CYBERSECURITY POLICY

Abstract

January 2022

EURAZEO

CYBERSECURITY POLICY
ABSTRACT

I. PREAMBLE

A. Scope

This Cybersecurity policy abstract applies to Eurazeo SE, Eurazeo Mid-Cap, Eurazeo Investment Manager, Eurazeo Funds Management Luxembourg, Eurazeo Infrastructure Partners and their wholly owned subsidiaries, herein referred to as "Eurazeo".

B. Purpose and process

Cybersecurity is a major stake at Eurazeo and thus a comprehensive strategy has been deployed to mitigate this growing risk both for Eurazeo and its portfolio companies. This document is an abstract of the detailed Cybersecurity Policy and sets out its key points.

C. Availability and governance

This Cybersecurity policy abstract is publicly available on Eurazeo's website and internally accessible on Eurazeo's intranet. The detailed Cybersecurity Policy has been approved by the Executive Board. For any information concerning the Cybersecurity Policy, please send a request at ITsecurity@eurazeo.com.

II. CYBERSECURITY GOVERNANCE AND ORGANISATION

- The first formalised **Cybersecurity Policy** for the Eurazeo Group has been established in 2018 and is reviewed on a regular basis.
- A **Digital Security Committee** is held at least twice a year. The committee is chaired by a member of the Executive Board and is composed of the CDO, the CRO, the CSO, the CIO, and the EIM COO.
- This committee is responsible for ensuring **strategic alignment** in terms of cybersecurity and monitoring the implementation of cybersecurity action plans.

- A cybersecurity review is done on every Eurazeo **Audit Committee Meeting**.
- The Cybersecurity Policy is operationally implemented by **a dedicated cybersecurity specialist and best-in-class subcontractors** .

III. EXTERNAL AUDITS AND PENETRATION TESTING

- **360° IT security audits** (including penetration testing, servers, laptops & smartphones configurations reviews, internal procedures reviews, etc …) are conducted every two years.
- Ad hoc **cybersecurity reviews** of applications configurations are triggered at implementation time and on a regular basis.

IV. PERSONNEL TRAINING AND AWARENESS

Personnel are the first level of defence against many cyberattacks therefore Eurazeo takes their training very seriously:

- A yearly mandatory online cybersecurity training for all Eurazeo personnel is deployed.
- Continuous phishing campaigns.
- Ad-hoc cybersecurity communication campaigns on specific projects

V. CYBERSECURITY SOLUTIONS AND PROCESSES

To prevent cyberattacks Eurazeo has implemented technical solutions as well as robust processes:

- Traditional firewalls, internet proxy, network access control, antivirus and VPN solutions have been deployed.
- Multi factor authentication is deployed on all critical applications.
- All user's end points (laptops, smartphones) are centrally managed using a state of-the art mobile device management solution.
- Data leak detection solution.
- Rigorous change and patch management processes have been implemented and annual privileged accounts reviews are done.

VI. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

To be able to guarantee business continuity, in case of a successful cyberattack, Eurazeo has deployed a full disaster recovery plan based on:

- A distant secondary datacentre that allows replication of all "on premise" systems.
- Contractually agreed Saas solutions recovery plans with SaaS providers.
- A 3-2-1 back up policy (3 copies of data, 2 different media, 1 off site).
- A Computer Emergency Response Team contract in place with i-Tracing.
- All employees are enabled to work remotely from home.

The disaster recovery plan is tested once a year.

VII. CYBERSECURITY PROGRAM FOR PORTFOLIO COMPANIES

Eurazeo has developed a cybersecurity program for its portfolio companies :

- Initial assessment of cybersecurity governance and practices vs cybersecurity exposure and risks.
- Measurement of the company's overall performance in cybersecurity, through a safety and security profile analysis, observable from the Internet using publicly available information.
- Planning of a 360° IT security audit within 100 days, if no recent audit exists (IT security organization, processes review, systems and endpoints configuration reviews, specific application security reviews and pen testing).
- Access to Eurazeo CIO / CTO / CISO community for best practises and solution sharing.
- Organization of regular events dedicated to cybersecurity (events & webinars).
- Eurazeo group contracts and solutions: data leak solution (Cybelangel), Computer Emergency Response Team access (i-Tracing), Security rating platform, Cybersecurity expert access.
- Follow up of cybersecurity roadmap during companies' audit committee.
- Biannual reporting of major cybersecurity events.

DISCLAIMER

Completed in January 2022.

This document has been prepared by Eurazeo and/or its partners and is intended solely for the recipient. It is for information purposes only and should in no way be construed as a solicitation or an offer to buy or sell financial instruments, nor as legal, tax or financial or any other kind of advice. No investment decisions should be based solely on the information contained in this document. This document has not been approved by a regulatory body. Recipients are encouraged to contact their own advisers for an analysis of any information contained in this document. The information presented does not purport to be exhaustive relative to the recipient's requirements.

This document was prepared as of the date shown using public information, information provided by the recipient, data owned by Eurazeo and information protected by confidentiality laws. Eurazeo takes the greatest care to ensure the quality of the information supplied. However, this information is not guaranteed by Eurazeo and is subject to change at any time without prior notice. None of the information in this document should be considered as a promise, commitment or past or future representation.

All projections, assessments, statistics, surveys, analyses, and quantitative information contained in this document involve subjective assessments for which Eurazeo may not be held liable. Past performance is not an indicator of future performance.

Any reproduction or dissemination, whether in full or in part, without prior written authorization from Eurazeo is strictly prohibited. Eurazeo may not be held liable for any unauthorized use of this document by a third party.