FXopen

when money makes money

Information Security Policy

v1 – November 2023

FXOpen EU Ltd is authorized and regulated by the Cyprus Securities and Exchange Commission (CySEC) under license number 194/13.

INFORMATION SECURITY POLICY

The Board of Directors and Management of FXOpen EU Ltd, which is investment firm situated at Spyrou Kyprianou 38, CCS Building, Office 101, 4154, Limassol, Cyprus, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets, including personally identifiable information (PII), throughout the organization in order to preserve its information security, legal, regulatory and contractual compliance, privacy of data, and commercial image.

Information, privacy and information security requirements will continue to be aligned with FXOpen EU Ltd goals, and the information security management system (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information- and privacy-related risks to acceptable levels.

This ISMS applies to the provision of Investment and Ancillary Services to customers of FXOpen EU Ltd, in accordance with the ISMS Statement of Applicability version 1, dated on 20th of November 2023, and FXOpen EU Ltd has adjusted the exclusions under this Statement and do not comprise the integrity of the ISMS.

FXOpen EU Ltd is committed to ensuring compliance with all applicable legislative, regulatory and contractual requirements, including all applicable PII protection legislation.

FXOpen EU Ltd current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information- and privacy-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information- and privacy-related risks are controlled. The Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and criminal hackers, access control to systems, and information security and privacy incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the InfoSec Manual and supported by specific documented policies and procedures.

FXOpen EU Ltd aims to achieve specific, defined information security and privacy objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees/Staff of FXOpen EU Ltd and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, and certain external parties, will receive appropriate training. The consequences of breaching the information security and privacy policies are set out in FXOpen EU Ltd disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

FXOpen EU Ltd has established an Information Security Steering Committee, chaired by the Chief Information Security Officer (CISO), and including the Risk Manager/Executive and Head of AML/Compliance Department to support the ISMS framework and to periodically review the security policy.

FXOpen EU Ltd is committed to achieving certification of its ISMS to ISO accredited certification by Q4 2024 and compliance with CySEC Circular 571.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full- or part-time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, responsibilities (which are defined in their job descriptions or contracts) to preserve information security and privacy, to report security and privacy breaches (in line with the policy and procedures identified in the Information Security Manual) and to act in accordance with the requirements of the ISMS. All Employees/Staff will receive information security and privacy awareness training, and more specialised Employees/Staff will receive appropriately specialised information and privacy security training.

the confidentiality,

This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorized access to FXOpen EU Ltd information and its systems related to the trading platforms, client accounts, and associated financial transactions.

integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for networks and website, and data backup plans along with security and privacy incident reporting. FXOpen EU Ltd must comply with all relevant data- and privacy-related legislation in the jurisdiction within which it operates.

and availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and FXOpen EU Ltd must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. Therefore, there must be a regular vulnerability assessment, appropriate encryption protocols and business continuity plans.

of the physical (assets)

The physical assets of FXOpen EU Ltd, including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information (whether PII or otherwise) printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.) of FXOpen EU Ltd.

FXOpen EU Ltd and its partners that are part of its integrated network, have signed up to its information security and privacy policy and have accepted its ISMS.

The **ISMS** is the information security management system, of which this policy (the Information Security Manual) and other supporting and related documentation are a part, and which has been designed in accordance with the specifications contained in ISO 27001:2022.

A **security breach** is any incident or activity that causes, or may cause, a breakdown in the confidentiality, integrity or availability of the physical or electronic information assets of FXOpen EU Ltd.

A **privacy breach** is any incident or activity that causes, or may cause, a breakdown in the confidentiality, integrity or availability of the PII assets of FXOpen EU Ltd.