HF Markets

HF Markets (Europe) Ltd

Address: Office 601, Nicolaides Shopping City, Angelos Court,
84 Spyrou Kyprianou Avenue & Papanikoli, 6052 Larnaca, Cyprus
T: +357 24400165 F: +357 24023093 E: info@hfeu.com W: www.hfeu.com

HF Markets (Europe) Ltd

INFORMATION SECURITY POLICY

Table of Contents

1. Introduction

1.1. This Information Security Policy (hereinafter the "Policy") safeguards the confidentiality, integrity, and availability of HF Markets (Europe) Ltd (hereinafter the "Company") information assets. It defines the approach for managing security risks and ensures the effective operation of business processes, particularly in response to disruptions, technology failures, and incidents.

1.2. The Company has appointed an Information Security Officer (ISO) to oversee security posture, compliance, and incident response management.

1.3. Roles and responsibilities are clearly defined for all personnel involved in managing information security, ensuring an effective governance structure. Senior management is committed to allocating adequate resources for security initiatives and continuously strengthening the security framework.

2. Risk Management Framework

2.1. The Company maintains a structured risk management framework that continuously assesses, mitigates, and monitors risks impacting information systems and services. Regular risk assessments identify emerging threats and vulnerabilities, with appropriate mitigation measures implemented. The Company keeps an up-to-date inventory of critical information systems, applications, and services, prioritizing those essential for ongoing operations.

2.2. A formal incident management process is in place to promptly identify, respond to, and recover from security incidents. Employees are required to report suspected or actual security incidents to designated personnel. The Company investigates incidents, identifies root causes, and implements corrective actions to prevent recurrence. Incident response plans are regularly tested and updated to ensure preparedness for various potential disruptions.

2.3. The Company retains ultimate responsibility for fulfilling all incident reporting requirements, ensuring that all relevant stakeholders, including regulatory bodies, are notified as necessary. This includes ensuring that internal and external reporting protocols are followed,

and that incidents are communicated promptly and accurately, in compliance with applicable regulations and organizational policies.

3. Third party contractors

3.1. The Company ensures that third-party service providers, partners, or vendors adhere to security and operational resilience standards as outlined in their contracts. Vendor risk assessments evaluate third-party risks, including those related to security, availability, and business continuity. Periodic reviews of third-party relationships ensure that security measures align with organizational and regulatory expectations. The Company retains ultimate responsibility for ensuring that third parties adhere to these standards.

4. Business Continuity Plan

4.1. The Company implements a Business Continuity Plan (BCP) program to ensure critical operations continue during disruptions. A Disaster Recovery Plan (DRP) outlines procedures for recovering information systems and services within predefined recovery time objectives (RTOs) and recovery point objectives (RPOs). Both the BCP and DRP undergo regular testing to verify their effectiveness and ensure that The Company can respond effectively to various disruption scenarios.

5. Security measures implemented

5.1. Sensitive data, including personally identifiable information (PII) and financial data, is protected through encryption, access control, and other appropriate security measures. The Company defines data retention policies to specify how long data will be stored and when it will be securely deleted. Employees and contractors receive training on data protection principles to ensure compliance with applicable data privacy regulations. Information systems are continuously monitored to detect unauthorized access, security breaches, and anomalous activity. Security testing, including penetration testing and vulnerability assessments, is regularly conducted to identify potential weaknesses. Logs and audit trails are maintained for all critical systems to facilitate monitoring and incident investigation.

6. Internal and External Audits

6.1. The Company conducts regular internal and external audits to ensure compliance with this Policy and applicable laws and regulations. Mechanisms for monitoring and enforcing security standards are in place, and deficiencies are promptly addressed. Compliance with security policies is evaluated through periodic reviews, with corrective actions taken as necessary.

6.2. Regular security training and awareness programs are conducted for all employees to emphasize the importance of security and safe practices. Specialized training is provided to individuals in sensitive roles, ensuring they understand the specific risks and security measures relevant to their duties.

6.3. This Policy undergoes an annual review or is updated whenever there is a significant change to Company's' operational environment or regulatory requirements. Updates are communicated to all relevant stakeholders.

7. Compliance responsibility

7.1. The Company retains full responsibility for ensuring compliance with all relevant local, national, and international regulations, standards, and legal requirements applicable to the security, confidentiality, and integrity of its data and systems. This includes, but is not limited to, financial regulations, data protection laws, industry standards, and regulatory compliance frameworks. The Company will continuously monitor regulatory changes and adapt its information security measures accordingly to maintain compliance with applicable laws and regulations.

8. Enquiries and Contact Details

8.1. For any general enquiries regarding this Policy please contact the Company by emailing the Customer Support Department at support@hfeu.com.

Version: 2025/02