

# Sécurité de l'information

## Introduction

La confidentialité, l'intégrité et la disponibilité des informations sont essentielles pour nos clients et constituent donc une priorité absolue pour EFG International. Nous hébergeons des centaines de milliers d'enregistrements individuels dans le monde entier. La sécurité de ces informations revêt une importance capitale et nous réalisons en permanence des investissements considérables pour protéger nos informations, systèmes informatiques, applications, infrastructures et processus.

Le présent document vise à résumer notre approche de la sécurité de l'information. Il offre une vue d'ensemble de la manière dont nous sécurisons les informations des clients ainsi que de nos systèmes abritant ces informations, sachant que les spécificités de ces mesures peuvent varier en fonction du service et/ou des exigences réglementaires applicables dans chaque pays.

Notre programme et nos pratiques de la sécurité de l'information sont axés sur le caractère approprié et légal du partage de données, parallèlement à la confidentialité, à l'intégrité et à la disponibilité de l'information.

## Notre approche de la sécurité de l'information et de la résilience commerciale

EFG International a mis au point et implémenté un cadre complet de sécurité de l'information et de résilience commerciale, aligné sur les meilleures pratiques du secteur telles que la norme ISO/IEC 27001:2013, la norme internationale pour les systèmes de management de la sécurité de l'information (SMSI), l'IT Infrastructure Library (ITIL) pour la gestion des services informatiques et la norme ISO22301:2012 pour les systèmes de management de la continuité d'activité (BCMS).

EFG International adopte une approche de défense en profondeur en plusieurs couches afin de protéger les données dont elle a la responsabilité ; cela inclut la sécurité physique, procédurale, technique et du personnel afin de préserver la confidentialité, l'intégrité et la disponibilité des informations et des services.

## Gouvernance et politique de sécurité de l'information

La politique de sécurité de l'information d'EFG International démontre la grande importance qu'EFG accorde à la sécurité des informations et établit le cadre nécessaire pour la gestion et le contrôle de la sécurité de l'information. Elle formule les objectifs à atteindre et définit les normes minimales qui s'appliquent à l'information, à l'informatique et à la cybersécurité au sein d'EFG, ainsi que les principes à respecter pour protéger l'information tout au long de son cycle de vie.

La sécurité de l'information est supervisée par le comité de la sécurité de l'information (ISC). L'ISC définit les objectifs des contrôles, supervise les projets de sécurité, les rapports et les principaux indicateurs de performance en la matière.

## Sécurité des ressources humaines

Tous les membres du personnel d'EFG International sont soumis à une sélection avant leur entrée en poste. Les processus de sélection sont menés conformément aux droits nationaux et aux règles en vigueur dans le secteur concerné, et inclut la vérification de l'identité et de l'intégrité des candidats et de l'authenticité de leurs certificats.

Tous les membres du personnel d'EFG International sont soumis à des accords de confidentialité/non-divulgateion dans le cadre des contrats de travail standard et doivent se conformer aux contrôles mentionnés dans la politique de sécurité de l'information, y compris à une charte définissant le cadre d'utilisation acceptable des ressources informatiques.

Le comité de la Sécurité Informatique supervise les programmes de formation et de sensibilisation à la sécurité de l'information dans plusieurs langues afin de s'assurer que tous les membres du personnel ont conscience de leurs responsabilités et possèdent les ressources nécessaires pour maintenir notre position en matière de sécurité de l'information.

Lors du départ d'un membre du personnel, EFG International applique des procédures bien établies pour garantir la suppression en temps voulu des droits d'accès aux systèmes informatiques ainsi que le retrait de tout actif physique enregistré dans les inventaires.

### Gestion d'actifs

EFG International a mis en œuvre un schéma de classification de l'information pour toutes les données sur lesquelles reposent ses activités commerciales courantes. EFG International tient à jour des inventaires de ses actifs d'information, y compris de ses applications et systèmes informatiques.

Il fait appel à des entreprises locales certifiées dans la destruction de documents papier ainsi que des supports magnétiques. La méthode de destruction par défaut pour tout actif contenant des informations est la destruction physique. Des certificats de destruction sont demandés et conservés.

### Sécurité physique et de l'environnement

Tous les sites d'EFG International réalisent des contrôles basés sur le risque pour interdire les accès physiques non autorisés. Cela inclut des systèmes de contrôle d'accès physique et électronique, des zones d'accueil disposants d'une permanence, des caméras de surveillance et des éclairages de sécurité.

L'accès à nos « Data Centers » et à d'autres sites de traitement d'informations est soumis à un contrôle strict et limité uniquement aux personnes autorisées. Ces accès sont enregistrés dans un journal et les droits d'accès sont régulièrement vérifiés.

### Contrôle des accès

EFG International opère selon le principe du « moindre privilège » pour le contrôle des accès. Cela vise à garantir que seules les personnes autorisées puissent obtenir l'accès à nos applications métier, bases de données, systèmes et réseaux et qu'une responsabilité individuelle soit établie. Les utilisateurs bénéficient ainsi des autorisations suffisantes pour effectuer leurs tâches, sans toutefois pouvoir outrepasser leur autorité. L'accès est basé sur les rôles métier (Role Based Access Control – RBAC), et les activités liées sont protocolées et surveillées.

### Chiffrement

La politique de sécurité de l'information d'EFG International détaille les algorithmes de chiffrement approuvés et le processus de gestion des clés de cryptage au sein d'EFG International. Les ordinateurs de bureau et ordinateurs portables d'EFG International disposent d'un de chiffrement

total des disques selon le standard AES256. Les échanges d'informations confidentielles empruntant des réseaux non sécurisés sont chiffrés.

### Sécurité des communications et des opérations

EFG International a mis en place une approche de défense approfondie pour protéger ses informations et ses systèmes informatiques de menaces existantes et émergentes. Tous les systèmes informatiques d'EFG International sont configurés selon des standards techniques de sécurité incluant des contrôles applicables tels que le renforcement des systèmes, le chiffrement, les antivirus, la prévention de la fuite de données et les mises à jour régulières.

Les contrôles techniques de sécurité informatique d'EFG International sont surveillés par un centre de sécurité opérationnelle qui collecte et met en relation les journaux d'évènements provenant des équipements informatiques tel que pare-feu, IDS et pare-feu d'applications web. Tout événement inhabituel ou suspect déclenche des alertes, qui sont alors traitées selon nos processus de gestion des incidents de sécurité de l'information.

### Acquisition, développement et maintenance des systèmes

EFG International suit un cycle de vie de développement des systèmes (System Development Life Cycle – SDLC) intégrant la sécurité de l'information à chaque étape, y compris l'évaluation du risque, l'identification et la mise en œuvre d'exigences de contrôle, l'analyse de code statique et dynamique ainsi que les tests d'intrusion.

### Relations avec les fournisseurs

Le programme d'assurance de la chaîne d'approvisionnement d'EFG International couvre les activités de tiers via un audit lié aux risques en matière de sécurité de l'information. Cela inclut l'évaluation des fournisseurs potentiels en matière de respect de la politique de sécurité de l'information d'EFG International, d'évaluation des risques et des faiblesses constatées, l'analyse des contrats (y compris des clauses de confidentialité), le droit d'audit et les exigences contractuelles détaillées en matière de sécurité.

### Gestion des incidents de sécurité de l'information

EFG International implémente des processus basés sur le risque pour répondre aux incidents de sécurité de l'information, aux événements inhabituels ou suspects et aux violations des directives. Ces processus sont détenus et coordonnés par le service de la sécurité de l'information avec l'implication formelle des parties prenantes concernées (p.ex. Légal, Compliance, IT, Ressources Humaines, Business relations, Anti-Fraude, Marketing et Public relations).

Tous les membres du personnel d'EFG International bénéficient de formations et conseils requis pour identifier et déclarer les incidents de sécurité de l'information.

### **Gestion de la continuité opérationnelle**

EFG International a mis en place un programme de gestion de la continuité opérationnelle répondant à nos exigences réglementaires et contractuelles. Notre programme est géré par des coordinateurs dédiés à la continuité des affaires et est supporté par des directives, des procédures et de la technologie pertinente en matière de continuité opérationnelle.

### **Audit et Compliance**

EFG International adhère au modèle éprouvé de gestion des risques « Trois lignes de défense » et applique les standards du secteur (« bonnes pratiques opérationnelles ») concernant la sécurité de l'information. Le comité de la sécurité de l'information supervise et mesure le respect de la politique de sécurité de l'information au moyen d'évaluations régulières des contrôles techniques et non techniques.

### **Résumé**

Les clients et les membres du personnel exigent à juste titre que toute organisation traitant leurs données personnelles et confidentielles le fasse de manière responsable. Nous comprenons l'importance des mesures appropriées visant à protéger l'information et nous nous engageons à implémenter les mesures techniques et organisationnelles requises.