GENNAIO 2023

Sicurezza delle informazioni

Introduzione

La riservatezza, l'integrità e la disponibilità delle informazioni sono fondamentali per la nostra clientela e rappresentano dunque una priorità per EFG International. Conserviamo centinaia di migliaia di record di dati in tutto il mondo. La sicurezza di tali informazioni è della massima importanza ed effettuiamo incessantemente investimenti considerevoli per proteggere informazioni, sistemi IT, applicazioni, infrastruttura e processi.

Il presente documento ha lo scopo di presentare in sintesi il nostro approccio alla sicurezza delle informazioni. Fornisce una panoramica di come proteggiamo le informazioni della clientela e i nostri sistemi contenenti tali informazioni, fermo restando che gli aspetti specifici di tali misure possono variare a seconda del servizio e dei requisiti normativi applicabili in ciascun Paese.

Il nostro programma e le nostre procedure di sicurezza delle informazioni sono incentrate su una condivisione appropriata e legale delle informazioni, garantendo al tempo stesso riservatezza, integrità e disponibilità.

Il nostro approccio alla sicurezza delle informazioni e alla resilienza aziendale

EFG International ha sviluppato e implementato un piano completo per la sicurezza delle informazioni e la resilienza aziendale, in linea con le migliori prassi del settore, come l'ISO/IEC 27001:2013, lo standard internazionale per il sistema di gestione della sicurezza delle informazioni (ISMS), la biblioteca dell'infrastruttura informatica (ITIL) per la gestione dei servizi IT e l'ISO22301:2012 per i sistemi di gestione della continuità operativa (BCMS).

EFG International adotta un approccio di difesa in profondità su più livelli, per proteggere i dati che rientrano nella sua sfera di responsabilità; tale approccio coinvolge la sicurezza fisica, procedurale, del personale e tecnica per tutelare la riservatezza, l'integrità e la disponibilità di informazioni e servizi.

Governance e linee guida di sicurezza delle informazioni

Le linee guida di sicurezza delle informazioni definite da EFG International dimostrano l'alto grado di importanza attribuito da EFG alla sicurezza delle informazioni aziendali e fissano i parametri necessari per la gestione e il controllo della sicurezza delle informazioni. Definiscono gli obiettivi prioritari e i requisiti minimi applicabili alle informazioni, all'IT e alla sicurezza informatica all'interno di EFG, e individuano i principi da rispettare per proteggere le risorse informative durante il loro ciclo di vita.

La sicurezza delle informazioni è supervisionata dell'Information Security Committee (Comitato per la Sicurezza delle Informazioni – ISC) di EFG. Tale comitato supervisiona progetti, rapporti, obiettivi e indicatori chiave di prestazione relativi alla sicurezza.

Sicurezza delle risorse umane

Tutte le persone che lavorano per EFG International sono sottoposte a screening prima dell'assunzione. I processi di screening sono condotti in conformità alle leggi nazionali e alle normative di settore pertinenti e sono finalizzati a verificare l'identità e le credenziali, nonché a valutare l'integrità della persona candidata.

Tutte le persone che lavorano per EFG International sono soggette ad accordi di riservatezza/non divulgazione come parte dei contratti di lavoro standard e sono tenute a rispettare i controlli stabiliti nelle linee guida di sicurezza delle informazioni, incluso uno standard di utilizzo accettabile.

Il Comitato per la sicurezza delle informazioni sovrintende ai programmi multilingue di formazione e sensibilizzazione in materia di sicurezza delle informazioni, per garantire che l'intero personale sia consapevole delle proprie responsabilità e disponga delle risorse necessarie per mantenere la nostra posizione sulla sicurezza delle informazioni.

Quando una persona lascia l'azienda, EFG International attua procedure consolidate per garantire la rimozione tempestiva dei diritti di accesso ai sistemi IT e il recupero di qualsiasi risorsa informativa fisica registrata negli inventari delle risorse.

Asset management

EFG International ha realizzato un sistema di classificazione per tutte le informazioni alla base delle sue attività aziendali quotidiane. EFG International gestisce gli inventari delle proprie risorse informative, comprese le applicazioni e i sistemi IT.

Per la distruzione sicura di materiale cartaceo e supporti magnetici, ricorriamo ad aziende locali certificate. Il metodo di distruzione standard per tutte le risorse contenenti informazioni è la distruzione fisica. A tal proposito, richiediamo e conserviamo i certificati di distruzione.

Sicurezza fisica e ambientale

Tutte le sedi di EFG International eseguono controlli basati sul rischio per prevenire l'accesso fisico non autorizzato, che possono includere sistemi di controllo degli accessi fisici ed elettronici, postazioni di reception presidiate, telecamere a circuito chiuso e illuminazione di sicurezza.

L'accesso alle nostre strutture di data center e ad altre sedi di elaborazione delle informazioni è strettamente controllato e riservato unicamente a persone precedentemente autorizzate. Tale accesso è registrato e i diritti di accesso sono periodicamente rivisti.

Controllo degli accessi

EFG International gestisce il controllo degli accessi in base al principio del privilegio minimo, in modo da garantire che solo alle persone autorizzate sia consentito accedere alle applicazioni, ai sistemi, alle reti e ai dispositivi informatici aziendali; inoltre stabilire le responsabilità individuali e fornire alle e agli utenti autorizzati i diritti di accesso sufficienti per permettere loro di svolgere le loro mansioni senza oltrepassare i limiti della loro autorità. L'accesso è fornito nell'ambito del controllo degli accessi basato sui ruoli (RBAC) e l'attività è registrata e monitorata.

Crittografia

Le linee guida di sicurezza delle informazioni di EFG International definiscono dettagliatamente gli algoritmi di crittografia approvati e il processo di gestione delle chiavi di crittografia applicato all'interno di EFG International.
I computer fissi e portatili di EFG International dispongono di crittografia completa del disco mediante AES256.
Gli scambi di informazioni riservate tra reti non attendibili sono crittografate in-transit.

Sicurezza delle comunicazioni e delle operazioni

EFG International ha posto in essere un approccio di difesa in profondità per proteggere le sue informazioni e i suoi sistemi IT da minacce esistenti ed emergenti. Tutti i sistemi IT di EFG International sono configurati in base a standard tecnici di sicurezza che comprendono controlli applicabili come hardening dei sistemi, crittografia, antivirus e data loss prevention, nonché l'applicazione regolare di patch.

I controlli tecnici di sicurezza IT di EFG International sono monitorati da un centro operativo di sicurezza che raccoglie e correla i log degli eventi da dispositivi di rete, firewall, IDS e firewall di applicazioni web. Tali dati sono analizzati e qualsiasi evento insolito o sospetto genera gli opportuni avvisi, affrontati attraverso i nostri processi di gestione degli incidenti in materia di sicurezza delle informazioni.

Acquisizione, sviluppo e manutenzione del sistema

EFG International segue un ciclo di vita dello sviluppo del software definito (SDLC), che integra la sicurezza delle informazioni in ogni fase, comprese le valutazioni del rischio, l'identificazione e l'implementazione dei requisiti di controllo, l'analisi statica e dinamica del codice e i test di penetrazione della sicurezza tecnica.

Rapporti con i fornitori

Il programma di garanzia della catena di fornitura di EFG International copre le attività di terze parti, sottoposte ad audit in base al rischio in materia di sicurezza delle informazioni. Ciò può includere la valutazione dei potenziali fornitori dal punto di vista della conformità alle linee guida di sicurezza delle informazioni di EFG International, uniformate a ISO27001/2, l'identificazione dei rischi, la gestione delle valutazioni e delle conclusioni, la revisione dei contratti comprese le clausole di riservatezza, il diritto di audit e requisiti di sicurezza contrattuali specifici, se necessario.

Gestione degli incidenti di sicurezza delle informazioni

EFG International attua processi globali basati sul rischio per reagire a incidenti di sicurezza delle informazioni, eventi insoliti o sospetti e violazioni delle linee guida. Tali processi sono interni e coordinati dall'ufficio di Information Security con il coinvolgimento formale delle parti interessate (p. es. Legal, Compliance, Technology, Human resources, Business relations e anti-fraud, Marketing e Public relations). La totalità del personale di EFG International riceve formazione e opportune direttive per individuare e segnalare gli incidenti di sicurezza delle informazioni.

Gestione della continuità operativa

EFG International ha un programma consolidato di gestione della continuità operativa che supporta i nostri requisiti normativi e contrattuali. Il nostro programma è gestito da personale specializzato nella coordinazione della continuità operativa ed è sostenuto da linee guida, procedure e tecnologie di supporto specifiche per la continuità operativa.

Audit e compliance

EFG International aderisce al comprovato modello di gestione del rischio «Three Lines of Defence» e segue gli standard del settore («buone prassi aziendali») in materia di sicurezza delle informazioni. Il Comitato per la sicurezza delle informazioni sovrintende e misura la conformità alle linee guida di sicurezza delle informazioni attraverso valutazioni periodiche di natura tecnica e non tecnica.

Sintesi

La clientela e gli individui si aspettano legittimamente che ogni organizzazione gestisca i loro dati personali e riservati in modo responsabile. Siamo consapevoli dell'importanza di adottare misure appropriate per salvaguardare le informazioni e ci impegniamo pertanto a proteggere le informazioni relative alla nostra clientela e al nostro personale.