INTRODUCTION

The Enterprise Data Management Policy ("EDM Policy") establishes a framework of responsible Data management best practices focused on the governance and protection of Royal Caribbean Group's ("RCG" or "Company") Data. Adherence to this EDM Policy ensures compliance with relevant laws and regulations, enhances Data Privacy controls, and mitigates risk.

This EDM Policy sets the minimum requirements to safeguard the Company's Data within the scope of these main Data components: Data access, Data Usage, and Data sharing. Additionally, this EDM Policy shall be used in conjunction with the Data Classification and Handling Standard ("Standard") which sets the minimum requirements to classify and handle the Company's Data. The main Data components addressed in the Standard are data classification, data handling, and data destruction.

1. Policy Detail

1.1 Scope

This EDM Policy applies to all Employees, referred to as Data Users herein, who use (access, maintain, and/or analyze), and share (internally and/or externally) the Company's electronic Data residing in enterprise Systems, such as, a Data store or a database.

1.2 Purpose

This EDM Policy, together with other policies, standards, procedures, and guidelines referred to in *Appendix A*, establish the minimum set of controls to be implemented, monitored, and audited to prevent Unauthorized access, Data Loss, or Unauthorized disclosure.

This EDM Policy sets forth the Company's minimum responsibilities of each Data User in implementing and maintaining the controls in *Section 2.1* below.

2. Rules and Guidelines

To ensure the Company's Data is protected, this EDM Policy establishes the permitted uses of Data for daily business operations, and the actions that are strictly prohibited. Requirements to be followed for permitted use are in *Section 2.2* and prohibited use are in *Section 2.3*.

2.1 Data User Roles and Responsibilities

All Data Users shall have the responsibility to protect and manage Data under their oversight to prevent Unauthorized Data Usage and/or Data sharing.

All Data Users shall be responsible for following EDM Policy requirements in conjunction with the organization's other policies, standards, procedures, and guidelines in *Appendix A* to ensure the Company's Data controls are maintained across all Data management functions across the enterprise.

In addition, Data Users identified as a Data Custodian, Business Data Steward, or Domain Steward would be accountable for undertaking additional responsibilities, as outlined in *Table 1* below.

TABLE 1: Defines Data User Roles and Responsibilities

DATA USER = All Employees that use and/or share the Company's Data.			
ADDITIONAL ROLES AND RESPONSIBILITIES	DATA CUSTODIAN	BUSINESS DATA STEWARD	DOMAIN STEWARD
	Subject matter expert who oversees Systems and is responsible for the security and storage of Data within Systems. Resides in technology teams.	Subject matter expert responsible for the use, meaning, and quality of Data within their oversight. They are decision makers for their respective areas. Resides in business teams.	Subject matter expert of a Data Domain responsible for how the Data is collected, created, and used in Systems. Resides in the Enterprise Data and AI Governance Office.

2.2 Data User Requirements

The following provides Data User requirements for the acceptable use of the Data in business operations, including, but not limited to:

- The Company's Data must be used only for legitimate business purposes for which it is intended, any additional business purpose must be stated in the request for access when using the established Data Access Controls Procedures in *Appendix A*.
- When collecting and storing Data, Data Users must only retain the Data that is intended for the operations of the business.
- All Data Users must ensure the accurate input and representation of the Company's Data.
- All Data Users must utilize the established Data Access Controls guidelines in *Appendix A* to request access to the Company's Data.
- Access to Restricted, Confidential, and/or Internal Data must be granted based on Data User's roles, accessed by a unique account identifying the Data User and intended only for the specified Data User.
- Internal Data sharing is permitted in accordance with the Data Classification and Handling Standard (see *Section 2.2 – Data Classification and Handling Requirements*) to properly classify Restricted, Confidential, and/or Internal Data before sharing.
- External Data sharing – When sharing Data with Third-Parties, Data Users must ensure the appropriate Third-Party contractual agreements are in place and include the acceptable use Data User requirements established in this EDM Policy.
- Data Users shall properly classify newly created Data or Data Sets using the Data Classification & Handling Standard.
- All Data Users must report any Unauthorized use, Data Loss, or disclosure that may have occurred with the Company's Data as outlined in *Section 5* below.

2.3 Data User Prohibited Use

The following explicitly outlines activities that are forbidden when using or sharing the Company's Data, including, but not limited to:

- This EDM Policy prohibits the use of Restricted, Confidential, or Internal Data, except when approved in advance through the established Data Access Controls Procedures outlined in *Appendix A*.
- Data access requests to Restricted, Confidential, or Internal Data outside a Data User's respective role will only be provisioned with a valid business justification and authorization. This procedure is outlined in the Data Access Controls Procedures in *Appendix A*.
- Data should not be altered or modified, except as required for business operational purposes.
- Unauthorized access, Unauthorized changes, or misrepresentation of the Company's Data is prohibited.
- The use of any Data for personal purposes is prohibited.
- All Data Users with access to Restricted, Confidential, and Internal Data are prohibited from sharing this Data with Third-Parties or with other Data Users who have lower access levels than they do.
- The storing of Restricted, Confidential, or Internal Data on any local or external storage device other than one(s) centrally managed by the Company.
- Data Users are prohibited from engaging in deliberate or Unauthorized destruction of the Company's Data.
- Data theft, attempting to breach, or the use of the Company's Data for insider trading are examples of Data misuse and are strictly prohibited.
- The use of Restricted, Confidential, or Internal Data not for intended business purposes, without business justification, and authorized approval is prohibited.

Violations of these Data Users prohibited use of Data activities shall result in the actions outlined in *Section 6* below.

3. Relation to Other Company Policies, Standards, and Procedures

See *Appendix A* for other Company policies, standards and procedures related to this Policy.

4. Certification

The Company may require Employees to certify that they have reviewed this Policy, received training, and are in compliance with this EDM Policy.

5. Approvals and Exceptions

Any request for exceptions to this EDM Policy must be submitted in writing to the Chief Data Officer and Chief Information Officer for review and approval.

6. Violations, Questions, and Reporting

Violations of this EDM Policy may result in disciplinary action, up to and including termination of employment. Questions regarding this Policy should be communicated to the Enterprise Data and AI Governance Office at Email: datapolicy@rccl.com.

If you have concerns or need to report a violation of this Policy, contact your supervisor, the Enterprise Data and AI Governance Office at Email: datapolicy@rccl.com, the Global Compliance and Ethics Group at Email: ethics@rccl.com, the Chief Compliance Officer at Email: compliance@rccl.com, or any of the other Compliance and Ethics contacts set forth in the Company's Code of Business Conduct and Ethics. You may also make a report through the AWARE Hotline by phone at 1-888-81-AWARE (29273) or extension **88 for shipboard Employees, or online at RCLaware.ethicspoint.com.

The Company does not tolerate any kind of retaliation for reports or complaints made in good faith. For more information, please refer to the Company's Reporting and Non-Retaliation Policy.

7. Definitions

For purposes of this EDM Policy, the following terms shall have the following meanings:

Company or RCG: Royal Caribbean Cruises Ltd. and its wholly owned subsidiaries – Royal Caribbean International, Celebrity Cruises, and Silversea Cruises.

Data: represents the quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media. Data is contained within a record.

Data Access Controls: a set of procedures and processes that grant and/or restrict Data access to a Data User.

Data Classification: the process of identifying and categorizing Data according to its sensitivity and impact level based on the Data type to prevent the risk of Data Loss, alteration, and/or harm from disclosure.

Data Domain(s): a grouping of common types of Data in an organization. For example, Product, Revenue, Medical, and Consumer are all types of Data Domains for the Company.

Data Loss: the intentional or unintentional destruction of information, caused by Data Users or processes from within or outside of the Company.

Data Privacy: the confidentiality and protection of Data.

Data Set(s): a collection of Data.

Data Usage: Data that is currently being accessed, read, updated, processed, or deleted by a Data User, System, or process.

Data User(s): user(s) who use (access, maintain, and/or analyze) and share (internally and/or externally) the Company's electronic Data residing in enterprise Systems, such as, a Data store or a database.

Employee: means any Employee of the Company, whether land or ship based.

Handling: the process of treating the Data that is gathered, archived, or disposed of in a protected and safe way during and after the completion of the analysis process based on the Data Classification level.

System(s): a set of IT or Operational Technology (OT) Systems and software used to store, process, transfer, or maintain company information or Data for a specific purpose.

Third Party(ies): a non-Employee, whether an individual or entity engaged by the Company to provide goods or services to the organization.

Unauthorized: without official written permission or approval from the Company.

7. Policy Administration and Governance

This Policy will be managed by the following roles and span of control:

Chief Executive Officer
The Chief Executive Officer is responsible for the approval of this Policy and any amendments to this Policy.

Chief Information Officer
The Chief Information Officer is responsible for overseeing and implementing this Policy and proposing any amendments to this Policy to the Chief Executive Officer. The Chief Information Officer is also responsible for approving any exceptions to this Policy.

Chief Data Officer
The Chief Data Officer is responsible for overseeing and implementing this Policy and proposing any amendments to this Policy to the Chief Information Officer. The Chief Data Officer is also responsible for reviewing any exceptions to this Policy and submitting the exceptions for approval to the Chief Information Officer.

Chief Legal and Compliance Officer
The Chief Legal and Compliance Officer is responsible for reviewing this Policy and proposing any amendments to this Policy to the Chief Data Officer.

Chief Audit and Risk Officer
The Chief Audit and Risk Officer is responsible for reviewing this Policy and proposing any amendments to this Policy to the Chief Data Officer.

Enterprise Data and AI Governance Office
The Enterprise Data and AI Governance Office is responsible for overseeing and establishing audit controls for this Policy. The Enterprise Data and AI Governance Office is also responsible for reviewing this Policy annually to determine if any amendments are appropriate and propose such amendments to the Chief Data Officer.

This Policy must be reviewed by all the parties below and approved by the Chief Executive Officer of the Company no less than once every three (3) years.

Owner: /s/ Martha Poulter Date: 4/27/2024
Chief Information Officer

Reviewed by: /s/ Moez Hassan Date: 4/30/2024
Chief Data Officer

Reviewed by: /s/ Alex Lake Date: 4/29/2024
Chief Legal and Compliance Officer

Reviewed by: /s/ Christopher Rush Date: 4/26/2024
Chief Audit and Risk Officer

Approved by: /s/ Jason Liberty Date: 5/6/2024
Chief Executive Officer

Appendix A

Company Data Policies, Standards, Procedures, and Guidelines

Document Name	Audience	Content
Data Classification and Handling Standard	All Data Users	Defines the Data Classification levels, Handling requirements, impacts, Data types, and decision workflow.
Data Access Controls Guidelines	All Data Users	Guidelines for requesting and provisioning Data access requests, including the approval process and role-based assignments for the analytics environments.
Metadata Guidelines	Technical: Data Custodian, Domain Steward	Guidelines for metadata management throughout the Data lifecycle to improve data understanding.
Data Quality Guidelines	Technical: Data Custodian, Domain Steward -------- Administrative: Business Data Stewards	Guidelines for Data quality dimensions and Critical Data Element level identifications to improve the quality of Company Data.
Data Engineering Guidelines	Technical: Data Custodian	Guidelines for Data development, tools, pipelines, and engineering practices.
Data Guidelines by Domain (Consumer, Human Resources, and Revenue Data)	Technical: Data Custodian, Domain Steward -------- Administrative: Business Data Stewards	Guidelines for setting best practices ensuring Data is accessible, consistent, usable, and protected for each of the Company's Data Domains.
Data Creation and Sharing Guidelines	All Data Users	Guidelines for Data sharing best practices ensuring data sets remain protected and shared only with permitted data access controls.
Data Domain Business Data Steward Guidelines	All Data Users	Guidelines for Data Domains and Business Data Stewards mapping.