FDJ UNITED

INSTITUTIONAL CYBERSECURITY POLICY

01 Our Commitment

At FDJ UNITED, cybersecurity is at the core of the trust we maintain with our players, partners, and stakeholders.

As a leading gaming operator in Europe, FDJ UNITED processes millions of transactions and personal data records every day on behalf of players, partners, and suppliers. This responsibility requires us to maintain the highest standards of cybersecurity and information security.

In response to increasingly sophisticated cyber threats (including ransomware, fraud, social engineering attacks, and risks associated with agentic AI), we continuously strengthen our capabilities in detection, protection, and incident response through a process of ongoing improvement.

02 A Highly Regulated Environment

FDJ UNITED operates in a highly regulated environment. The Group ensures compliance with obligations related to data protection, gaming integrity, and information security, under the oversight of competent regulatory authorities such as the French National Gaming Authority (ANJ).

FDJ UNITED also relies on internationally recognized standards and industry frameworks, including ISO 27001, the World Lottery Association Security Control Standard (WLA-SCS), and payment security requirements such as PCI DSS, to ensure a high level of security and compliance across the Group.

03 Group-Wide Cybersecurity Governance

Cybersecurity is regularly monitored and reviewed through the Group's governance bodies. Oversight is ensured by the Executive Committee (ExCom), through the representation of the Information Security function by the Chief Technology Officer (CTO) and the conduct of regular management reviews, as well as by the Board of Directors through the Audit and Risk Committee.

The Group Cybersecurity Department defines and implements the cybersecurity strategy in alignment with business, regulatory, and technological objectives. It relies on a structured organization and dedicated governance forums bringing together key business and IT stakeholders, ensuring a coordinated and risk-based approach.

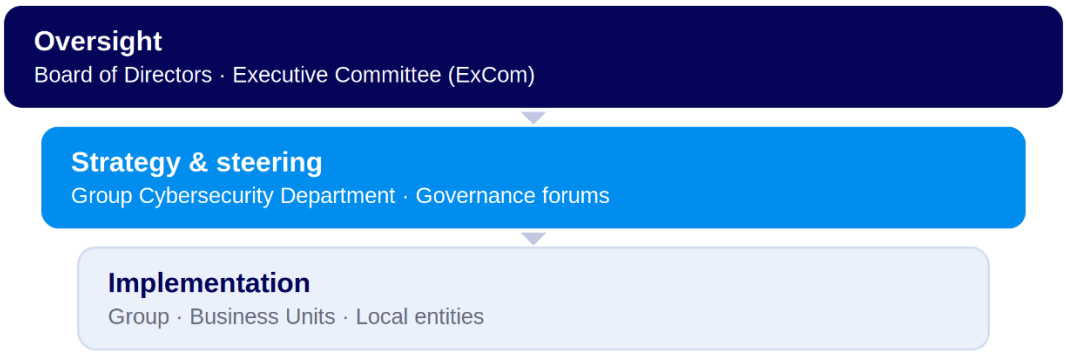

Figure 1 — Governance structured from Board of Directors down to local entities.

04 Cybersecurity Roles and Responsibilities

Information security responsibilities are formally defined and assigned across the entire workforce through FDJ UNITED's Group Information Systems Security Policy (GISSP) and cybersecurity governance framework. Clear roles and accountabilities are established at Group, Business Unit and entity levels, from Executive Management and cybersecurity leadership to local cybersecurity representatives.

Managers are responsible for enforcing security requirements, supporting awareness activities and ensuring compliance within their teams. Project managers integrate security and risk management into projects, while all employees are required to comply with security policies, participate in awareness programs and promptly report suspected security incidents.

05 A Structured and Auditable Security Framework

FDJ UNITED's cybersecurity program is based on a structured control framework inspired by internationally recognized standards (including ISO 27001 and the NIST Cybersecurity Framework) as well as applicable regulatory requirements.

This framework establishes common security principles across all Group entities, including:

- A risk-based approach supported by continuous improvement, particularly through our Information Security Management Systems;
- Protection of information systems and sensitive data;
- Compliance with applicable regulations and industry standards;
- Implementation of security controls commensurate with risk and criticality levels.

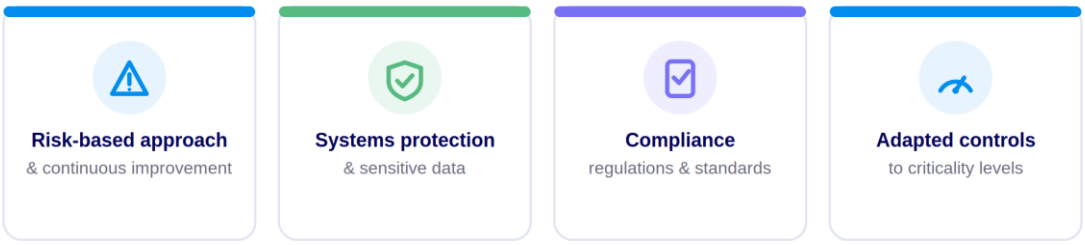

Figure 2 — The four founding principles of the security framework.

These principles are implemented through policies, procedures, and operational controls covering, among others:

- Protection and integrity of player and business data;
- Secure and responsible use of Artificial Intelligence;
- Identity, access, and privileged access management (IAM/PAM);
- Vulnerability, patch, and incident management;
- Cyber incident and crisis management;
- Security exception management;
- Security awareness and training programs.

06 A Proactive Approach to Emerging Risks

FDJ UNITED fully integrates risks associated with technological evolution and emerging digital practices into its cybersecurity strategy.

The Group relies on key guiding principles to govern the adoption of emerging technologies, including:

- Prior risk assessments before deployment;
- Controlled and supervised use of automated systems;
- Enhanced protection of sensitive information;
- Management of technology dependencies with a focus on sovereignty and resilience.

This approach enables FDJ UNITED to balance innovation with effective risk management in a rapidly evolving environment.

07 Strengthened Governance and Support for Artificial Intelligence

FDJ UNITED applies specific governance measures to the use of Artificial Intelligence, recognizing both the opportunities and risks associated with these technologies.

AI governance is built upon clear principles relating to security, data protection, ethics, and regulatory compliance, embedded within dedicated governance mechanisms. Use cases are subject to risk assessments proportionate to their business and technological impact.

In addition, the Cybersecurity Department supports AI-enabled projects throughout their lifecycle, with the objective of embedding security by design from the earliest stages. This support aims to balance innovation, risk management, and alignment with Group requirements.

08 Continuous Detection and Response Capabilities

FDJ UNITED relies on its Security Operations Centers (SOCs) to provide continuous monitoring of information systems and to detect, analyze, and respond to security events and incidents. Cybersecurity monitoring, threat detection, and incident response activities are centralized at the Group level.

These monitoring capabilities contribute to the protection of information systems, the reduction of compromise risks, the mitigation of incident impacts, and the strengthening of the organization's resilience against cyber threats.

09 A Three Lines of Defense Control Model

Our control environment is structured according to the Three Lines of Defense model: operational teams integrate security into their day-to-day activities; the Cybersecurity Department defines security requirements, supports business entities, and controls compliance; Internal Audit performs independent assessments of our security posture.

Figure 3 — The Three Lines of Defense model.

This approach is complemented by regular penetration testing, Red Team, cyber crisis exercises, and external maturity assessments.

10 Cybersecurity Is Everyone's Responsibility

Cybersecurity depends on the commitment of every employee. FDJ UNITED deploys awareness and training programs tailored to different business functions to promote best practices and strengthen the security culture throughout the organization.

These initiatives include an annual security awareness program, phishing simulation campaigns, and dedicated events designed to empower employees to actively contribute to cybersecurity.

11 Supplier Relationship Security

FDJ UNITED applies a risk-based approach to third-party cybersecurity management. Security requirements are defined during supplier onboarding through cybersecurity assessments and contractual security clauses. Critical suppliers are identified through a formal segmentation process and are subject to enhanced monitoring, including periodic reviews, audits and remediation follow-up. These requirements are maintained and reassessed throughout the supplier lifecycle to ensure alignment with the Group's cybersecurity standards.

12 A Commitment to the Wider Cybersecurity Ecosystem

FDJ UNITED actively contributes to the cybersecurity ecosystem through collaboration with competent authorities, industry organizations, and professional communities, while supporting the development of cybersecurity skills and talent.

Through this commitment, the Group aims to help strengthen security standards across its ecosystem, especially for small and medium-sized enterprises (SMEs).

In this context, FDJ UNITED actively participates in industry initiatives and collaborative networks such as **Campus Cyber** (National and Euromed), contributing to information sharing, cybersecurity working group, best practices, and peer cooperation.

The Group also supports initiatives promoting diversity and inclusion in cybersecurity, notably through its engagement with **CEFCYS** (CErcle des Femmes de la CYberSécurité).