to baseline and monitor system activities, exceptions and information security events which include the following. - Audit logs which include relevant event details such as user IDs, dates, times and details of event, changes to system configuration, files, protocols, etc. - Monitoring of system use which include details for authorized access, privileged operations such as use of privileged accounts, unauthorized 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 unauthorized 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 take any required action
Remote Devices	The DSB maintains a policy on and restricts the use of personal devices on the network that could access Client information or Client 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- Handle.NET Registry
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 of the company based on the Annual Audit Plan. The audit includes checking external IPs for analysing network vulnerabilities; identify the open ports, which software listening these ports, check the software is vulnerable, security settings etc.…). - Alert logic and Tripwire are used for network audit. - The output of this audit is the Audit Report that contains the vulnerabilities, their description and recommendation for the fix. The issues are registered and tracked. - The audits are repeated until all issues are fixed.
Incident Reporting Process	The DSB maintains a defined, implemented and maintained information security incident reporting processes that includes: - A defined escalation process to the client (In the event of loss of client 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 in accordance with service requirements - responses to information security related incidents are prioritized, 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 man-made 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 Plans	The DSB will provide a copy of the Business Continuity and Disaster Recovery Plans
	These will be reviewed and tested annually
External Party Details	The Datacentres are AWS: AWS EU West region, Republic of Ireland AWS US East region, N. Virginia
	etrading software are the Management Services Partner
	Datapipe/Rackspace are the Service Provision Partner
	The DSB data is encrypted to at least 128bit AES encryption during transmission to any external party
External Party Management	All external parties have signed a data confidentiality and a non-disclosure agreement.