Information Security Statement

version 1.1

Approved by the CTO on August 7th, 2025

Commitment

At P3 Parks Logistics we recognize that information security is fundamental to earning and maintaining the trust of our clients, employees and partners. We are committed to protecting the confidentiality, integrity and availability of all information assets under our care and to meeting the requirements of the EU NIS2 Directive and Luxembourg implementing law.
Overall accountability rests with the Chief Information Security Officer (CISO) and Chief Technology Officer (CTO), who reports quarterly KPIs to the Audit & Risk Committee. Adequate financial and human resources are allocated to maintain effective defences.

Scope

Our information security standards apply to all employees, contractors and external partners and to any environments we manage on behalf of our clients.

Our Security Objectives

We pursue a proactive, systematic approach to information security based on GDPR regulation, EU standards and best practices, and the Cybersecurity Capability Maturity Model (C2M2).

Our key objectives include:

- 100% of P3 Network and Server assets covered by Vulnerability Management
- Vulnerability Response plan KPI: Critical < 7 days, High < 14 days.
- Vulnerability Remediation KPI: Critical < 30 days, High < 45 days
- Protecting both company and client data from unauthorized access, alteration, or destruction
- Continuously identifying, evaluating, and mitigating security risks
- Conducting regular internal security audits
- Preventing and detecting security incidents, with response and mitigation
- Complying with all applicable laws, regulations, and contractual obligations
- Preserving the reputation and trustworthiness of our organization and services
- Ensuring we remain a strong and reliable partner to our clients

People and Responsibility

Security is everyone's job. We, therefore:

- Educate our employees and partners about their security responsibilities (via security-specific trainings, phishing campaigns, newsletters, info emails etc)
- Apply consistent policies globally across our teams, contractors, and service providers
- Require third-party partners to meet the same standards we enforce internally

Reporting Security Concerns

We encourage all employees and partners to report of any suspected security issues. Local Security Managers escalate incidents to the Chief Information Security Officer (CISO).
Any vulnerability is to be reported via security@p3parks.com; we commit to acknowledging all the reports and resolve the valid findings in a timely manner.

Related Policies

(available upon request)

- Data Classification Policy
- Acceptable Use of IT
- IT-Asset Management Policy
- AI Governance Policy

Continuous Improvement

Our security roadmap is reviewed at least annually and updated to align with evolving threats, new regulations, and lessons learned from incidents.