Information Security Policy

Contents

Introduction

Clarus Financial Technology understands the importance of information, and processes and systems used to process, store and access that information. Unauthorized access to, or lack of availability of, information can have serious consequences to both Clarus and its customers.

The senior management of the company is therefore committed to preserving the confidentiality, availability and integrity of information and resources under its custody at all times. This document established the processes and practices that will enable Clarus to meet its Information Security objectives.

Objectives

All data and information assets under the custody of Clarus Financial Technology, including information received from customers or third parties, and generated in-house, are of vital importance and must be protected at all times. The objective of information security management within the company is to protect and preserve the confidentiality, integrity, and availability of this data, defined as follows:

- Confidentiality – ensure that information and systems used to process information is protected from unauthorized access
- Integrity – ensure that information and systems used to process information are free from unauthorized modifications
- Availability – ensure that information and systems used to process information are available to authorized parties when required

Scope

This policy applies to all Clarus Financial Technology employees and external consultants or contractors who will be accessing or in any way come into contact with information and systems used by Clarus Financial Technology to conduct its operations.

Roles and Responsibilities

All Clarus employees have a shared responsibility to protect resources to which they have access. The following responsibilities will be allocated to individuals depending on the role they play in the information security management process. An individual employee may hold more than one role.

- Senior Management – Set the overall vision and direction of information security initiatives within the company; regularly review the Information Security Policy and supporting policies; ensure that Owners (see below) are identified and assigned for each information asset or asset category
- Information Security Officer – Develop and maintain the Information Security Policy and supporting policies and communicate these to employees; develop and evaluate processes, controls and technologies to secure information and systems; act as main point of contact for security incidents
- Information and System Owners – Classify information assets according to Information Classification Guidelines; determine the required level of protection and access controls and verify these have been applied; control changes to information; ensure information is disposed of securely when no longer needed.
- Administrators – Apply and implement controls and processes to secure information and systems as specified by their owners; ensure appropriate backup and recovery processes are in place for all critical information and system; report any suspected or actual information security incidents to the Information Security Officer
- Information Users – Understand and comply with the requirements of the Information Security Policy and supporting policies; report any suspected or actual information security incidents to the Information Security Officer

Administrators will be classified according to the type of system they are responsible for (Amazon Web Services, Linux Systems, Databases, Network). Users will be subdivided according to the role they play within the organisation (e.g. development, support, sales) in order to ease administration of access controls and policies. See the Access Control Policy for details.

Information Ownership and Classification

Senior Management will ensure that each information asset or category of asset handled by the company has an Owner assigned. The Owner has primary responsibility for securing the information assets under their care. The Owner should assign one of the following classification categories to each asset based on the level of protection required:

1. Private – Client Confidential
2. Private – Company Confidential
3. Public – Business Use Only
4. Public – Unrestricted

For guidance on how classification categories should be assigned and how classified information should be handled, see the Information Classification Policy

Access Control

Controls must be in place to ensure that only those employees who have a business need to have access to information assets and systems are permitted to do so, and that such employees are assigned the least level of access privileges that allows them to carry out their duties. Refer to the CHARM Access Control Policy document for details.

Network Security

Network Administrators must ensure that networked resources are protected against unauthorized access and attack. Attack surfaces must be reduced by limiting exposure to untrusted networks (including the public internet) as much as possible. In particular, administrative access to servers should only be permitted from known IP addresses. Suspicious access patterns such as repeated login failures should be monitored, and Network Administrators should take preventative measures such as IP bans if a credible threat is detected. Further details of how network security should be implemented can be found in the CHARM Network Security Architecture document.

Operational Security

Administrators must develop and implement a backup policy which ensures regular backups are taken of all critical systems and information. The recovery process for each type of backup must be regularly tested.

Administrators must ensure security patches are applied in a timely manner to systems under their care.

All users who electronically access any protected information asset or system must ensure up to date anti-virus and anti-malware protection is installed on their equipment, and that all latest security patches are installed.

No software changes will be deployed on production systems before going through the internal software development lifecycle in full, and where appropriate, user acceptance testing.

Any software or configuration change required for production systems must be approved by the system owner. Only Administrators shall be permitted to make such changes, which must be thoroughly tested before being applied to production systems. Backups must be in place in case configuration changes lead to unexpected behaviour.

Cryptography and Encryption

All systems should have Full Disk Encryption (FDE) enabled whenever feasible. In addition to FDE all information assets stored on the system should have an additional layer of encryption applied according to the Information Classification Policy, for example at the database, file system, or application level.

Cryptographic keys must be protected using appropriate measures. Keys should be rotated periodically, for example once a year.

Incident Management

When an information system administrator or user has reason to suspect a data breach has occurred, the Information Security Officer must be informed immediately. Administrators should also take steps to limit the breach, for example by isolating compromised servers from the network. The Information Security Officer should investigate the report, and if a breach is considered likely to have occurred, work with senior management to take appropriate action.

Where the suspected breach involves sensitive customer data, senior management should ensure that the affected customers are fully informed of the nature and likely scope of the breach.

Supporting Documents

- Information Classification Policy
- CHARM Access Control Policy
- CHARM Network Security Architecture