CYBER & INFORMATION SECURITY POLICY

Key Principles

Through this Policy and the objectives set forth below, Euronext is committed to ensuring the security of its information, as well as the security of all associated resources, whether procedural, technological, or human. Cyber and Information security is critical to the strategic success and business sustainability.

With this purpose InfoSec in cooperation with Risk and Compliance Department has established a framework that contains all the necessary requirements for the secure management of information and support systems, and which seeks to ensure, through an approach based on risk management and continuous improvement, the confidentiality, integrity, and availability of information. In addition, Euronext Group CISO is fully committed and oriented to delivery excellence recognized services that fits interested parties' legitimate expectations.

Safeguarding these pillars guarantees the preservation and improvement of cyber and information security strategy which enables the company to better preserve its image, reputation, and credibility, especially among regulators, partners, customers, and investors.

Purpose

This Policy defines the purpose, direction, principles, and objectives for managing information security and cyber risk in accordance with the Euronext business requirements but also with its interested parties' expectations and objectives.

This Policy is also a core component of the ICT Risk Management Framework ("ICT RMF"), which is implemented across Euronext Group to fully embed operational resilience across the organization.

Euronext is a major player in the European financial infrastructure, and it is mandatory to act with due diligence in what concerns the management of information security risks and prove the capability to delivery essential services in a safe and controlled way even in the occurrence of an incident without compromising the Confidentiality, Integrity, Availability, Authenticity and Traceability of information.

To protect and enable Euronext business, InfoSec relies on well-known framework based on a risk management approach to allow Euronext group to be confident in the preservation of reputation ensuring compliance with all legal, regulatory, contractual requirements and Euronext internal policies.

Related Standards

This policy is supported and enforced via the implementation of specific and more detailed cyber and information security standards specifying mandatory requirements, more detailed objectives and practices, aligned with ISO 27001:2022 operational capabilities, to ensure the required secure control environment and security posture at Euronext Group and at Company levels.

1) Application Security

This standard outlines the minimum-security activities that are required during the development of software systems to protect Euronext Group ICT assets (including systems, applications, and infrastructure) against compromise of confidentiality, integrity, availability, authenticity and traceability. The application of the appropriate security measures will reduce the risk to ICT assets, thereby reducing the overall risk of the Group.

This standard sets the boundaries for strengthening the operational resilience and readiness of projects implementation within Euronext.

This standard also covers the Release Management process related to software and defines organizational expectations for addressing, controlling and reporting releases, until deliver.

2) Vulnerability Management

This standard outlines the security requirements associated with infrastructure vulnerability (vulnerabilities resulting on the automated scans performed by specific tools) and patch management to maintain the security of its information assets and ICT systems, protecting the Group, Users and all relevant stakeholders from cyber threats. To mitigate vulnerabilities, Euronext shall identify, acquire, install, and verify patches for its products and systems.

3) Information Protection

Classification of ICT Assets, i.e. assigning data to classes according to the severity of the associated information security risks in relation to confidentiality, integrity, availability, authenticity and traceability is a convenient and cost-effective way of determining the generic types of information security controls that are considered appropriate to protect data, including accurate and prompt data transmission controls. The information protection standard defines the levels of data classification, classification lifecycle and the respective baseline controls.

4) Identity and Access Management

This standard is the basis for implementing a suitably controlled User life cycle management process (IAM process), Access and Privilege Access Management, Password Management and Authentication and Authorization Management to ensure that only authorized Users/entities have access to Euronext's systems, in accordance with their functional role.

Identity and Access Management (IAM) security controls ensure access to ICT assets across the Group by clearly identifying 'who has access to what, when where and how', following successful authentication, thereby protecting the confidentiality, integrity, availability, authenticity and traceability of Euronext data.

5) Secure Configuration

The standard outlines the requirements regarding use of cryptographic systems/tools and algorithms and establishes rules in relation to cryptographic keys and key lifecycle management within Euronext.

In addition, the standard outlines the security requirements associated with logging and monitoring of security events within Group's systems and networks.

Lastly, this standard also defines the requirements for the cloud computing services independently of the approach, IaaS, PaaS, or SaaS, and states the requirements to be addressed with Cloud Service Providers (CSP), to ensure compliance with applicable legal and regulatory requirements with a mindset to reduce the cyber security risks raised by the adoption of cloud and ensuring the adequate controls are implemented.

6) Systems and Network Security

This standard outlines the security activities required to ensure the protection of information within our networks and the supporting information processing facilities, which must be managed and controlled to protect Euronext ICT assets. Security controls must be implemented to ensure the security of information in networks and the protection of connected services and disruption from unauthorised access.

7) Information and Communications Technology Incident Management

This standard defines the guidelines for incident identification and reporting, incident classification and prioritization as well as communication and coordination during the incident, along with the restoration of the normal service. It also highlights the process for post-incident reviews.

8) Cyber Security Crisis Management

This standard defines the key aspects of business continuity management, from the planning of information security continuity activities to their implementation and continued maintenance with regular tests and reviews.

9) Asset Management

This standard defines what an information asset is, how information assets relates with other supporting assets, and provides guidance about required controls that shall be implemented to protect those assets.

It also outlines the endpoint, mobile devices and remote connection security requirements that are needed to protect Euronext data and financial assets (including systems, applications, and infrastructure), against improper or unauthorized access, that could result in compromise of confidentiality, integrity, or availability of Euronext data.

10) Information and Communications Technology Risk Management

The ICT Risk Management Standard defines the organization’s risk management processes. This involves identifying critical assets, assessing the potential threats and vulnerabilities, and determining the impact of various risk scenarios.

11) Supplier Relationship Security

This standard documents the high-level requirements, roles, and responsibilities with respect to the protection of ICT assets belonging to Euronext and all its entities hereby referred to collectively as "Group" or "Euronext", its subsidiaries, and joint ventures in the context of risks introduced by arrangements with Third Party Service Providers.

12) Legal and Compliance

This standard describes the legal, statutory, regulatory and contractual requirements, independent review of information security and the compliance with policies, rules and standards for information security.

13) Human Resource Security

The aim of this standard is to ensure that Users understand their responsibilities and are suitable for the roles for which they are employed.

14) Physical Security

The purpose of this standard is to outline the security requirements regarding physical access management to be adhered to prevent unauthorized physical access, damage and interference to Euronext information and information processing facilities.

15) Acceptable Use

This standard establish what is deemed of acceptable use by Users (employees and contractors) of Euronext's information systems and ICT assets. By implementing acceptable use standard statements, Euronext aims to limit its risk from inappropriate User's activity.

Euronext Infosec demonstrates the commitment also in the URD document, and applies what is written in the compliance policies as: Euronext NV Code of business conduct and ethics, Anti-Fraud Policy, Conflicts of Interest Policy and Confidential and Inside Information Policy. In case of doubts and clarification the compliance policies should be used.

16) Change Management

This standard communicates management intent that all changes are managed in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation.

17) Problem Management

Problem Management standard communicates management intent to identify and classify problems and their root causes, to identify validated workarounds and permanent fixes.

Additionally, this standard communicates the requirement to provide timely resolution to prevent recurring incidents and to provide recommendations for improvements.