RIDGE

INFORMATION CLASSIFICATION AND HANDLING POLICY

CONTENTS

1. DOCUMENT CONTROL

1.1. Distribution

This document, once issued, becomes a live document and, subject to updates and changes, shall be maintained as a configuration-controlled item. Any subsequent amendments must be submitted to the Systems Manager and controlled using document versioning.

DISTRIBUTION
All internal staff
Relevant external parties

1.2. Version Control

VERSION	DATE	DESCRIPTION	CREATED BY	REVIEWED BY
1.0	27.11.2021	Creation	LS	DW
1.1	24.01.2022	Review	LE	DW

1.3. Applicable Documents

DOCUMENT TITLE	DOCUMENT LOCATION

1.4. Definitions and Abbreviations

ACRONYM	DEFINITION

2. INTRODUCTION

Ridge's assets vary in their sensitivity and their criticality. It is important that there is a system to classify these assets and to lay out how these assets should be handled, this ensures that these assets are adequately protected both in transit and at rest.

This policy aims to lay out Ridge's information classification system, as well as rules around handling assets of various classifications.

2.1. Scope

This policy applies to all information assets generated or processed by Ridge, including those created prior to the publishing of this policy. This includes electronic information as well as information on paper and information shared orally or visually (such as telephone and video conferencing). Where the organisation holds information on behalf of another organisation with its own classification system, an agreement shall be reached as to which handling policy shall apply.

2.2. Responsibilities

- The Equity Partners within Ridge have ultimate responsibility for ensuring compliance with this policy.
- Information Asset Owners have the responsibility of implementing this policy with regards to the assets they own.
- All staff shall adhere to this policy and handle information assets according to their classification.

3. INFORMATION

3.1 All Information assets shall be assigned one of four levels of classification, as defined below:

Level	Description	Examples
Public	Information which is authorised to exist on the public domain. This information would cause no discernible harm if compromised	• Published company brochures • Published annual reports • Published marketing materials
Internal	Information which should only be accessible within Ridge unless authorisation to share externally has been obtained. This information would cause little to no harm if compromised.	• Internal policy documents • Organisational structure charts • Staff manuals • Day-to-day announcements
Confidential	Information that should only be available to select groups. This information could cause moderate operational, financial, or reputational damage if compromised	• Data about current, potential, or ex-customers or employees. • Internal or external audit reports. • Operating procedures for sensitive functions (Finance, HR, etc.) • 3rd party contracts. • Operational data, logs or reports. • Data which could provide a competitive advantage.

Restricted	Information that should only be made available to named individuals. This information would cause significant operational, financial, or reputational damage if compromised	• Data used in the control of security systems (passwords, encryption keys etc.) • Personal data of employees, customers or third parties. • Financial records. • Data restricted to company Execs.
Customer – Classification	In some situations, Ridge may be required to comply with a customer's classification scheme. In this situation a document should be labelled with the customer's name and the classification that the customer has assigned to it. Format: Customer name – Classification	This is situation is handled on a case-by-case basis.

Table 1 – Information classification scheme

3.2 All information and information assets shall be assigned an owner.

3.3 All Information and information assets shall be assigned an owner. All information asset owners are responsible for assigning their asset a classification level according to Table 1.

3.4 Information assets should be made available to all who have a legitimate need to access them.

3.5 The confidentiality of information must be maintained in line with the classification scheme.

3.6 The integrity of information must be maintained such that the information is accurate and fit for the purpose it was acquired or created.

3.7 In cases where customers are working to their own information classification scheme, Ridge may be required to handle customer information according to that classification scheme. This should be agreed with the customer as part a of project's initiation.

4. LABELLING

4.1 All documentation of a classification internal or higher must be labelled.

4.2 Documents should be labelled as below:

- Digital documentation should have its classification level identified in the footer, in line with Appendix 1.
- Documents that are not labelled must only be stored in a repository of the correct classification. This point extends to lockable cabinets for paper information.

4.3 Other information assets should be labelled on the information asset register.

5. DATA HANDLING

5.1 Data must only be handled by persons with appropriate authorisation or a valid business reason to do so.

5.2 For the specific requirements around handling data of each classification level, see Appendix 1.

5.3 Any storage and portable media must be handled in a way which is compliant with guidance on the highest classification information, which is stored within it, unless there is authorisation to do otherwise.

5.4 In the case where data is to be shared to and from an external organisation, or third party, an agreement must be put in place which addresses each of the requirements found in Appendix 1.

5.5 When sensitive and confidential documents are circulated, and not live, they should be shared in read only formats.

5.6 Where information does need to be shared and an agreement or authorisation to do so has been obtained, this should be done on a need-to-know basis and with named individuals.

6. INFORMATION TRANSFER

6.1 Information/Data must be transferred in line with the guidance laid out in appendix 1.

6.2 Information with a sensitivity higher than "Public" must only be shared with third parties once a data sharing agreement and NDA (if necessary) has been obtained either separately or as part of a contract.

6.3 Where possible, data should be hosted on Ridge systems to which third parties have access. As a general principal data/information should only be copied and transferred if it is necessary.

Appendix 1 – Data Handling Guidance

Below are requirements for data in a printed/paper format. Any exceptions to the guidance stated below must be approved by the Asset owner				
Usage	**Restricted**	**Confidential**	**Internal**	**Public**
Labelling	Each page to be marked as "Sensitive"	Each page to be marked as "Confidential"	None	Each page to be marked as "Public"
Storage	Must be stored within a locked storage unit, housed within a locked office.	Must be stored within a locked storage unit. Within an office or secure location.	Must be stored in an office or secure location.	None
Transportation	To be hand delivered and stored out of sight in transit, when carried by a Ridge employee. If mailed, must be transported by an approved courier, and marked "To be opened by the addressee only".	Must be within the possession of a Ridge and stored out of sight during transit. If mailed, can be sent via normal postal services, and must be marked "To be opened by the addressee only".	Must be within the possession of a Ridge Employee and stored out of sight during transit. If mailed, can be sent via normal postal services.	None
Disposal	Must be disposed of securely in confidential waste bins or be shredded by a cross-cut shredder. If third parties dispose of this information certificates of destruction must be obtained from them.	Must be disposed of securely in confidential waste bins or be shredded by a cross-cut shredder. If third parties dispose of this information certificates of destruction must be obtained from them.	Must be disposed of securely in confidential waste bins or be shredded by a cross-cut shredder.	None

Below are requirements for data in an electronic format. Any exceptions to the guidance stated below must be approved by the Asset owner:				
Usage	**Restricted**	**Confidential**	**Internal**	**Public**
Document Labelling	Must be marked "Sensitive" in the footer	Must be marked "Confidential" in the footer	None	Must be marked "Public" in the footer
Email	The email must be encrypted or contain the data in an encrypted form. E.g. a password protected zip file	The email must be encrypted or contain the data in an encrypted form. E.g. a password protected zip file	The data must only be sent to internal email addresses or approved 3rd parties.	None
Storage	The data must be protected via password or through AD defined permissions. Preferably on a encrypted network drive.	The data must be protected via password or through AD defined permissions	The data must be protected via password or through AD defined permissions	None
Removeable media	The media must be Hardware encrypted, and the data deleted when no longer required.	The media must be encrypted, and the data deleted when no longer required.	The media must be encrypted, and the data deleted when no longer required.	None
Mobiles	Sensitive data is not to be stored on mobiles.	The mobile phone must be PIN or protected.	The mobile phone must be PIN protected.	None
Laptops	The laptop storing data must have an encrypted hard disk.	The laptop storing data must have an encrypted hard disk.	The laptop storing data must have an encrypted hard disk.	None
Transfer				None
Disposal	Ensure that no sensitive data remains within the recycle bin after deletion. Physical hard drives must be returned to the IT for secure wipe or disposal. A record of destruction must be retained.	Ensure that no sensitive data remains within the recycle bin after deletion. Physical hard drives must be returned to the IT for secure wipe or disposal. A record of destruction must be retained.	Ensure that no sensitive data remains within the recycle bin after deletion. Physical hard drives must be returned to the IT for secure wipe or disposal. A record of destruction must be retained.	None