Chief Data Officer

MHI Data Policy

December 2019 – Version 1.3

Mizuho International plc
Mizuho House
30 Old Bailey
London
EC4M 7AU
Telephone +44 (0) 20 7236 1090

Content

1 Introduction

This document sets out the Mizuho International plc (MHI) Data Policy. This policy applies to MHI, including overseas offices, branches and subsidiaries.

1.1 Definitions, Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this document

BRC	Board Risk Committee
C&IC	Change and Implementation Controls Committee
CEO	Chief Executive Officer
CDO	Chief Data Officer
CRO	Chief Risk Officer
DSA	Data Supply Agreement
DISC	Data and Information Security Committee
ExCo	Executive Committee
ISD	Information Systems Department
MHEU	Mizuho Securities Europe GmbH
MHI	Mizuho International plc
MHSC	Mizuho Securities Co., Ltd.
NPC	New Product Committee
ORC	Operational Risk Committee
RMGCC	Risk Management Governance & Control Committee

1.2 Purpose

This document defines the governance and management of data at MHI. The principles in this Data Policy underpin MHI's effective management of data in order for it to achieve its business objectives.

The purpose of this document is to detail the Data Management Framework and how it relates to other data policies across MHI.

1.3 Scope

This document provides an overview of MHI's data management framework and the specific roles and responsibilities of senior management and relevant stakeholders in relation to management and use of data under the data principles of MHI's Data Management Framework.

All provisions in this document are made to regulate MHI's own affairs, as well as MHEU's affairs provided by MHI to MHEU under the existing Outsourcing Services Agreement between the two aforementioned entities. MHI ensures that all services and procedural steps covered by or described in this document are performed in accordance with the aforementioned Outsourcing Services Agreement as well as in line with the laws applicable to MHI and MHEU respectively.

1.4 Approval

This document is endorsed DISC by and approved by the ExCo.

2 Data Management Framework

MHI's framework for managing data is made of 3 pillars and can be summarised as follows:

Data Policy: This data policy details the governance and management of data at MHI.

Data Principles: The MHI Data Principles articulate what should be considered and strived for in the management of our data.

Departmental Data Processes: Each department is responsible for maintaining the processes and documentation for the data owned by the department.

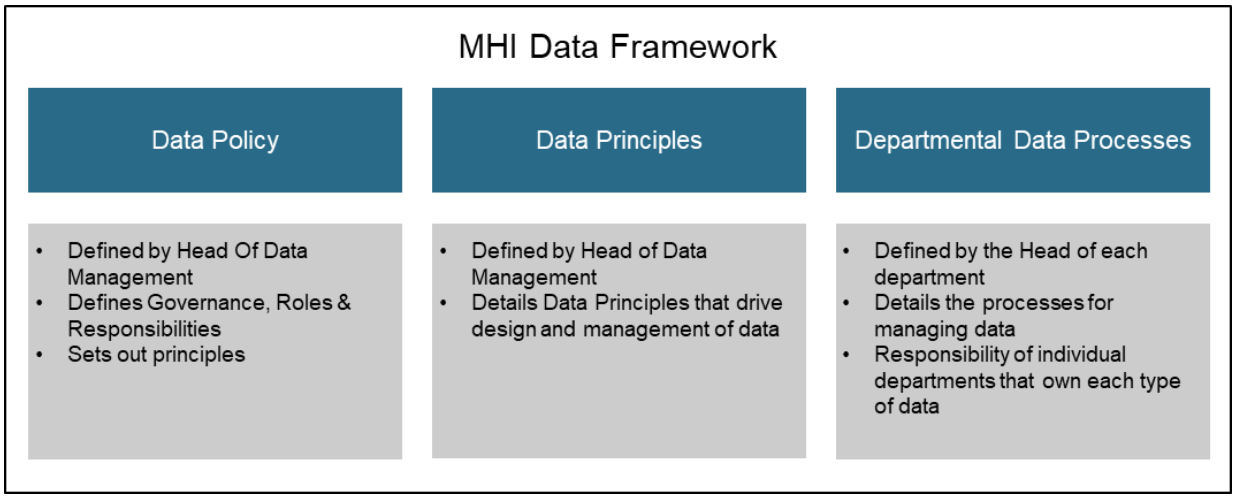

Figure 1

2.1 Data Policy

This policy document is the primary data policy at MHI. As such other data related policies at MHI need to be compliant with this document.

2.2 Data Principles

Data quality is the responsibility of all members of staff as part of their day to day roles. MHI has laid out data principles to which all members of staff should adhere. They are summarised in section 4 with the full details available in a supplementary document, MHI Data Principles.

2.3 Departmental Data Processes

Data is assigned to specific departments who have ownership responsibilities for that data on behalf of MHI. Data owners are responsible for defining and managing the processes around the data they own. Specifically, each data owner is responsible for documenting and running the data policies and procedures for their respective data to cover maintenance, quality assurance and retention.

2.4 Data Control Framework

Data governance driven from our inter-departmental data flows as noted in Figure 2: Data control framework.

When data is shared between two or more departments, business functions naturally agree what data is shared, the quality of the data and the timing. A Data Supply Agreement (DSA) is a simple document to standardise this process and record the agreement.

The DSA is a light but very important document as it facilitates the MHI data governance

- The data quality requirements in the DSA are used by IT teams to include validation rules.
- DSA stakeholders are responsible for tracking the results of the validation rules and resolving issues.
- The Data Office helps to govern the quality of the data flows through KPIs and metrics generated from the results of the validation rules. This being a second line of defence.

Data controls (KPIs and metrics) are closely related to the interfaces and data supply agreements.

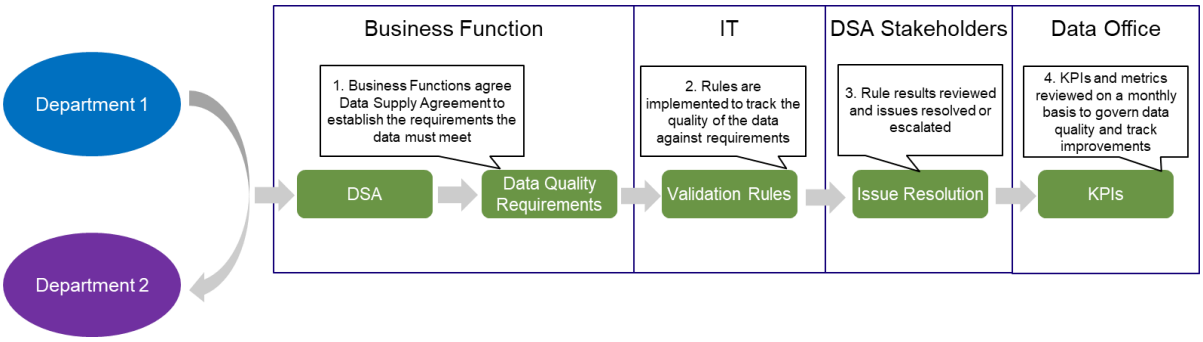

Figure 2: Data control framework

3 Governance

3.1 Governance Arrangements

MHI asserts that high quality data is a vital part of our business operations and is essential to achieving its business objectives. The Board of Directors is ultimately responsible for effective data management within MHI. It has delegated the execution to the ExCo which approves the data policy and ensures that the data processes within MHI are robust so that the reports presented to the Board, Regulators and other decision making stakeholders are reliable and fit for purpose.

3.2 MHI Board

The MHI Board has ultimate responsibility for the following:

- Approval of the data policies (delegated to the ExCo).
- Promotion the data policies and their application across all operations, project deliveries and strategic decisions;
- Defining MHI's policies on data confidentiality, integrity, retention and availability;
- Ensuring appropriate policies & procedures are in place to protect MHI's operations;

- Ensuring data issues and data management are taken into consideration for all strategic decisions.
- Review and approval of MHI's group risk data aggregation and risk reporting framework and ensure that adequate resources are deployed.
- Ensuring it can confidently rely on the aggregated information to make critical decisions about risk.
- Ensuring data provided to the Board provides it with the ability to monitor emerging trends through forward-looking forecasts and stress tests.

In many cases these responsibilities are executed by the **Board Risk Committee** (risk oversight) and **Executive Committee** (operational oversight) which have sub committees to focus on more specific details. They include

- Risk Management Governance & Control Committee
  - The RMGCC is responsible for ensuring an appropriate governance and control framework is provided for risk management. This includes ensuring Risk Management data processes enable adequate Risk Reporting and Data Aggregation.
- Data and Information Security Committee
  - Supervises the use of data across MHI, the implementation of the MHI Data Strategy and data related change programmes. It also oversees information security at MHI.
- New Product Committee
  - Reviews new products and business to identify risks and put in place procedures, or systems changes, to mitigate those risks.
- Change and Implementation Controls Committee
  - Responsible for approving the drawdown of budget and expenditure for any new IT projects and IT change so has to consider data implications of the projects.

More detail on the committees is available on MDL.

3.3 Chief Data Offices (CDO)

Management of data and data quality is inherent in daily activities, as well as strategic decisions taken at Board and Executive level. Effective data management is a key element in the ability to produce suitable risk measures by which to identify, assess, mitigate, monitor and report exposures.

The CDO is responsible for ensuring that data is managed effectively and in line with best practice. In order to achieve this, the CDO is responsible for:

- Championing correct data practices across MHI.
- Implementing an appropriate data governance structure.
- Creating and implementing the MHI data strategy.
- Ensuring clear business ownership of all important data types across MHI.
- Working with key technical staff in ISD (e.g. Data Architects) to ensure the implementation of the MHI Data Strategy and initiatives underpinning delivery against the Data Policy.
- Ensuring that each department has policies and tools to ensure that reporting is complete, accurate and timely.
- Ensuring business heads are informed of progress and issues related to data initiatives.
- Overseeing the implementation of data changes as it pertains to regulatory mandates.

3.4 All employees

Given the importance of data to the risk management of MHI, it is incumbent on all staff to be aware of the impact of their actions on data quality. All staff must be aware of the importance of data both within MHI and externally to regulators.

In addition to existing business, MHI's data requirements should be considered during the review and approval process for all new businesses and products.

3.5 Three lines of defence

MHI operates a three-lines-defence model:

- As the first line of defence, all staff have responsibility for identifying, monitoring and managing data quality in their business or support area. All staff have responsibility for ensuring that data quality issues and incidents are appropriately escalated.
- Support functions, as the second line of defence, have a role in overseeing the identification and management of data issues. This includes Operations, Product Control, Financial Control, Risk Management, ISD and the Data Office.
- As the third line of defence, Audit is responsible for assessing the design and operation of internal controls and adherence to policies and procedures, including the framework for managing Data.

3.6 Specific responsibilities

In accordance with Principle 5 of the MHI Data Principles, every department is responsible for data according to the MHI Data Inventory Matrix which details data ownership, accountability, consulted parties and informed parties for each type of data in MHI. Data owners are responsible for defining and managing the processes around the data they look after. Specifically, each data owner is responsible for documenting and running the data policies and procedures for their respective data.

4 Data Principles

A set of Key Data Principles have been defined to ensure the entire organisation understands what is required. These are explained in more detail in the MHI Data Principles.

1. Data is an Asset	Data is an asset that has value to the enterprise and is managed accordingly. More specifically, Data is a business asset and issue rather than an IT one.
2. We are a data driven organisation	Data is core to our business - without good data MHI will cease to function. As such, all members of staff have a responsibility to ensure data is accurate, complete and correct.
3. Data has meaning	Data semantics are as important as data content. Using correct data for the wrong purpose as it has been misinterpreted can be as damaging as incorrect data.

4. Data changes are centralised *Edit once, use many.*	Data should be edited in its master repository, by the data owner or an authorised delegate, and then distributed for consumption. On the occasions where business processes mandate local data overrides, these should be done under strict controls and subject to a robust governance process.
5. Data needs owners	Every data object has a data owner. Data should only be changed by the data owner (or an authorised person). A data owner is a trustee accountable for quality for the data they own.
6. Data is shared	Changes to data have a broader impact to the organisation than might be assumed. The implications of data changes should be considered before updating data or processes.
7. Know your data	The solution to data isn't just to have somewhere to store it. There are a number of key questions to answer as addressed by the MHI Data Requirements Template.
8. Data Security	Data is protected from unauthorized use and disclosure. This is important from a licensing, regulatory, sensitivity and privacy perspective.
9. Data is accessible	For data to deliver the most value it can, it must be made accessible so it may be exploited by other processes, systems and users.
10. Information is Data	Information is data regardless of how it is stored. Information stored in Excel spreadsheets, Word documents, emails, hardcopy and handwritten notes is data. The policy is not restricted to data stored electronically in a structured database.

5 Reporting and escalation

5.1 Data quality issues

Data quality issues that can't be fixed in real time, should be tracked and escalated to the data owner. Who should own getting them fixed at source.

5.2 Escalation

Where data issues are identified that pose a risk to MHI's operations or Risk Reporting and Data Aggregation capabilities, the issues should be raised to the Head of Data Management and logged for prioritisation and mitigation.

6 Document Maintenance

This document will be reviewed by the DISC and updated by the Head of Data Management at least annually.

This document will be updated by the Head of Data Management as necessary to ensure that it remains consistent with global policies issued by MHSC.

This document is endorsed by DISC and approved by the ExCo.

7 Related Documents

The Data Policy is underpinned by the policies and documents detailed below.

- New Product Committee - Terms of Reference
- Risk Management Governance & Control Committee - Terms of Reference
- Operational Risk Committee – Terms of Reference
- Data and Information Security Committee – Terms of Reference
- New Product Procedures document
- MHI Information Security Standards

  Basel Committee on Banking Supervision - Principles for effective risk data aggregation and risk reporting – Jan 2013
- The Open Group Architecture Framework (TOGAF) data principles

8 Document Control

Title: MHI Data Policy

Issue: Version 1.3

Date: 23 October 2019

Author: Harsharan Nijjar

Distribution:

Reference:

Document Signoff

Nature of Signoff	Person	Date	Role
Author	Harsharan Nijjar	30 Nov 2019	Head of Data Management
Approver	Kevin Gage as Chairman of the Executive Data Committee	30 Nov 2019	CIO and Head of Operations (CDO)
Endorsed	Executive Committee		
Authoriser	MHI Board of Directors		

Document Change Record

Date	Version	Author	Change Details
24/04/15	0.1	Gary Goldberg	Initial draft
27/04/15	0.2	Gary Goldberg	Updated and changes based on feedback
10/05/15	0.3	Gary Goldberg	Updated with feedback from ARCC.
20/05/15	0.4	Gary Goldberg	Updated with further feedback.
21/05/15	0.5	Gary Goldberg	Ratified by the Aggregation and Reporting Change Committee
28/05/15	1.0	Gary Goldberg	Endorsed by the MHI Executive Committee
08/08/16	1.1	Gary Goldberg	Updated address to Mizuho House and changed references from MSUKH to MHI.
11/01/18	1.2	Gary Goldberg	Added Section 2.4. Updated MHI principles.
09/12/19	1.3	Harsharan Nijjar	Updated after 2019 review to cover organisational changes primarily. Approval by ExCo from MHI Board.

			RMC to RMGCC EDC to DISC