Data Security and Storage Policy for Market Data Service International (MDSI)

Purpose

This policy governs the secure handling, storage, and processing of the Bicycle Association's (BA) Market Data Service covering both the UK and International markets (MDSI) using Amazon QuickSight and Snowflake as the principal technologies. It ensures compliance with UK, EU and Australian data protection laws, including the General Data Protection Regulation (GDPR), and aligns with industry best practices for data services.

Scope

This policy applies to all market data ingested, processed, visualised, or stored using:
- Amazon QuickSight for business intelligence and data visualisation.
- Snowflake for cloud-based data warehousing and analytics.

General

The BA owns MDSI and sub-contracts the data processing operation and ongoing service development to Mesosys Ltd and from time to time other suitably competent third party suppliers. All sub-contractors are bound by strict confidentiality and data anonymity clauses meaning that no retailer data is ever exposed to any other party without their permission.

1. Data Residency and Storage

1.1 Amazon Quick Sight

Our data for MDSI is stored in SPICE, QuickSight's in-memory engine, within the selected EU AWS regions of Ireland or Frankfurt. These can be specifically selected where required.
MDSI is configured to allow Quick Sight to operate exclusively in EU regions to ensure data sovereignty.

1.2 Snowflake

Snowflake supports UK & EU data residency across the AWS platform.
Market Data and the MDSI product is stored in the designated EU region of AWS EU (Ireland) to comply with GDPR and regulatory requirements (aligned to Privacy Act 1988 - APPs). This can be stored based on geographic specific requirements i.e. only in EU West (Frankfurt).

2. Security Controls

These are the technical security controls that are used to ensure encryption and access management to industry standards.

2.1 Encryption

- At Rest: All data is encrypted using AES-256.
- In Transit: TLS 1.2+ is enforced for all data transfers.
- Customer-Managed Keys: Both platforms support customer-managed encryption keys for enhanced control. These are currently used to manage role and row level security features for MDSI.

2.2 Access Management

- Role-Based Access Control (RBAC) is enforced.
- Multi-Factor Authentication (MFA) is required for all administrative access using Duo as the Authenticator App

with 3-way code distribution between Mesosys and the BA to ensure Retailer anonymity and compliance with contract obligations.
- Least Privilege Principle is applied to all user roles.

2.3 Monitoring and Auditing
- AWS CloudTrail and Snowflake Access History are used to log and monitor all access and changes.
- Logs are retained in accordance with industry standards (e.g., GDPR, FCA).

3. Compliance and Certifications

3.1 Amazon QuickSight (via AWS)
- GDPR: Full support for data subject rights and data processing agreements.
- ISO/IEC 27001, 27017, 27018: Information security and cloud privacy.
- SOC 1, 2, 3: Independent audits of internal controls (SOC 2 & 3 specific to MDSI).
- FedRAMP: For U.S. government-grade security (where applicable but not required for MDSI).

3.2 Snowflake
- GDPR: Data residency and processing controls aligned with UK & EU law.
- ISO/IEC 27001, 27017, 27018: Certified for cloud security and privacy.
- SOC 1 Type II & SOC 2 Type II: Verified operational and financial controls (SOC 2 & 3 specific to MDSI).
- FedRAMP Moderate: For U.S. federal data handling (where applicable but not required for MDSI).

4. Market Data-Specific Considerations
- Latency Sensitivity: Ensure low-latency access to real-time and historical market data through optimised Snowflake compute clusters and SPICE caching.
- Data Retention: Retained market data in accordance with regulatory requirements (e.g. 7 years).
- Data Classification: Market data is classified as confidential and must be protected accordingly.
- Third-Party Data Feeds: Ensure all third-party data providers comply with equivalent security and compliance standards.

5. Data Retention Policy

5.1 Regulatory Requirements
Market data, including trade records, communications, and analytics, must be retained in accordance with the following regulations:
- EU Directive 2014/65/EU: Requires data service providers to retain records of all services, activities, and transactions for a minimum of five years, and up to seven years if requested by a competent authority. This includes voice recordings, electronic communications, and market data feeds used in decision-making or trade execution.

5.2 Internal Retention Standards
To meet and exceed regulatory expectations, the following internal standards apply:
- Retention Period: All market data, including raw feeds, processed analytics, and user-generated reports, will be retained for the duration of the service back to day one where relevant. Communications (emails, meeting recordings) related to MDSI decisions will also be retained for seven years.
- Storage Location: Data will be stored in EU-based regions of Snowflake and Amazon QuickSight (e.g., AWS EU (Ireland). Archived data (where relevant) will be encrypted and stored in cold storage tiers with retrieval capabilities.
- Data Integrity and Auditability: All retained data must be tamper-evident, timestamped, and indexed for

efficient retrieval. Audit logs of data access and modifications will be retained for the same duration.
- Deletion and Disposal: Upon expiration of the retention period, data will be securely deleted using cryptographic erasure and certified data destruction protocols. Deletion logs will be maintained for audit purposes.

6. Escalation Process

To ensure timely and effective response to security incidents, the following escalation process is in place:

- Level 1 – Initial Detection and Triage
All users and automated systems must report anomalies or suspected breaches to Mesosys via the designated email. Alerts and notifications are in place to manage this in AWS and Snowflake.

- Level 2 – Security Team Review
Mesosys will assess the incident severity and classify it as Low, Medium, or High. For Medium and High severity incidents, the issue is escalated to the DPO within 2 hours of detection (Daniel Gillborn in this context).

- Level 3 – Executive Notification
If the incident is classified as High severity (e.g., potential data breach, system compromise), the Data Protection Officer (DPO – Daniel Gillborn on behalf of the board of directors) is notified immediately. A cross-functional incident response team is assembled including the BA, Mesosys and representatives from Snowflake and Quick Sight.

- Level 4 – Regulatory and Legal Involvement
If the incident involves regulatory exposure, the Data Protection Officer (DPO – Daniel Gillborn in this context) and Legal Counsel (David Hill & Alexis Colfer) are engaged to assess notification obligations under GDPR or other applicable laws.

- Post-Incident Review
A root cause analysis and lessons-learned session is conducted within 5 business days of incident resolution. Findings are documented and used to improve controls and response procedures.

7. Data Breach Resolution Process

In the event of a confirmed or suspected data breach, the following steps will be taken:

1. Identification and Containment
   - Immediate isolation of affected systems to prevent further data loss.
   - Activation of the Cyber Incident Response Plan (CIRP).

2. Assessment and Classification
   - Determine the nature, scope, and impact of the breach.
   - Identify affected data types (e.g., company data, market data, access credentials).

3. Notification
   - Notify the DPO within 1 hour of breach confirmation.
   - Notify the relevant supervisory authority where relevant within 72 hours as required by GDPR.
   - Notify affected data subjects or parties (Members, Subscribers).

4. Remediation
   - Apply patches, revoke credentials, or reconfigure access controls as needed.
   - Monitor systems for signs of continued compromise.

5. Documentation and Reporting
   - Maintain a breach register (Template in place) with details of the incident, response actions, and outcomes.
   - Submit internal and regulatory reports as required.

6. Review and Improvement
   - Conduct a post-breach review to identify gaps and update policies, training, and technical safeguards.

Cyber Incident Response Plan (CIRP)

MDSI response to cyber incidents

Objectives and Scope

The objectives of the CIRP are to:

- Establish a clear and consistent framework for responding to cyber incidents
- Minimise the impact and duration of cyber incidents on MDSI
- Protect MDSI assets, data, and reputation from cyber threats
- Ensure compliance with the applicable laws, regulations, and policies
- Improve the organisation's cyber resilience and readiness
- Maintain appropriate security certification (through our providers).

The scope of the CIRP includes:

- All types of cyber incidents that affect information systems, applications and data
- All MDSI business matters and functions within that are involved or affected by cyber incidents
- All key stakeholders that need to be notified or consulted during cyber incident response events
- All phases and activities of cyber incident response, from identification to closure.

Cyber Incident Classification and Escalation Criteria

The cyber incident classification and escalation criteria are used to determine the severity level and the urgency of the cyber incident response. The severity level indicates the impact and risk of the cyber incidents on MDSI and the urgency indicates the time frame and priority of the cyber incident response. The following table summarises the cyber incident classification and escalation criteria:

Severity Level	Impact and Risk	Urgency	Escalation
Low	The cyber incident has minimal or no impact and risk on the organisation's operations, assets, data, and reputation	The cyber incident response can be performed within the normal working hours and procedures	The cyber incident can be handled by the Mesosys team and reported to the CIRT coordinator (Daniel Gillborn)
Medium	The cyber incident has moderate impact and risk on the organisation's operations, assets, data, and reputation	The cyber incident response requires immediate attention and action	The cyber incident requires the activation of the CIRT and the notification of the CIRT leader and the board (Daniel Gillborn)
High	The cyber incident has significant or critical impact and risk on the organisation's operations, assets, data, and reputation	The cyber incident response requires urgent and priority action	The cyber incident requires the activation of the CIRT and the notification of the CIRT leader (Danel Gillborn), the board, and external stakeholders

Cyber Incident Response Team

Senior Leadership	***Primary Contact***	***Backup Contact***
Incident Manager	Daniel Gillborn, +447730490357	Simon Irons +447776238365
Infrastructure Management		
Systems Manager	Peter Cameron +447788581331	Daniel Gillborn +447730490357
External Technical Liaison (Snowflake & Quick Sight)	Peter Cameron +447788581331 peter.cameron@meso.systems	Scott Wilkinson scott.wilkinson@meso.systems
Business Management		
Product Owner	Simon Irons +447776238365	Daniel Gillborn +447730490357
Legal Advice	Alexis Colfer, alexis@legallycompliant.net	Daniel Gillborn +447730490357
Marketing/PR	Tom Payton tom@bicycleassociation.org.uk	Simon Irons +447776238365
External Contacts		
Mesosys	Peter Cameron +447788581331 peter.cameron@meso.systems	
Snowflake	Max Douglas +447845672594 max.douglas@snowflake.com	
Toucan Tech	Tom Payton (BA) tom@bicycleassociation.org.uk	Jenifer Kinaird - Toucan Tech - jennifer@toucantech.com
Action Fraud	0300 123 2040 https://www.actionfraud.police.uk	
Insurers	Paul McGirr - Butterworths	pmcgirr@butterworthspengler.co.uk
National Cyber Security Centre (NCSC)	0300 020 0964 https://report.ncsc.gov.uk	

Prevention and mitigations

Prevention and mitigations are the measures and actions that aim to reduce the likelihood and severity of the disruptions caused by the threats and vulnerabilities identified in this policy. These can include:

- Antivirus: The antivirus is the software that detects and removes the malicious software, viruses, worms, trojans, or ransomware, that could infect our systems. Antivirus is installed and updated on all our devices as a part of our access to Google Suite and Shared Drives.
- Firewall: The firewall is the software or hardware that monitors and controls the incoming and outgoing network traffic. A firewall is installed at our boundaries and a software equivalent on every device accessing the Internet – supported by Google Suite. We also have a CDN (Cloudflare) in front of the main BA website.
- Encryption: The encryption is the process of transforming the data into an unreadable format using a secret key or algorithm. The encryption is applied to all our devices and the data transmitted and received over our network and Internet.

- Authentication: Passwords and Multi Factor Authentication are needed to access all of our resources using authentication. Access to applications is based on least required permissions for the users role. We use authentication apps such as Duo to support this.
- Backup: The data backup is the process of copying and storing the data from the primary systems to a secure and remote location, such as a separate cloud service or an external resources as a part of the cloud based service. For this we use the native services of both Google and AWS.
- Infrastructure Redundancy: Backup infrastructure providing instant failover in the event of an outage, an example of this would be Snowflake or Quick Sights multiple failover facilities as a part of a cloud based service provision.

Phases and Activities

The cyber incident response process consists of five phases summarised in the table below, each phase has a set of activities that the CIRT performs to achieve the objectives of the phase.

Phase 1: Identification

Detect and confirm a cyber incident.

- Monitoring and alerting: Monitor and analyse the data and events from various sources, such as security tools, logs, reports, and notifications. Configure alerting mechanisms that can notify of any suspicious or anomalous activities or indicators of compromise.
- Validating and triaging: Validate and triage the alerts and notifications received, and determine whether they are false positives, false negatives, or true positives. Prioritise the alerts and notifications based on their severity, impact, and urgency, and assign them to the appropriate CIRT members or teams for further investigation.
- Investigating and scoping: Investigate and scope the cyber incident and gather as much information as possible about its nature, cause, source, extent, and impact. Identify the affected systems, data, and users, and assess the potential risks and consequences of the cyber incident.

Phase 2: Containment

Limit the damage and stop the spread of the cyber incident.

- Identify the containment strategy: Choose the best containment strategy for the cyber incident, based on the information and analysis from the previous phase. The containment strategy can be either short-term or long-term, and can involve actions such as disconnecting, blocking, quarantining, or patching the affected systems or networks.
- Implementing the containment strategy: Implement the chosen containment strategy and monitor and verify its effectiveness. The process should be documented and communicated to the relevant stakeholders.
- Evaluating the containment strategy: Evaluate the containment strategy, and determine whether it has achieved its objectives, or whether it needs to be modified or replaced. Identify and address any issues or challenges that arise during the containment phase, such as technical difficulties, operational disruptions, or legal implications.

Phase 3: Eradication/Mitigation

Eliminate the root cause and the traces of the cyber incident from all affected systems.

- Identifying and removing the malicious elements: Identify and remove the malicious elements that caused or contributed to the cyber incident, such as malware, emails, backdoors, vulnerabilities, or misconfigurations.
- Restoring and securing the systems and networks: Restore and secure the systems and networks that were affected by the cyber incident and ensure that they are functioning normally and securely. Where applicable the latest security patches should be applied and security scans on all devices to verify their integrity and compliance.
- Collecting and preserving the evidence: Collect and preserve the evidence related to the cyber incident, such as logs, reports, screenshots, or forensic images. Follow the proper chain of custody and documentation procedures and store the evidence in a secure location. The evidence can be used for further analysis, investigation, or legal action.

Phase 4: Recovery

Restore and resumes the normal operations and services of the organisation.

- Planning and testing the recovery: Plan and test the recovery process, and ensure that it is feasible, effective, and efficient. Consider the potential risks and impacts of the recovery process and prepare contingency plans and backup solutions in case of any failures or complications.
- Executing and monitoring the recovery: Execute and monitor the recovery process and ensure that it is completed successfully and smoothly. Document and communicate the recovery process and its results to the relevant stakeholders.
- Validating and verifying the recovery: Validate and verify the recovery process, and ensure that it has met its objectives, and that no residual issues or problems remain. Confirm that systems, networks, and services are fully functional and operational.

Phase 5: Closure

Evaluate the cyber incident and the CIRT process, identify and implement the lessons learned.

- Conducting the post-incident review: Analyse the cyber incident and the CIRT process from various perspectives, such as technical, operational, organisational, and legal. Identify the strengths, weaknesses, opportunities, and threats of the cyber incident and the CIRT process, and determine the root causes, contributing factors, and key findings.
- Preparing the post-incident report: Prepare a post-incident report and document the cyber incident and the CIRT process in a comprehensive and concise manner. The post-incident report should also include the recommendations, action items, and best practices for preventing, detecting, responding, and recovering from cyber incidents in the future.
- Implementing the improvement actions: Implement the improvement actions that were derived from the post-incident review and report and monitor and measure the effectiveness and efficiency of the improvement actions and make any necessary adjustments or modifications.

Threat Types (most common)

Threats	Identify	Containment	Eradication/ Mitigation	Recovery	Closure	Proactive remediation
Phishing	Source Payload Affected devices Compromised credentials	Isolate device(s) Disable sync for affected users Block outgoing emails/data	Remove affected emails and submit to Google / AWS Check for email rules that may have been added Change user(s) password	Recover lost data Ensure integrity of remaining user data, company data and all systems	Did our AV/browser detect/block it? What can we change? Reinforce defences	On going cyber security awareness Phishing tests Dark web monitoring Web breach monitoring
Virus	Source Payload Affected devices Compromised data	Isolate device(s) Block outgoing data Secure backups	Clean affected devices(s) with standalone AV e.g. Malwarebytes or Reimage device(s) using known good image Change user(s) password	Restore compromised data Ensure integrity of all user data, company data and systems Monitoring	Did our AV detect it? What can we change? Reinforce defences	On going cyber security training Enabling new security within existing products
Ransomware	Source Payload Affected devices Compromised data	Turn off Internet Isolate device(s) Secure backups	Change user(s) password	Restore compromised data Monitoring	Why didn't our AV detect it? What can we change? Reinforce defences	On going cyber security training Enabling new security within existing products

Threats	Identify	Containment	Eradication/Mitigation	Recovery	Closure	Proactive remediation
Web/partner apps			Change password/update MFA	SLAs Monitor service status Vendor reporting	Understand how the app was compromised Is the company taking a proactive approach to ensure this won't happen again Investigate alternatives	DPIAs User training Enforce complex passwords and MFA Access services from company devices

Author	Version Number	Revisions	Date
Daniel Gillborn	1.1	3rd Draft	19/05/2025
Daniel Gillborn	1.2	4th Draft	09/03/ 2026