FDJ UNITED

POLITIQUE INSTITUTIONNELLE DE CYBERSÉCURITÉ

01 Notre engagement

Chez FDJ UNITED, la cybersécurité est au cœur de la confiance que nous entretenons avec nos joueurs et partenaires.

En tant qu'opérateur de jeux de référence en Europe, FDJ UNITED traite quotidiennement des millions de transactions et de données personnelles de joueurs, partenaires, fournisseurs. Cette responsabilité nous impose un niveau d'exigence élevé en matière de cybersécurité.

Face à des cybermenaces de plus en plus sophistiquées (rançongiciels, fraudes, attaques par ingénierie sociale, risques liés à l'IA agentique), nous renforçons en permanence nos capacités de détection, de protection et de réponse dans une logique d'amélioration continue.

02 Un environnement fortement encadré sur le plan réglementaire

Les activités de FDJ UNITED évoluent dans un environnement fortement réglementé. Le Groupe veille au respect des obligations en matière de protection des données, d'intégrité des jeux et de sécurité des systèmes d'information, notamment sous le contrôle des autorités compétentes telles que l'Autorité Nationale des Jeux (ANJ) en France.

FDJ UNITED s'appuie également sur des standards reconnus du secteur, incluant notamment les normes ISO 27001, le standard World Lottery Association Security Control Standard (WLA-SCS) et les exigences liées aux activités de paiement (PCI-DSS), afin de garantir un niveau élevé de sécurité et de conformité à l'échelle du Groupe.

03 Une gouvernance cybersécurité à l'échelle du Groupe

La cybersécurité fait l'objet d'un suivi régulier au sein des instances de gouvernance du Groupe, avec une implication du Comité Exécutif (COMEX), via la représentation de la fonction sécurité par le Directeur Technologie et la tenue de revues de direction régulières, et des administrateurs à travers le Comité d'Audit et des Risques.

La Direction Cybersécurité du Groupe définit et met en œuvre la stratégie de cybersécurité, en cohérence avec les enjeux business, réglementaires et technologiques. Elle s'appuie sur une organisation structurée et sur des instances de pilotage réunissant les principales directions métiers et IT, garantissant une approche coordonnée et adaptée aux risques.

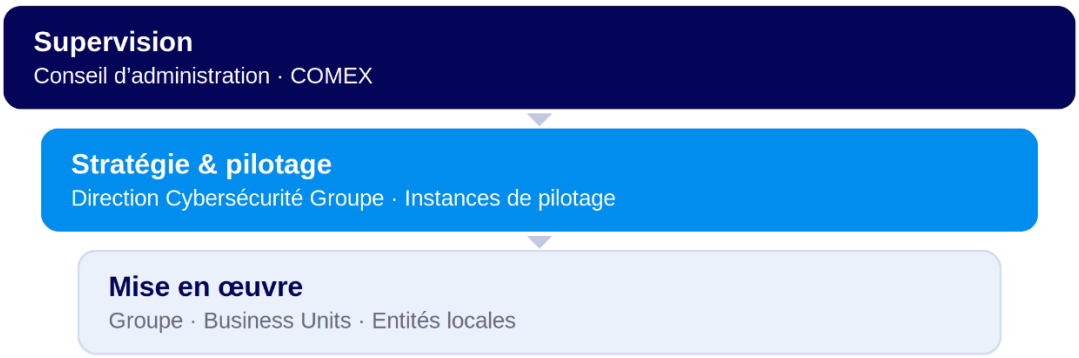

Figure 1 — Une gouvernance structurée, du Conseil d'Administration jusqu'aux entités locales.

Ce document est la propriété de FDJ UNITED. Toute reproduction, même partielle, est interdite.

04 Rôles et responsabilités en matière de cybersécurité

Les responsabilités en matière de sécurité de l'information sont formellement définies et attribuées à l'ensemble des collaborateurs au travers de la Politique Groupe de Sécurité des Systèmes d'Information (PGSSI) de FDJ UNITED et de son cadre de gouvernance cybersécurité. Des rôles et responsabilités clairement établis existent aux niveaux Groupe, Business Unit et entité, depuis la Direction Générale et les responsables cybersécurité jusqu'aux correspondants cybersécurité locaux.

Les managers sont responsables de l'application des exigences de sécurité, du soutien aux actions de sensibilisation et du respect des règles au sein de leurs équipes. Les chefs de projet intègrent les exigences de sécurité et la gestion des risques dans leurs projets, tandis que l'ensemble des collaborateurs est tenu de respecter les politiques de sécurité, de participer aux programmes de sensibilisation et de signaler sans délai tout incident ou événement de sécurité suspect.

05 Un cadre de sécurité structuré et auditable

La démarche cybersécurité de FDJ UNITED repose sur un référentiel structuré inspiré des standards internationaux (notamment ISO 27001 et NIST) et des exigences réglementaires applicables à ses activités.

Ce cadre définit des principes de sécurité communs à l'ensemble des entités du Groupe, reposant notamment sur :

- Une approche fondée sur l'appréciation des risques et l'amélioration continue, notamment via nos systèmes de management de la sécurité de l'information ;
- La protection des systèmes d'information et des données sensibles ;
- La conformité aux réglementations et standards applicables ;
- L'application de contrôles de sécurité adaptés aux niveaux de criticité.

Figure 2 — Les quatre principes fondateurs du cadre de sécurité.

Ces principes sont déclinés en politiques, procédures et dispositifs opérationnels couvrant notamment :

- La protection et l'intégrité des données joueurs et métiers ;
- La sécurisation de l'usage de l'IA ;
- La gestion des identités, des accès et des comptes à privilèges (IAM/PAM) ;
- La gestion des vulnérabilités, des correctifs et des incidents ;
- La gestion des incidents et des crises cybersécurité ;
- La gestion des exceptions ;

Ce document est la propriété de FDJ UNITED. Toute reproduction, même partielle, est interdite.

06 Une approche proactive face aux risques émergents

- La sensibilisation des collaborateurs.

FDJ UNITED intègre pleinement dans sa stratégie cybersécurité les risques liés aux évolutions technologiques et aux nouveaux usages.

Le Groupe s'appuie sur des principes structurants permettant d'encadrer l'adoption des technologies émergentes, notamment :

- Une évaluation préalable des risques avant tout déploiement ;
- Une utilisation maîtrisée et supervisée des systèmes automatisés ;
- Une protection des données sensibles ;
- Une gestion des dépendances technologiques dans une logique de souveraineté et de résilience.

Cette approche vise à concilier innovation et maîtrise des risques dans un environnement en constante transformation.

07 Une gouvernance et un accompagnement renforcés pour l'IA

FDJ UNITED encadre de manière spécifique l'usage de l'intelligence artificielle, compte tenu des opportunités et des risques associés.

La gouvernance de l'IA s'appuie sur des principes clairs en matière de sécurité, de protection des données, d'éthique et de conformité réglementaire, intégrés dans les dispositifs de gouvernance spécifiques. Les cas d'usage font l'objet d'une évaluation des risques adaptée, en lien avec les enjeux métier et technologiques.

Par ailleurs, la Direction Cybersécurité accompagne les projets intégrant des solutions d'IA tout au long de leur cycle de vie, avec l'ambition de sécuriser les usages dès la phase de conception. Cet accompagnement vise à concilier innovation, maîtrise des risques et cohérence avec les exigences du Groupe.

08 Une capacité de détection et de réponse continue

FDJ UNITED s'appuie sur ses Centres des Opérations de Sécurité (SOC) pour assurer une surveillance continue des systèmes d'information et détecter, analyser et traiter les événements et incidents de sécurité. Les activités de supervision, de détection et de réponse aux menaces cyber sont centralisées au niveau du Groupe.

Ces dispositifs de surveillance contribuent à la protection des systèmes d'information, à la réduction des risques de compromission, à la limitation de l'impact des incidents et au renforcement de la résilience de l'organisation face aux cybermenaces.

09 Un dispositif de contrôle à trois lignes de défense

Notre environnement de contrôle s'organise selon le modèle des trois lignes de défense : les équipes opérationnelles intègrent la sécurité dans leurs pratiques quotidiennes ; la Direction Cybersécurité définit les exigences, accompagne les entités et contrôle leur conformité ; l'Audit Interne réalise des contrôles et audits indépendants de notre posture de sécurité.

Ce document est la propriété de FDJ UNITED. Toute reproduction, même partielle, est interdite.

Figure 4 — Le modèle des trois lignes de défense.

Cette approche est complétée par des tests d'intrusion réguliers, du Red Team, des exercices de crise cyber et des évaluations externes de notre maturité.

10 La cybersécurité est l'affaire de chaque collaborateur

La cybersécurité repose sur l'implication de l'ensemble des collaborateurs. FDJ UNITED déploie des programmes de sensibilisation et de formation adaptés aux différents métiers, afin de diffuser les bonnes pratiques et renforcer la culture de sécurité à tous les niveaux de l'organisation.

Ces actions incluent un parcours de sensibilisation annuel, des campagnes de phishing, des événements dédiés permettant à chacun d'agir en acteur de la cybersécurité.

11 Sécurité des relations avec les fournisseurs

FDJ UNITED applique une approche fondée sur les risques pour la gestion de la cybersécurité des tiers. Les exigences de sécurité sont définies dès l'entrée en relation avec les fournisseurs au travers d'évaluations de cybersécurité et de clauses contractuelles de sécurité. Les fournisseurs critiques sont identifiés selon un processus formel de segmentation et font l'objet d'une surveillance renforcée, incluant des revues périodiques, des audits et le suivi des plans de remédiation. Ces exigences sont maintenues et réévaluées tout au long du cycle de vie de la relation fournisseur afin de garantir leur alignement avec les standards de cybersécurité du Groupe.

12 Un engagement au service de l'écosystème

FDJ UNITED s'engage activement dans l'écosystème cybersécurité, en collaborant avec les autorités compétentes et les acteurs sectoriels, et en contribuant au développement des compétences et des talents.

Cet engagement reflète la volonté du Groupe de contribuer à l'amélioration du niveau de sécurité de son écosystème, et en particulier des petites et moyennes entreprises.

À ce titre, FDJ UNITED s'inscrit activement dans des initiatives et réseaux de place tels que le **Campus Cyber** (National et Euromed) contribuant ainsi aux groupes de travail, au partage de bonnes pratiques, à la veille et à la coopération entre pairs.

Le Groupe soutient également des initiatives favorisant la diversité et l'inclusion dans la cybersécurité, notamment à travers son engagement auprès du **CEFCYS** (Cercle des Femmes de la Cybersécurité).

Ce document est la propriété de FDJ UNITED. Toute reproduction, même partielle, est interdite.