JANUARY 2023

Information Security

Introduction

The Confidentiality, Integrity and Availability of information is critical to our clients and is therefore a key priority for EFG International. We host hundreds of thousands of individual records worldwide. The security of this information is of the utmost importance and we continually make sizeable investments to protect our information, IT systems, applications, infrastructure and processes.

The purpose of this document is to summarise our approach to information security. It provides an overview of how we secure client information and our systems housing this information, keeping in mind that the specifics of these measures may vary depending on the service and the applicable country regulatory requirements.

Our information security programme and practices are focused on sharing information appropriately and lawfully, while providing confidentiality, integrity and availability.

Our Approach to Information Security and Business Resilience

EFG International has developed and implemented a comprehensive information security and business resilience framework aligned to industry best practices such as ISO/IEC 27001:2013 the International Standard for Information Security Management System (ISMS), IT Infrastructure Library (ITIL) for IT Service Management, and ISO22301:2012 for Business Continuity Management Systems (BCMS).

EFG International takes a multi-layered, defence-in-depth, approach to protecting the data EFG International has responsibility for; this includes physical, procedural, personnel and technical security to protect confidentiality, integrity and availability of information and services.

Information Security Governance and Policies

EFG International's Information Security Policy set demonstrates the high level of importance that EFG assigns to the security of business information and it sets out the necessary parameters for the management and control of information security. It formulates the overriding objectives and minimum standards that apply to information, IT and cyber security at EFG and defines the principles that must be observed to protect information assets during their lifecycle.

Information security is overseen by the EFG Information Security Committee (ISC). The ISC oversees security projects, reports, objectives and key performance indicators.

Human Resource Security

All EFG International workers are subject to screening prior to employment. The screening processes are conducted in accordance with relevant national laws and industry regulations and provide verification of identity and credentials, as well as evaluating applicant integrity.

All EFG International workers are subject to confidentiality/non-disclosure agreements as part of the standard employment contracts and are required to comply with the controls outlined in the Information Security Policy set, including an Acceptable Use Standard.

The Information Security Committee oversees the multi-lingual information security training and awareness programmes to ensure that all workers are aware of their responsibilities and possess the necessary resources to maintain our position on information security.

When a worker leaves, EFG International applies robust procedures to ensure the timely removal of access rights to IT systems as well as the retrieval of any physical information assets which are recorded in the asset inventories.

Asset Management

EFG International has implemented an information classification scheme for all information that supports its day-to-day business activities. EFG International maintains inventories of its information assets, including applications and IT systems.

Local certified companies are used for secure destruction for paper and magnetic media. The default destruction method for all assets containing information is physical destruction. Certificates of destruction are required and retained.

Physical and Environmental Security

All EFG International office locations operate risk-based controls to afford protection against unauthorised physical access. These can include physical and electronic access control systems, manned reception desks, CCTV and security lighting.

Access to our data centre facilities and other information processing locations is strictly controlled and restricted to pre-authorised individuals only. This access is logged and the access rights are reviewed on a regular basis.

Access Control

EFG International operates on the principle of 'least privilege' for access control. This is to ensure that only authorised individuals are permitted access to our business applications, systems, networks and computing devices; that individual accountability is established and to provide authorised users with the access permissions that are sufficient to enable them to perform their duties but do not permit them to exceed their authority. Access is provided under Role Based Access Control (RBAC) and activity is logged and monitored.

Cryptography

EFG International Information Security Policy set details the approved cryptographic algorithms and the process for encryption key management within EFG International. EFG International desktops and laptops have full disk encryption using AES256. Exchanges of confidential information across untrusted networks are encrypted-in-transit.

Communications and Operations Security

EFG International has implemented a defence-in-depth approach to protect its information and IT systems from existing and emerging threats. All EFG International IT systems are configured following technical security standards which include applicable controls such as system hardening, encryption, anti-virus and data loss prevention and regular patching.

The EFG International IT technical security controls are monitored by a security operations centre which collects and correlates the event logs from network devices, firewalls, IDS and web application firewalls. This data is analysed and any unusual or suspicious events generate the necessary alerts which are handled by our information security incident management processes.

System Acquisition, Development and Maintenance

EFG International follows a defined System Development Life Cycle (SDLC) that incorporates information security throughout each stage including risk assessments, the identification and implementation of control requirements, static and dynamic code analysis and technical security penetration testing.

Supplier Relationships

EFG International supply chain assurance program covers third party activities which are audited based on risk for information security. This may include the evaluation of prospective vendors for compliance with EFG International ISO27001/2 aligned information Security Policy set, risk identification, rating and finding management, contract review including confidentiality clauses, the right to audit and detailed contractual security requirements where required.

Information Security Incident Management

EFG International has global risk-based processes to respond to information security incidents, unusual or suspicious events and breaches of policies. These processes are owned and coordinated by the Information Security with formal involvement from relevant stakeholders (e.g. legal, compliance, technology, human resources, business relations and anti-fraud, marketing and public relations). All EFG International employees are provided with training and guidance to identify and report information security incidents.

Business Continuity Management

EFG International has an established Business Continuity Management programme that supports our regulatory and contractual requirements. Our programme is managed by dedicated office business continuity coordinators and is underpinned by relevant business continuity policies, procedures and supporting technologies.

Audit and Compliance

EFG International adheres to the proven 'Three Lines of Defence' risk management model and follows industry standards ('good business practice') regarding information security. The Information Security Committee oversees and measures compliance with the Information Security Policy set through periodic technical and non-technical control assessments.

Summary

Clients and individuals rightfully demand accountability from any organisation handling their personal and confidential data. We understand the importance of taking appropriate steps to safeguard information and are committed to protecting information relating to our clients and to our people.