2 Introduction

Protection of Customer Information is vital to the success and integrity of our Business. Graphical Financial Analysis Limited (also referred to as GFA in this document), is committed to protecting the confidentiality of our Customer Information. To achieve this goal, the company has implemented an Information Security Management System in accordance with ISO/IEC 27001:2013. GFA will also utilise a Personal Information Management System (PIMS) to comply with (EU) GDPR 2016/679 and the Irish Data Protection Acts 1998 to 2018.

2.1 What are GFA's Objectives of the ISMS?

The ISMS is designed to reflect our key business objectives. This includes:

- Provide Client confidence that all Client data is appropriately protected.
- Zero data breaches of Client or Company data.
- Compliance with all relevant laws & regulations.
- Optimum IT security awareness across the company.
- Implement effective IT security incident response procedures.

Our seven key security and privacy objectives are aligned with our key business objectives, and to our security and privacy strategy. The achievement of these key security and privacy objectives assists with the achievement of our overall business objectives at GFA.

2.1.1 Security and Privacy Organisation:

GFA shall ensure an appropriate security and privacy governance structure including a Head of Compliance, a Head of Operations, a trusted third party security provider, information asset owners, board-level oversight, and oversight of service providers.

2.1.2 Culture and awareness:

GFA shall establish and embrace a security and data privacy culture aligned with the organisation's risk and a security and data privacy training program backed by processes and incentives along with continuous improvement to ensure global best practices.

2.1.3 Risk Management:

GFA shall assess security and privacy risk to enable informed business decisions. This includes a set of security and privacy policies and procedures that support risk management; an understanding of organisational security and privacy risks; methods to assess threats, vulnerabilities and impacts; the implementation of controls to mitigate risk; and an assurance process to monitor and manage risk.

2.1.4 Handling of Personally Identifiable Information:

GFA shall ensure all staff are well trained to handle Personally Identifiable Information (PII) appropriately, establish mechanisms to classify and protect PII, and ensure adequate controls are in place to respect and protect PII. This assists with the avoidance of regulatory problems and the enhancement of customer experience.

2.1.5 Technology and Services Management:

GFA shall identify any technology or services that are part of the critical infrastructure and appropriately manage risk. Security and privacy controls shall be selected and implemented based on a risk-based process. The controls shall be kept current, managed, protect against malicious behaviour and ensure the technology is resistant to disruption.

2.1.6 Physical Security:

GFA shall implement appropriate physical security measures that protect the working environment. These measures shall include the implementation of defence in-depth design to protect against unauthorised access, and substantial controls for physical sites housing critical infrastructure.

2.1.7 Incident Response:

GFA shall implement procedures to appropriately handle security and privacy incidents and reduce damage to sensitive assets and critical information systems. These procedures shall cover business arrangements to maintain key business services, the method for risk and vulnerability assessments, plans to be followed in the event of specific threats, management structures enacted during incidents and disasters and reporting mechanisms to appropriate parties.

2.2 What is required of the ISMS

We will ensure adherence by creating and maintaining an Information Security Management System (ISMS) appropriate to our business. The ISMS includes the requirement to:

- Conduct ongoing risk assessments to identify key areas of risk to customer data and the controls required to mitigate these risks to acceptable levels.
- Provide a Data Classifications and Handling Policy.
- Engage and take part in an Information Security Forum to take ownership and provide leadership.
- Create and assign a set of roles and responsibilities for Information Security, including information asset owners

2.3 Who is responsible for Information Security?

Information Security is the responsibility of all GFA employees and contractors with access to customer information. We are obliged to take breaches of policy seriously and it is incumbent upon all of us to read and understand the security policies that apply to us in performing our duties. Violation of the policies may result in disciplinary action for employees and, in the case of others engaged in GFA, may result in legal redress.

3. Management Commitment to Security

Senior management have reviewed the Information Security Policy and endorse its use across all GFA Information Systems and within the day to day operations.

Senior management has made a commitment to ensure that all security controls and policies put in place align with the overall goals of GFA and are committed to the continual improvement of the information security management system. Coordination of these goals will be achieved through direct assistance with all stakeholders.

3.1 Compliance

Senior Management will employ multiple methods, tools, and audit processes to monitor and assess whether security controls and measures have been implemented and are being followed.

GFA expects all employees, temporary, consultants and contractors, business partners, vendors, suppliers, outsource service providers, to adhere to and support Its Information Security Policy.

3.2 Policy Definition Approval and Review Process

It is the responsibility of GFA's management team to enforce, create and review all security policies including this Information Security Policy. All policies are approved and signed by GFA senior leadership.

This policy will be reviewed annually or if significant changes occur, to ensure its continued adequacy and effectiveness.

4. Regulatory, Legal and Industry Requirements

The principle regulatory, legal and industry privacy and security requirements are listed below:

- GDPR (EU) 2016/679

This Information Security Statement is based on ISO/IEC family of standards, and particularly:

- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management system requirements;
- ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security management;

5. Information Security Principles

5.1 Who is responsible for Information Security?

Information Security is the responsibility of all GFA employees and contractors with access to customer information. GFA are obliged to take breaches of policy seriously and it is imperative that we read and understand the security policies that apply to us in performing our duties. Violation of the policies may result in disciplinary action for employees and, in the case of others engaged in GFA, may result in legal redress.

5.2 Information Security Overview

Information security is defined as the set of measures (rules, methods, control, instruments, principles) and operational processes that provide an appropriate level of protection of critical information and systems (the “Assets”) throughout their entire life cycle.

Within the context of information security:

- Confidentiality refers to the ability to ensure that the information is not made available or disclosed to unauthorized entities (individuals and processes).
- Integrity refers to the protection of the accuracy and completeness of information.
- Availability refers to the accessibility and usability of information when an authorized entity demands access.

GFA considers ‘*accountability*’ as a key concept for information security. To make an entity accountable means to assign actions and decisions to that entity and to expect that entity to be answerable for those actions and decisions. Therefore, accountability is the state of being responsible for the actions and decisions that have been assigned.

Measures and processes in place for the management of information security are intended to:

- Ensure the confidentiality, integrity and availability of data and information related to interactions with customers;
- Ensure the confidentiality of personal data relating to customers, particularly according to the current legislation regarding the protection of personal data;
- Ensure the confidentiality, integrity and availability of critical information to ensure the development and competitiveness of the business;
- Ensure the confidentiality of information relating to source code, patents and trade secrets for the products and the company services;
- Ensure the availability of its services and electronic channels for the delivery of products and services to customers;
- Ensure the integrity and availability of institutional information used for communications and corporate image.

5.3 General Principles

This Information Security Statement defines a set of general security principles that help to ensure an appropriate level of protection of GFA’s business operations:

- "Regulatory compliance": ensure compliance with national and international laws, regulations and standards applicable to the company context and with internal company rules and codes of conduct;
- "Risk-based implementation": adapting the strength and effectiveness of security measures in relation to the applicable threats, vulnerabilities and risks and prioritize the treatment decision based on real risk severity;
- "Cooperation with Public Authorities": support the judicial authorities and the Institution in the prosecution and resolution of criminal acts committed against or by the resources of GFA;

- "Segregation of duties": select organizational processes that guarantee the absence of conflicts of interest between security objectives and other interests;
- “Least Privilege”: isolate information resources based on the user’s need to have access to that resources in order to perform their job but no more;
- "Control" shall ensure the monitoring and continuous improvement of the security measures in relation to the evolution of the business and technological environment;
- "Proportionality": the implementation of security measures is suited according to the company context and available resources.

The actions arising from those principles, in particular, should be aimed at:

- Ensuring appropriate supervision and reporting in relation to breaches of information security (past or current);
- Ensuring adequate information security training and awareness to company staff;
- Pursuing the continuous improvement processes and updating of the technological solutions adapted to the evolution of threats;
- Deploying security measures on different levels, in line with the “defence-in-depth” information assurance strategy;
- Ensuring the implementation of any security check including the procedures and mechanisms to verify the effectiveness and proper implementation in the long period.

6. Information Security Management System (ISMS)

The GFA Information Security Management System (ISMS) applies to everyone working within and for GFA. The purpose of this policy-set is to communicate standards of care to ensure consistent and appropriate protection of information throughout GFA, and to meet the key business, legislative, and regulative requirements.

The overall approach for the Information Security Management (ISMS) is based on an iterative four-step management method (Plan -> Do -> Check -> Act), that is used as a reference by each process, to ensure control and continual improvement of processes and products.

The main processes defined and implemented by GFA for adequately managing the information security can be summarised as below described.

6.1 Risk Management

The Risk Management process aims to promptly identify, evaluate and treat any potential risk that could affect the business and assets of the Company.

In order to guarantee an effective Risk Management process, GFA performs the following activities:

- Definition of Risk Management process, procedures and methodology that are suitable to the Company context and business needs, within the applicable laws and regulations;
- Identification of the most critical assets within the business context;
- Evaluation of the likelihood and business impact upon the organisation that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets;
- Estimation and evaluation of the risk level, in respect of the risk acceptance and tolerance criteria;
- Definition of an adequate risk treatment plan and continuous monitoring of the related execution;
- Improvement of the Risk Management process, procedures and methodology in order to guarantee better effectiveness and efficiency.
- Reviews of the ISMS are performed annually or after significant changes to the environment

6.2 ISMS Security Policies Management

GFA intends the Information Security Policy as the overall general statement to establish security requirements compatible with the business objectives and applicable laws, regulations.

In order to support that Policy, an Information Security Management System [ISMS] has been defined in order to satisfy the company needs in terms of operational activities. Security policies, procedures, standards and guidelines must be developed and implemented that includes the following main activities:

- Definition of the applicable context and specific purpose and audience of the security policies;
- Drafting, review and approval of security policies, procedures and guidelines;
- Communication of the security policies and procedures within the organisation and to the interested/involved third parties;
- Implementation of the security policies and procedures within the organisation;
- Continuous monitoring for verifying adequate implementations;
- Periodic review for evaluating the effectiveness of the security policies and apply any potential improvement.

6.3 Training and Awareness

GFA promotes an information security training and awareness program, to increase staff information security awareness and to empower staff with the security skills needed to conduct their activities in a secure way.

The information security training program is conducted throughout the following activities:

- Selection of the target audiences within the Company and the definition of the specific programs based on the employees' awareness and knowledge of the organisation's security requirements;
- Preparation and execution of training sessions to:
  a. Increase the level of awareness about the relevant issues of Information Security;
  b. Make employees aware of internal policies and procedures, and their own role and responsibilities;
  c. Ensure knowledge of laws, regulations, best practices and standards in force, regarding Information Security;
  d. GFA personnel to increase the knowledge and skills of technical personnel.

6.4 Framework Review and Improvement

GFA performs an annual review of the performance of its Information Security Management System to guarantee the efficiency and effectiveness of security of its information and assets.

Colm Begley	15th October 2022
Colm Begley, CEO	**Dated**
Graphical Financial Analysis Limited.	