INTRODUCTION

This Data Classification and Handling Standard ("Standard") outlines the enterprise method for classifying and handling of Royal Caribbean Group's ("RCG" or "Company") Data. Data Classification reflects the level of Data sensitivity and the impact if Confidentiality, Integrity, or Availability is compromised or unauthorized disclosure occurs.

Employees play an important role in maintaining the Confidentiality, Integrity, and Availability of the Company's Data. Therefore, it is the responsibility of each Data User as defined in the Enterprise Data Management (EDM) Policy, to abide by the Data Classification and Handling Standard to ensure the Company's Data is safeguarded to prevent unauthorized access, loss, or disclosure.

1. Standard Detail

1.1 Scope

This Data Classification and Handling Standard applies to all Employees and Data Users who use, access, maintain, handle, store, query, or analyze the Company's Data regardless of where the Data is stored, processed, or transmitted and regardless of the format.

This Standard applies to all Company Information Assets, including but not limited to Data found in Systems, applications, Corporate Mobile Devices, portable electronic devices, tools, physical documents, digital assets, and removable media.

All Data Users are responsible for applying Data controls with the Data they use and/or share internally and/or externally as prescribed in this Standard. This Standard applies to the entire Company, including shipboard and shoreside.

1.2 Purpose

The purpose of this Standard is to provide minimum requirements to classify the Company's Data based on its level of sensitivity and impact that would result by unauthorized access and/or Data Loss. The classification of Data aids in determining appropriate security controls for the protection of RCG Data.

2. Rules and Guidelines

All Data Users shall assign a Data Classification and Handling label in Company applications. With the labeling of Data, it ensures the appropriate Handling is applied to Data according to the level of Data sensitivity and impact to the organization.

The Company requires Data Users take reasonable and appropriate steps to identify and protect Data originated or owned by the Company.

2.1 Data Classification Levels, Definitions, and Impact

Data Classification also reflects the level of impact to RCG in the event of unauthorized disclosure, alteration, or destruction of Data. Impact varies for each Data Classification level, the total impact to RCG increases as Data becomes more sensitive moving from Public to Restricted.

It is important to understand the impact on RCG within each Data Classification level.

Data Users shall classify the Company's Data into one of four classification levels: Restricted, Confidential, Internal, and Public.

TABLE 1: Description of Data Classification Levels, Data Classification Definitions, and Impacts

Data Classification Level	Data Classification Definition	Impact
Restricted Data	Restricted Data is Data that a law or applicable industry standard requires the Company to protect with additional safeguards in place to secure the Data. This requires a high level of oversight and control. Public disclosure is strictly prohibited.	The unauthorized disclosure, alteration, or destruction of Data could have a significant adverse effect on the Company's competitive advantage, operations, operational assets, brand reputation, or individuals. Possible damage from unauthorized disclosure, alteration, or destruction of Data can include financial loss, damage to the Company reputation, governmental sanctions (e.g., fines and penalties), and legal action.
Confidential Data	Confidential Data is private or sensitive information for business use only and is not meant for public disclosure. This is information related to business departments. Public disclosure is strictly prohibited.	The unauthorized disclosure, alteration, or destruction of Data could seriously harm the Company's reputation and business position. This could result in a financial, reputation, and business loss along with legal ramifications for the organization.
Internal Data	Internal Data is potentially private or sensitive information for business use only and not meant for public disclosure. It consists of routine business communications and documents created and used as part of normal, day-to-day activities for the organization. Public disclosure is strictly prohibited.	The unauthorized disclosure, alteration, or destruction of Data could have a potentially adverse effect on the Company, or individuals employed by or affiliated with the organization.
Public Data	Public Data is information that may be disclosed to the public regardless of affiliation with the Company. There is no expectation of privacy restriction or Confidentiality, and it can be disclosed freely to the public. This information is already available to the public.	The disclosure, alteration, or destruction of Data has no impact on the Company, or individuals employed by or affiliated with the organization. This information is available for public consumption.

2.2 Data Classification Handling Requirements

Data Users shall adhere to the following requirements when classifying and Handling Data.

- The default Data Classification level shall be "Internal." All information is at the "Internal" Data Classification level, unless otherwise labeled or explicitly defined in this Standard.

- All Personal Data must be treated with due care and as Restricted Data in accordance with this Standard, even when some of that Personal Data is already available in the public domain. This is because Personal Data can be defined as Data by which an individual can be identified; an individual may be identified when different Data points are aggregated.

- Data Users may not change the location of the Data if the new location does not have the same level of security controls in place, unless specifically necessary to comply with foreign immigration requirements or otherwise approved under this standard. For example, Users should not export Restricted Data from a secured database to Microsoft Excel spreadsheet to email an external address. If uncertain about the level of Data controls, consult the Enterprise Data and AI Governance Office at Email: DataPolicy@rccl.com.

- Some Data may fall into more than one Data Classification level. The Data should always be classified and handled according to the highest level of Data it contains. For example: A document contains Personal Data that has Restricted and Public marketing information. This document shall be classified and handled as Restricted due to the Personal Data.

- Access Controls are defined and configured per the Access Control and Authentication Requirements Standard and the development of the software is set up per the Software Development Life Cycle (SDLC) Standard, located on Homeport.

- Encryption and Handling Requirements applies to Data at Rest (stored) and Data in Transit (in motion).

TABLE 2: Description of Data Classification Levels and Encryption and Handling Requirements

Data Classification Level	Encryption and Handling Requirements
Restricted Data	Encryption is required on removable media and Corporate Mobile Devices/laptops.
Confidential and Internal Data	Encryption is recommended on removable media, Corporate Mobile Devices, and laptops.
Public Data	No encryption required, no Access Control requirement

2.3 Data Destruction

All Information Assets and Data shall be disposed of when it is no longer necessary for business use; provided the disposal does not conflict with the applicable Records Retention Schedule of the **Record Management Policy** outlined in *Section 3*. Destruction shall be suspended immediately, upon issuance of a legal hold and shall be reinstated after receiving a release notification for the hold.

Information Technology (IT) shall be engaged to conduct electronic disposition of Systems. If disposition of Systems will be provided by a Third-Party, IT should engage Information Security (IS).

TABLE 3: Description of Data Destruction Requirements for System and Physical Data Disposal

Data Classification Level	System Disposal	Physical Data Disposal
Restricted Data and Confidential Data	At a minimum, IT to conduct a Forensic Data Wipe of 3 passes. Physical destruction recommended.	Destroy documents to the point that reconstruction is not possible.
Internal Data	At a minimum, IT to conduct a Forensic Data Wipe of 1 pass.	Destroy documents in a secure manner.
Public Data	No requirement.	No requirement.

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

The policies and standards listed below may also apply or affect the subject matter of this Standard:

- Enterprise Data Management (EDM) Policy
- Global Information Security (GIS) Policy
- Records Management Policy
  - *Records Retention Schedule*

4. Certification

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

5. Approvals and Exceptions

Any request for exceptions to this Standard 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 Standard may result in disciplinary action, up to and including termination of employment.

Questions regarding this Standard 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 Standard, 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 RCGaware.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 Company's Reporting and Non-Retaliation Policy.

7. Definitions

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

Access Controls: a security term used to refer to a set of policies for restricting access to information, tools, and physical locations. This determines who is allowed to access certain Data, applications, Systems, and resources and in what circumstances. This allows the right people in and keeps the wrong people out.

Availability: the need to ensure that the business purpose of the System can be met and that it is accessible to those who need to use it.

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

Confidentiality: the protection of Data from unauthorized access by entities and disclosures.

Corporate Mobile Devices: all Company mobile computing devices, Systems, applications, and accessories that allow the Employee to use computers, tablets, and/or smartphones to perform applicable job functions and/or tasks.

Data: 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 at Rest (Stored): Data that is stored physically on a computer Data storage in any digital form. Data at Rest includes both structured and unstructured Data. This Data has reached a destination and is not being accessed or used. It typically refers to stored Data. External portable storage devices are not considered a storage device for Data. They are to only be used when necessary to securely transfer Data when needed with proper approval and authorization.

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 loss, alteration, and/or harm from disclosure.

Data in Transit (In Motion): is digital information that is actively moving between two different computer Systems, applications, or hardware. The Data is in route between the source and target, typically on a computer network. Data in Transit can be separated into two categories: Data that flows over a public or trusted network such as the Internet, or Data that flows in the confines of a private network.

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

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.

Department Head: means the highest-level person (director or above) and decision maker for any given department.

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

Handling: the process of securing 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.

Information Asset(s): information in any form that is processed interpreted, organized, structured, or presented to make them meaningful or useful in both physical and electronic form to the organization. It includes but is not limited to Systems, applications, Corporate Mobile Devices, portable electronic devices, tools, physical documents, digital assets, and removable media.

Integrity: refers to the accuracy and consistency of Data over its entire lifecycle. This is a critical aspect of the design, implementation, and usage of any System that stores, processes, or retrieves Data.

Personal Data: any Data that could be used to identify a specific individual. This Data is private and must be safeguarded to prevent misuse or disclosure of the Data.

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.

8. Standard Administration and Governance

This Data Classification and Handling Standard shall be managed by the following roles and span of control:

Chief Information Officer

The Chief Information Officer is responsible for overseeing and implementing this Standard and approving any amendments and any exceptions to this Standard.

Chief Data Officer

The Chief Data Officer is responsible for the overseeing and implementing this Standard and reviewing and approving any exceptions of this Standard, as well as proposing any amendments to this Standard to the Chief Information Officer.

Chief Legal and Compliance Officer

The Chief Legal and Compliance Officer is responsible for review of this Standard and proposing any amendments to this Standard to the Chief Data Officer.

Chief Audit and Risk Officer

The Chief Audit and Risk Officer is responsible for review of this Standard and proposing any amendments to this Standard 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 Standard and reviewing this Standard annually to determine if any amendments are appropriate and propose such amendments to the Chief Data Officer.

Department Heads

Each Department Head is responsible for ensuring that Data Users within their department comply with this Standard.

This Standard must be reviewed by all the parties listed in this section and approved by the Chief Information Officer the Company at least once every three (3) years.

Owner: /s/ Martha Poulter Date: 4/29/2024
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

APPENDIX A

1) Pre-Defined Data Types based on Data Classification Level

Table 4 provides examples of Data Classification Levels and Data Types. It is not an exhaustive list of Data Types, but representative of Data within scope of this Standard.

TABLE 4: Examples of Data Classification Levels and Data Types

Data Classification Levels	Data Types
Restricted Data	**Personal Data and information as defined by local, state, federal, and international regulations or guidelines including but not limited to:** ○ Date of Birth ○ Personal E-mail Address ○ Telephone Numbers ○ Race/ethnicity. ○ Sexual orientation ○ Biometric e.g., security photos, fingerprints, retinal scans, etc. ○ Device IDs and Serial Numbers ○ Government Identifier numbers ○ SSN or Tax ID ○ Passport number ○ Immigration or Visa ○ National ID ○ Driver's license number • **Financial Data including but not limited to:** ○ Sarbanes-Oxley Act (SOX) financial reporting ○ Payment Card Industry Data Security Standard (PCI DSS) payment information ○ Bank Account Information ○ Pre-released SEC filings ○ Financial Forecasts • **Payment Card Industry Data Security Standard (PCI DSS) payment information including but not limited to:** ○ Account Data consists, at a minimum, of cardholder data and/or sensitive authentication data ○ Cardholder Data, at a minimum, consists of the full Primary Account Number (PAN), but may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. ○ Sensitive Authentication Data consists of security-related information used to authenticate cardholders and/or authorize payment card transactions, including, but not limited to: ○ Card validation verification codes / values ○ Full track data (from magnetic stripe or equivalent on a chip) ○ PINs ○ PIN blocks • **Health Data including but not limited to:** ○ Health and medical Data tied to any person. ○ Disability information ○ Treatment Information

TABLE 4: Examples of Data Classification Levels and Data Types

Data Classification Levels	Data Types
	• **Business Data including but not limited to:** ○ Strategic plans and mergers activities ○ Legal proceedings and investigations ○ Attorney-Client Privileged Data ○ Investigations ○ Board Reports ○ Executive Audit Report ○ Trade Secrets ○ Intellectual Property • **Authentication Data including but not limited to:** ○ Login Credentials ○ Passwords or password hashes ○ PINs and secret question/answer ○ Sensitive Authentication Data (SAD)
Confidential Data	• **Departmental Data, including but not limited to:** **Human Resources (*for example)*:** ○ Employee file ○ Compensation ○ Benefits ○ Professional Development • **Company Strategic Data, including but not limited to:** ○ Strategy Plan ○ Accounting information ○ Budgeting information ○ Forecasting information ○ Business unit plans for the development of new products that have not yet been publicly released. ○ Pricing and Costing information, including that of Company suppliers. ○ Contract negotiations. ○ Any information of a non-Company individual or party that is covered by an obligation of Confidentiality. ○ Technology documentation including but not limited to policies, standards, and guidelines related to physical and technical security and Data Governance ○ Unreleased press releases* ○ Unpublished marketing materials* ○ Contracts with Third-Party suppliers* ○ Audit reports*
Internal Data	• **Internal Data including but not limited to:** ○ Policy, Standards, Guidelines, and Procedures to include in Employee handbooks. ○ Organization charts ○ Business IP address ○ Internally used Web URL (even if the web-facing) ○ Internal memos or newsletters* ○ Project reports* ○ Meeting minutes*

TABLE 4: Examples of Data Classification Levels and Data Types

Data Classification Levels	Data Types
Public Data	• **Public Data including but not limited to:** ○ Published annual reports including SEC filings. ○ Publicly filed documents. ○ Published marketing materials. ○ Published promotional materials. ○ Published advertising materials and sales brochures. ○ Published mailings and solicitations. ○ Published press releases and announcements. ○ General contact information of the Company (e.g., business addresses, phone numbers not specific to any Employee, & business email addresses) ○ Published interviews with news media. ○ Published external job postings. ○ Published product datasheets that do not include pricing information.

** This is the minimum level at which the Data must be classified; if the information contained therein is classified as more restrictive, the document must be classified at the same level.*

2) Sensitivity Types based on Usage

Table 5 presents Data Classification levels that are labeled and used within Microsoft Office products as sensitivity types. The sensitivity types are categorized into two groups based on usage, one for all Data Users and the other one used for tool service accounts. The table below represents the sensitivity types and their description.

TABLE 5: Description of Data Sensitivity Types

A. Visible to ALL Users

Sensitivity Type	Sensitivity Description
Restricted (Encrypted)	The unauthorized disclosure, alteration, or destruction of Data could have a significant adverse effect on RCG's competitive advantage, operations, operational assets, brand reputation, or individuals. Adds encryption to documents requiring all recipients to authenticate with their email address. Forward with caution, printed documentation must be destroyed after use.
Restricted Recipients Only (Encrypted)	Restricted Data plus adds permissions to documents requiring only specified recipients to authenticate with their email address. Forwarding and/or printing is not permitted.
Confidential (Encrypted)	The unauthorized disclosure, alteration, or destruction of Data could have adverse effect on RCG's competitive advantage, operations, operational assets, brand reputation, financials, or individuals. Public disclosure is strictly prohibited. Adds encryption to documents requiring all recipients to authenticate with their email address. Printed documentation must be destroyed after use.
Internal (Default)	The unauthorized disclosure, alteration, or destruction of Data could have a potential adverse effect on RCG or individuals, especially when combined with public information. No encryption applied. Forwarding and /or printing is allowed.
Public	The disclosure, alteration, or destruction of Data would result in no adverse effect on RCG, or individuals employed by or affiliated with the company. No encryption. Forwarding and/or printing is allowed.

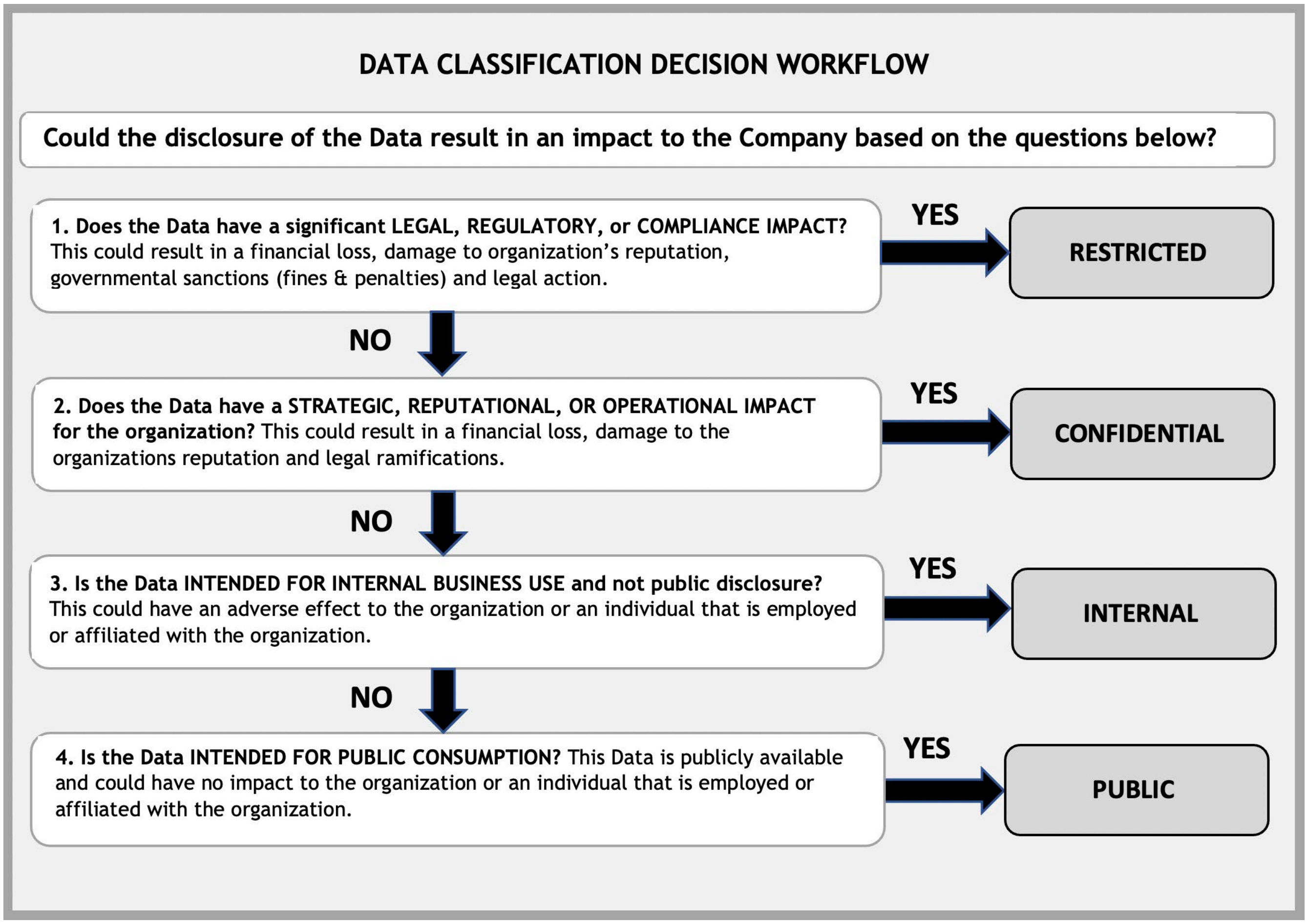
B. Visible to Tool Service Account Only

Sensitivity Type	Sensitivity Description
Restricted (Unencrypted)	The unauthorized disclosure, alteration, or destruction of Data could have a significant adverse effect on RCG's competitive advantage, operations, operational assets, brand reputation, or individuals. It requires all recipients to authenticate with their email address. Forward with caution, printed documentation must be destroyed after use. This is a Service account label for automatic classification of files. Labels can then be read by other programs if given access to enforce Data management policies. Label is only published to Data labeling service account and does not encrypt files, so it's not seen by all Data Users.
Confidential (Unencrypted)	The unauthorized disclosure, alteration, or destruction of Data could have adverse effect on RCG's competitive advantage, operations, operational assets, brand reputation, financials, or individuals. Public disclosure is strictly prohibited. It requires all recipients to authenticate with their email address. Printed documentation must be destroyed after use. This is a Service account label for automatic classification of files. Labels can then be read by other programs if given access to enforce Data management policies. Label is only published to Data labeling service account and does not encrypt files, so it's not seen by all Data Users.

APPENDIX B

Data Classification Decision Workflow

The Data Classification Decision Workflow assists Data Users with the decision-making process for selecting the appropriate Data Classification level based on the Data types referenced in *Appendix A*.



DATA CLASSIFICATION DECISION WORKFLOW

Could the disclosure of the Data result in an impact to the Company based on the questions below?

1. Does the Data have a significant LEGAL, REGULATORY, or COMPLIANCE IMPACT? This could result in a financial loss, damage to organization’s reputation, governmental sanctions (fines & penalties) and legal action.

2. Does the Data have a STRATEGIC, REPUTATIONAL, OR OPERATIONAL IMPACT for the organization? This could result in a financial loss, damage to the organizations reputation and legal ramifications.

3. Is the Data INTENDED FOR INTERNAL BUSINESS USE and not public disclosure? This could have an adverse effect to the organization or an individual that is employed or affiliated with the organization.

4. Is the Data INTENDED FOR PUBLIC CONSUMPTION? This Data is publicly available and could have no impact to the organization or an individual that is employed or affiliated with the organization.