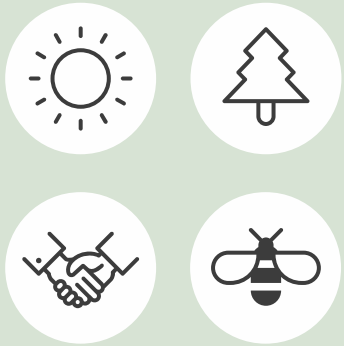
Group Cybersecurity Policy



Effective date : 8.12.2025
Last modified: 8.12.2025
Approved: Richard Wilkinson, Group CFO

Introduction

CTP is a dynamic, fast-growing organisation with a fully integrated platform operating internationally, led by local management teams. Group level tasks are executed by CTP International. The whole organisation is led by Group Leadership Team. The proven expertise and comprehensive market intelligence of the CTP team form the core of our competitive advantage and our ability to provide shareholders with superior and sustainable returns.

The management of CTP recognizes the necessity to satisfy our customers overall needs. High standards and professionalism in this aspect assures the best quality, keeping us ahead of competitors and ensuring the continuous prosperity of the company. CTP regards environmental protection and energy management as not just a substantial part of our business philosophy but also a reflection of our attitude towards common values. Therefore, all business activities are conducted in an environment-friendly way. CTP collaborates with stakeholders within its value chain to achieve its goals.

CTP is exposed to a range of cyber risks. These might have material and reputational consequences. CTP is committed to identifying and managing these risks in line with the best international practices and regulations in the countries where it operates.

Scope

This policy pertains to all operations and activities of CTP N.V. and its subsidiaries. This includes all countries of operation. All employees and individuals working in the organisation's name must know and follow the content of this document.

Governance - Roles & Responsibilities

The Board of Directors is ultimately responsible for integrating this policy into CTP operations and complying with this policy.

Cyber security Manager regularly leads the implementation of cybersecurity controls, coordinates incident response, ensures regulatory compliance, and reports to Group IT Director.

Cybersecurity Committee consists of Group IT Director, Internal Audit Director, Group AML Compliance Officer, IT Infrastructure Manager, Head of Risk Management, and Cyber security manager and report to Board during Audit Committees.

Country Heads are responsible for communicating this policy to their teams and ensuring local compliance.

IT & Asset Administrators maintain security infrastructure, implement remediation actions, and support forensic investigations.

Managed Security Service Provider provides 24/7 security monitoring, incident detection, and response.

Group Compliance Officer supports regulatory compliance and reporting.

All employees are required to follow security policies, report suspicious activities, and regularly participate in cybersecurity awareness training.

Furthermore, the Board of Directors is responsible for allocating the resources needed to comply with this policy and achieve the goals and targets aligned with the Cybersecurity topics of the company.

Core areas and actions

Compliance with European union Network and Information Security Directive (NIS2)

This group cybersecurity policy is adopted to align our organization with the NIS2 Directive by ensuring a high common level of security for our networks, information systems, and critical services across all entities. By implementing risk-based controls, clear incident reporting, and continuous improvement of our cyber resilience, we protect our operations, our customers, and the wider EU digital ecosystem from evolving cyber threats.

Risk Management & Assessment

CTP maintains a structured process to identify, assess, and mitigate cybersecurity risks. Risk assessments are conducted regularly and whenever significant changes occur in systems or business operations. Identified risks are prioritized and addressed through appropriate technical, administrative, and procedural controls. CTP conduct regular cybersecurity audits.

Access Control & Authentication

Access to systems and data follows the principle of least privilege. Strong authentication measures, including multi-factor authentication, are enforced for all critical systems. Privileged accounts are strictly managed, monitored, and reviewed periodically to prevent unauthorized access.

Asset & Data Classification

All information assets are inventoried and classified based on sensitivity and regulatory requirements. Data handling procedures ensure secure storage, transmission, and disposal of confidential and personal information. Employees must adhere to classification guidelines when accessing or sharing data.

Technical Controls & Monitoring

The company deploys industry-standard security technologies, including firewalls, intrusion detection systems, endpoint protection, and encryption. Continuous monitoring and centralized logging are implemented to detect anomalies and respond promptly to potential threats.

Incident Response & Management

A formal incident response plan governs the detection, reporting, and resolution of cybersecurity breaches. Employees must report suspected incidents immediately. The response team acts to contain, investigate, and remediate incidents while ensuring timely communication with stakeholders as required by law.

Business Continuity & Disaster Recovery

Regular backups of critical systems and data are maintained and tested to ensure recoverability. A disaster recovery plan outlines procedures for restoring operations following

a cyber event, minimizing business disruption and financial impact, ensuring business continuity.

Vendor & Third-Party Risk

All third-party providers with access to company systems or data must meet defined cybersecurity standards. Contracts include security obligations, and vendors are subject to periodic risk assessments to ensure compliance and resilience. Penetration tests are performed each year.

Employee Awareness & Training

Cybersecurity awareness training courses are mandatory for all employees and conducted regularly. Training covers phishing prevention, secure handling of data, and incident reporting. Employees are expected to remain vigilant and uphold the company's security standards in daily operations.

Continuous improvement

CTP follows the principles of continuous improvement, plan, do, check, act. This approach ensures the company remains flexible and prompt changes in development, technical evolution, changes in our customers' needs and expectations, and other business requirements. The Company adapts to these changes and applies new technologies and services accordingly.

Reporting noncompliance

To report noncompliance please send an email to: compliance@ctp.eu. For further guidance please visit: https://ctp.eu/ctp-policies/how-to-report-a-concern/