JANUAR 2023

Informationssicherheit

Einführung

Die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen ist für unsere Kunden entscheidend und damit oberste Priorität für EFG International. Wir haben weltweit hunderttausende Datensätze gespeichert. Die Sicherheit dieser Informationen ist von grösster Wichtigkeit, und wir investieren laufend beträchtliche Summen, um unsere Informationen, IT-Systeme, Anwendungen, Infrastruktur und Prozesse zu schützen.

Das vorliegende Dokument fasst unser Konzept der Informationssicherheit zusammen. Es gibt einen Überblick, wie wir Kundendaten sichern sowie unsere Systeme, in denen diese gespeichert sind, wobei sich diese Massnahmen im Detail unterscheiden können, je nach Dienstleistung und geltenden nationalen Bestimmungen.

Bei unserem Programm und unseren Verfahren zur Informationssicherheit liegt unser Fokus darauf, Informationen angemessen und gesetzeskonform weiterzugeben, unter Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit.

Unser Konzept der Informationssicherheit und Business Resilience

EFG International hat einen umfassenden Rahmen für Informationssicherheit und Business Resilience entwickelt und umgesetzt, orientiert an den bewährtesten Verfahren der Branche, wie ISO/IEC 27001:2013, die international führende Norm für Informationssicherheits-Managementsysteme (ISMS), IT Infrastructure Library (ITIL) für das Management von IT-Dienstleistungen und ISO22301:2012 für Business-Continuity-Management-Systeme (BCMS).

EFG International verfolgt ein mehrschichtiges, gestaffeltes Konzept zum Schutz der Daten, für die EFG International verantwortlich ist; dies umfasst physische, verfahrensbezogene, personelle und technische Sicherheit zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Dienstleistungen.

Governance und Leitlinien zur Informationssicherheit

Die Leitlinie von EFG zur Informationssicherheit reflektiert die hohe Bedeutung, die EFG der Sicherheit von Geschäftsinformationen beimisst, und legt die nötigen Rahmenbedingungen für Verwaltung und Kontrolle von Informationssicherheit fest. Sie beschreibt die übergeordneten Ziele und Mindestanforderungen für Daten, IT- und Cybersicherheit bei EFG und definiert die zu beachtenden Grundsätze zum Schutz wertvoller Informationen während ihres gesamten Lebenszyklus.

Die Informationssicherheit wird durch den Informationssicherheitsausschuss (Information Security Committee, ISC) überwacht. Der ISC überwacht Projekte, Berichte, Ziele und Leistungskennzahlen (KPI).

Human Resource Security

Alle Mitarbeitenden von EFG International werden vor der Einstellung überprüft. Gemäss den jeweiligen Landesgesetzen und Branchenbestimmungen werden Identität, Referenzen und Unbescholtenheit des Bewerbers oder der Bewerberin geprüft.

Alle Mitarbeitenden von EFG International sind durch Geheimhaltungsvereinbarungen als Teil des Standard-Arbeitsvertrags gebunden und müssen sich an die Kontrollmassnahmen aus der Leitlinie zur Informationssicherheit halten, darunter auch ein Acceptable Use Standard.

Der Ausschuss für Informationssicherheit leitet die mehrsprachigen Schulungen zur Informationssicherheit und Sensibilisierungsprogramme, damit alle Mitarbeitenden sich ihrer Pflichten bewusst sind und über die nötigen Mittel verfügen, um unsere Standards zur Informationssicherheit aufrechtzuerhalten.

Für Mitarbeitende, die uns verlassen, gelten bei EFG International strenge Verfahren, um zeitnah die Zugangsberechtigungen zu IT-Systemen zu sperren und alle physischen Informationsträger einzusammeln, die in den Beständen verzeichnet sind.

Asset Management

EFG International hat für alle Informationen die im Tagesgeschäft verwendet werden, ein Datenklassifizierungssystem umgesetzt. EFG International hat alle ihre Informationsressourcen, einschliesslich Anwendungen und IT-Systeme, katalogiert.

Für die sichere Vernichtung von Papiermedien und Magnetträgern werden zertifizierte lokale Betriebe eingesetzt. Standardverfahren zur Vernichtung aller Informationsträger ist die physische Zerstörung. Wir lassen uns Vernichtungszertifikate aushändigen und bewahren diese auf.

Physische und umgebungsbezogene Sicherheit

Alle Bürostandorte von EFG International haben risikobezogene Kontrollmechanismen als Schutz gegen unbefugten physischen Zugriff. Dazu gehören physische und elektronische Zugangskontrollsysteme, eine personell besetzte Rezeption, Kameraüberwachung und Sicherheitsbeleuchtung.

Der Zugang zu unseren Datenzentren und weiteren Orten der Informationsverarbeitung wird streng kontrolliert und ist auf vorab befugte Personen beschränkt. Jeder Zugang wird protokolliert, die Zugangsrechte werden regelmässig überprüft.

Zugriffskontrolle

EFG International arbeitet bei der Zugriffskontrolle nach dem Prinzip der geringsten Rechte (Principle of least Privilege). Damit soll sichergestellt werden, dass nur berechtigte Personen Zutritt auf unsere Geschäftsanwendungen, Systeme, Netzwerke und Rechner haben. So ist die persönliche Verantwortlichkeit zugewiesen, und berechtigte Nutzer erhalten Zugriffsrechte, die zur Erfüllung ihrer Aufgaben ausreichend sind, mit denen sie aber nicht ihre Befugnisse überschreiten können. Es gilt die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC), und alle diesbezüglichen Aktivitäten werden aufgezeichnet und überwacht.

Verschlüsselung

Die Leitlinie zur Informationssicherheit von EFG International definiert die genehmigten kryptografischen Algorithmen und das Verfahren zur Verwaltung der kryptographischen Schlüssel (Encryption Key Management). Desktop-PCs und Laptops von EFG International verfügen über komplette AES256-Festplattenverschlüsselung. Der Austausch vertraulicher Informationen über nicht vertrauenswürdige Netzwerke ist während der Übertragung verschlüsselt.

Kommunikations- und Betriebssicherheit

EFG International hat ein gestaffeltes Konzept implementiert, um seine Informationen und IT-Systeme vor aktuellen und zukünftigen Bedrohungen zu schützen. Alle Systeme von EFG International sind nach technischen Sicherheitsstandards konfiguriert, die geeignete Kontrollen umfassen wie etwa Systemhärtung, Verschlüsselung, Virenschutz, Verhinderung von Datenverlust und regelmässige Schwachstellenbehebung.

Die technischen IT-Sicherheitsmassnahmen von EFG International werden durch eine Sicherheitszentrale überwacht, welche die Ereignisprotokolle von Netzwerkgeräten, Firewalls, IDS und Web Application Firewalls sammelt und abgleicht. Diese Daten werden analysiert, und alle ungewöhnlichen oder verdächtigen Vorkommnisse lösen entsprechende Warnungen aus, die dann anhand unserer Prozesse zu Informationssicherheitsvorfällen bearbeitet werden.

Erwerb, Entwicklung und Wartung von Systemen

EFG International befolgt einen festgelegten Lebenszyklus der Systementwicklung (System Development Life Cycle, SDLC). Hierbei ist in jeder Phase Informationssicherheit vorgesehen, durch Risikobewertungen, Ermittlung und Umsetzung von Kontrollen, statische und dynamische Codeanalyse und Penetrationstests zur technischen Sicherheit.

Lieferantenbeziehungen

Im Rahmen des Lieferkettensicherheitsprogramms von EFG International werden Tätigkeiten Dritter anhand der Risiken für die Informationssicherheit geprüft. Das umfasst zum Beispiel: Prüfung potenzieller Anbieter auf Einhaltung der an ISO 27001/2 ausgerichteten Leitlinien zur Informationssicherheit von EFG International, Ermittlung, Einstufung und Absicherung von Risiken, Vertragsprüfung einschliesslich Vertraulichkeitsklauseln, das Recht zur Durchführung von Revisionen und, wo erforderlich, detaillierte vertragliche Sicherheitspflichten.

Umgang mit Vorfällen bezüglich der Informationssicherheit

EFG International verfügt über globale risikobasierte Prozesse zur Reaktion auf Vorfälle bezüglich der Informationssicherheit, ungewöhnliche oder verdächtige Vorkommnisse und Verstösse gegen Leitlinien. Die Abteilung Informationssicherheit ist für diese Prozesse zuständig und koordiniert sie, mit förmlicher Einbindung der jeweiligen Beteiligten (z. B. die Reachtsabteilung, Compliance, Informations Technologie, HR, Geschäftsbeziehungen und Betrugsbekämpfung, Marketing und Öffentlichkeitsarbeit). Alle Mitarbeitenden von EFG International erhalten Schulungen und Anweisungen, um Vorfälle bezüglich der Informationssicherheit zu erkennen und zu melden.

Business Continuity Management

EFG International hat ein Business-Continuity-Management-Programm umgesetzt, um unsere gesetzlichen und vertraglichen Verpflichtungen zu erfüllen. Das Programm wird von dedizierten Business-Continuity-Koordinatoren betreut, gestützt auf entsprechende Business-Continuity-Leitlinien, Verfahren und Technologien.

Audit and Compliance

Im Risikomanagement hält sich EFG International an das Drei-Linien-Modell und befolgt die Branchenstandards («gute Geschäftspraxis») zur Informationssicherheit. Der Ausschuss für Informationssicherheit (Information Security Committee) überwacht und beurteilt die Einhaltung der Leitlinien zur Informationssicherheit mittels regelmässiger technischer und nichttechnischer Kontrollbewertungen.

Schlusswort

Kunden und Einzelpersonen verlangen zu Recht von jeder Organisation einen verantwortlichen Umgang mit ihren persönlichen und vertraulichen Daten. Wir sind uns der Wichtigkeit angemessener Datenschutz-Massnahmen bewusst, und sehen uns dem Schutz der Daten unserer Kunden und Mitarbeitenden verpflichtet.