# Information Classification Policy

## Contents

## Introduction

Clarus Financial Technology understands the importance of information security to its customers as well as its own business, and is committed to protecting information under its custody from unauthorized access and dissemination at all times. The following information classification policy has been developed to help fulfil this commitment.

## Scope

This policy applies to all data and information assets under the custody of Clarus Financial Technology, including information received from customers or third parties, and generated in-house. It has been approved by senior management and all employees are expected and required to follow the policies and guidelines laid out herein.

## Classification Categories

Information is broadly classified as **Private** or **Public**. Information that must be accessible only to specific Clarus customers and/or employees, where unauthorized access or disclosure can have serious consequences to Clarus or its customers, should be classified as Private. Any other information should be classified as Public. All private data must be subject to strict controls with respect to their storage, transmission, and access.

Information is further subcategorized as follows:

- Private - Client Confidential
- Private - Company Confidential
- Public - Business Use Only
- Public - Unrestricted

## Classification Guidelines

For each information asset an Owner will be identified. This individual will be responsible for classifying the asset according to the guidelines below, verifying that the required level of protection and access controls have been applied, and ensuring it is disposed of securely when no longer needed.

Private - Client confidential

- All data uploaded by customers to Clarus systems, or fetched from customer systems
- All data fetched from third parties by Clarus systems on behalf of individual customers
- Any information sent by customers to Clarus via email or other methods

Private - Company confidential

- All cryptographic keys, passwords etc that control access to or ensure integrity of internal systems
- All cryptographic keys, passwords etc that control access to third party systems (hosting systems, payment processing etc)
- All company developed source code, algorithms, architecture diagrams, system images
- Any documents pertaining to Clarus business and operating procedures that is classified as "company confidential" by management or owner

Public - Business Use Only

- Any data fetched from third parties by Clarus systems not on behalf of, and not containing data specific to, individual clients (e.g. market data)
- Any documents pertaining to Clarus business and operating procedures that is not classified as "company confidential" by management or owner

Public - Unrestricted

- Any data or documentation produced by Clarus for public dissemination with prior management approval (e.g. blogs)

## Information Handling Guidelines

The following guidelines must be adhered to when handling information classified under each category.

| | Classification Category | | | |
|---|---|---|---|---|
| | Private - Client Confidential | Private - Company Confidential | Public - Business Use Only | Public - Unrestricted |
| Storage on Clarus systems | Not stored (in memory processing only), or encrypted using approved methods, preferably using client specific keys | Encrypted using approved methods | Encrypted where possible | No specific requirements |
| Storage on removable media (incl laptops) | Encrypted on disk, with encryption keys protected by a strong password | Encrypted on disk, with encryption keys protected by a strong password | Encrypted on disk where possible | No specific requirements |
| Transmission | Encrypted transmission with controlled access (e.g. protected behind a login) | Encrypted transmission with controlled access (e.g. protected behind a login) | Encrypted transmission with controlled access (e.g. protected behind a login) | No specific requirements |

| | | | | |
|---|---|---|---|---|
| Access - customer | Access granted only to specific customer, not shared with other customers | May be shared with customers subject to license and confidentiality agreements (Excluding passwords and cryptographic keys) | May be shared with customers subject to license agreements | No specific requirements |
| Access - Clarus employees | Strictly controlled and granted only when necessary to fulfil their duties | Strictly controlled and granted only when necessary to fulfil their duties | Read-only access generally granted without restrictions. Write access granted only when necessary to fulfil their duties | Read-only access generally granted without restrictions. Write access granted only when necessary to fulfil their duties |
| Destruction | Destruction by secure deletion of data and/or encryption keys | Destruction by secure deletion of data and/or encryption keys | Destruction by deletion of data | Destruction by deletion of data |