QUADRANT RESOURCES Pvt.Ltd.
ACHIEVE MORE TOGETHER

Data Classification Policy

Version 1.0

Revision History

Version #	Date (DD-MMM-YYYY)	Details of the Changes	Modified By	Reviewed & Approved By
1.0	1 July 2020	First Release	Barkha Jain	Shahed Akhter
1.0	10 Oct 2021	Reviewed No Changes Made	Barkha Jain	Shahed Akhter
1.0	5 Oct 2022	Reviewed No Changes Made	Barkha Jain	Shahed Akhter
1.0	5 July 2023	Reviewed No Changes Made	Barkha Jain	Shahed Akhter
1.0	19 Jun 2024	Reviewed No Changes Made	Barkha Jain	Shahed Akhter

Contents

1 Introduction

1.1 Overview

- The Data Classification policy provides Quadrant with a method to categorize the information collected, stored, and managed by the company.
- Using the data classification method will improve the ability of the company to properly manage access to company information in compliance with federal and state laws and regulations, and other company policy requirements.

1.2 Scope

This policy applies to:

- All persons or entities that have access to company data, and are employees, agents or contractors of Quadrant.
- Electronic and non-electronic representations of data utilized by the company for the purpose of carrying out its mission and data used in the execution of required business functions, limited by any overriding contractual or statutory regulations.

2 Information Classification

- Data stewards shall classify information according to the impact resulting from loss or unauthorized exposure as per the standards defined in the Information Classification Scheme.
- Data custodians and data users shall inform data stewards of any data that requires classification. Quadrant/client data stored electronically on company or non-company resources must be verifiably protected according to the Minimum Security Standards for Protected data.
- Data stewards, data custodians and data users shall ensure data is protected according to the classification assigned as prescribed in the Minimum Security Standards for Protected data.
- The classification of each information asset should be reviewed at least once a year by Asset Owner in cooperation with Information Security Team.

2.1 Information Classification Scheme

- When information of various classifications is combined, the resulting collection of information or new information should be classified at the most restrictive level among the sources.
- Subsets of data shall have the same classification level and utilize the same protective measures as the original data in the system of record.
- Data must be consistently protected throughout its life cycle in a manner commensurate with its sensitivity, regardless of where it resides or what purpose(s) it serves.

All the Quadrant information should be classified based on the following Classification Scheme:

- Data are classified in four categories depending on sensitivity and importance.

Information Classification Scheme According to Confidentiality	
Classification	**Description**
STRICTLY CONFIDENTIAL	This classification applies to extremely sensitive organizational information which is intended for use within the Company, protected by applicable law, statute or company policy, or which, if disclosed to the public could expose the company to legal or financial obligations. The unauthorized disclosure of such information can have serious adverse effects on the Company, the shareholders, employees, business partners and/or clients. This can result in immediate economic loss or have negative consequences on the Company market share. Examples of such information would be information about new products, business secrets, financial results that have not been published, management communication, driver's license number, export controlled information under U.S laws, authentication credentials or identify verification information etc.
CONFIDENTIAL	This classification applies to sensitive organizational information which is intended for use within the Company. Client data, and data that are protected by law have been classified as Confidential information. It also includes information that would otherwise be classified as "Strictly Confidential", but it has been determined that handling and storing of this data using standards for "Strictly Confidential" would significantly reduce effectiveness when acting in support of the company's mission. The unauthorized disclosure of this information can have as an immediate impact the loss of good faith or indirect financial loss. Examples of such information are personnel evaluation reports, short-term strategic plans, internal audit reports, personal data, client data, ID Card photographs, Shipment information etc.
INTERNAL USE	This classification refers to information that is to be used internally by the Company personnel only, and does not fall into the other categories. This information is not intended for public dissemination, but its disclosure is not restricted by federal or state law. It also includes information that would otherwise be classified as "Confidential", but it has been determined that handling and storing of this data using standards for "Confidential" would significantly reduce effectiveness when acting in support of the company's mission. Although unauthorized disclosure of this information is prohibited,
Information Classification Scheme According to Confidentiality	

Classification	Description
	in the case that it occurs, it is expected that there will not be any serious repercussions to the Company, shareholders, employees, business partners and/or clients. Examples of such information are internal training materials and manuals, internal communication documents, corporate policies, procedures, research data (electronic & physical), privileged communications etc.
PUBLIC	This classification applies to information which has been explicitly approved by the Company management for release to the public. This information is not restricted by local, state, national or international statute regarding disclosure or use. By definition, there is no threat by the disclosure of this information and can be freely circulated without any potential impact. Examples of such information are public leaflets, advertisements, press releases, directory information, approved information etc.

2.2 Guidance on Information Classification

If the appropriate classification is not prescribed in this document, the Data Steward shall consider each security objective and may use the following table as a guide. It is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

Security Objective	LIMITED IMPACT	SERIOUS IMPACT	SEVERE IMPACT
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational

repudiation and authenticity.	organizational assets, or individuals.	organizational assets, or individuals.	operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

As the potential impact to the company increases, data should be more restrictively classified, moving from Public to Strictly Confidential. Typically data involving severe or Catastrophic impact would be classified as Restricted.

2.3 Labelling of Information

- The Data Steward shall be responsible for labelling the asset, where applicable, and maintaining the asset record. The label shall be in accordance with the approved Company naming convention.
- All IT documents, hardware items and removable media physical labelling shall include appropriate security classifications in accordance with the Quadrant Asset Classification Scheme.
- All IT hard copy information should be labelled. The labelling can be done in a footer or header of a document.
- All IT hardcopy information that is classified as “Confidential” or “Strictly Confidential” must be conspicuously labelled as such.
- All pages of each labelled document must be numbered according to a reasonable scheme, i.e., ‘x of y’ (page 1 of 25) or sequential order (1, 2, 3 …) so that missing pages can readily be discovered.
- Photographs of a sensitive nature should be labelled and numbered on the reverse side.
- Some information in electronic form, data residing in a database, information displayed on intranet or Web page, etc., cannot be physically labelled and electronic means of labelling must be used instead. Examples are:
    - A watermark displaying “Confidential” in background of an intranet or Web page.
    - A notice or warning statement that displays before accessing data in a database.
    - Mark e-mail as “Confidential” using the built-in function of the e-mail client and displaying the label at the top of the message.

2.4 Information Handling Guidelines

- All the information stored on or transmitted over the organization's resources remains the organization's property and the organization has the right to monitor and audit that information.
- All organization's confidential information should be treated in strict confidence. Copying or transmitting the information is strictly prohibited except when required for organization business.
- All sensitive or "Confidential" information stored on a laptop should be password protected.
- Information classified as Confidential or Strictly Confidential should not be printed on a Networked Printer. In case of any such requirement, care should be taken not to lose the confidentiality of the information.
- All information classified as Confidential or Strictly Confidential should be printed only the required number of copies and all copies should be followed up for proper usage and when not required should be destroyed. Photocopying of these pages should be handled and done only by owners of the information.
- Individuals should access all business information based on NEED TO KNOW principle only. Provision / Feasibility to access an information / resource should not be construed to be eligibility for accessing the information.
- Employees should not discuss confidential information in public viz. inside Lifts, Airport Lounges, and Hotel Reception etc… Care should be exercised when using Mobile Phones in public areas. Employees using Laptops should ensure that information on the screen is not visible to others.
- Paper documents, when disposed, should be shredded to pieces using shredders.

2.5 User Do's and Don'ts

- Access to Classified data is denied unless the user has obtained explicit approval from the data owner.
- Declassification clause: Classification shall be reviewed on a quarterly basis to define the assets which can be declassified.
- Access to data classified as Strictly Confidential and Confidential should be based on legal requirements or on a need to know and job role.
- Access to data is given to authorized users. This access should not be shared, transferred or delegated (e.g., authorized users should not log on, access data and then let others use that data).
- Authorized users act in a manner which will ensure the data they are authorized to access is protected from unauthorized access, unauthorized use, invalid changes, destruction, or improper dissemination.
- Users are prohibited from viewing or accessing data, in any medium and/or form, for which they are not approved.
- Classified data shall not be copied without prior approval.

- While disposing-off data, it is to be ensured that the process is consistent with the classification of the information.

2.6 Review of Classified Data

- A regular audit of the classified data (once in 6 months) and applied security controls should be conducted. The output of the review will act as inputs to Declassification / Downgrading procedure described here below.

2.7 Reclassification / Downgrading

- The designated information owner may, at any time, Reclassify / Declassify or Downgrade Physical / Non-physical Assets. To achieve this, the owner must change the classification label appearing on the physical asset / original document.
- Declassification / Downgrading of Physical / Information Assets may happen because of the following factors:
    - Physical assets have been removed from production / not working / became obsolete / replaced etc.
    - Non-physical assets have been released to the public like annual reports / project is complete / confidentiality period of data / reports has expired.

I acknowledge receipt of the above Data Classification Policy, and I confirm that I have read and understood the same and am in agreement with the terms and conditions contained herein.

Date: _____

Employee Name: _____

Employee Signature: _____