SECURITY

Information Security Controls Overview

At eMoney, our mission is to revolutionize the way trusted advisors serve the needs of their clients. We help them succeed by providing knowledge, systems, and tools to support the “next generation” of trusted advisors. We realize that fulfilling this mission requires constant attention to the security of our clients’ information. eMoney has designed and implemented a robust information security program intended to ensure the confidentiality, integrity, and availability of this information. This overview provides information regarding security practices and controls we employ to ensure that data is safe and secure.

Governance, oversight & policies

We maintain a robust and comprehensive set of Formal Security policies including, but not limited to:

- Access control
- Privacy and confidential information handling
- Encryption
- Security incident management
- Secure development life-cycle
- Awareness and education
- Vendor oversight
- Business continuity and disaster recovery

These policies are reviewed by the eMoney Executive Team on a regular basis to ensure that they address the latest technological advances, trends, and changes in the threat landscape.

Secure development practices

The eMoney platform was developed and is administrated internally. We maintain a robust set of practices for our application development process and various data environments. Important elements of our development process include:

- Physical and logical separation of development, testing, and production environment
- Manual and automated code analysis
- Restricted physical and logical access to the production environment
- Penetration and code analysis scans conducted internally and externally
- A formal change management process to systematically manage any platform changes
- Access to production servers and databases regularly audited and reviewed by management
- No use of shared or generic IDs. Each individual is uniquely identified and accountable for actions that occur within their ID.

Human resources & access control

Information Security and Human Resources coordinate to ensure that security processes related to both areas work together effectively and efficiently.

- As a requirement for employment, all employees submit to a background check. This process includes employment verification, criminal and credit checks, and drug screening.
- Every employee is required to participate in security awareness training upon hire and annually thereafter.
- All eMoney employees are required to confirm their understanding and acceptance of a non disclosure agreement and eMoney’s formal policies.
- eMoney has implemented a formal security incident response plan to respond appropriately to any suspected incidents. All eMoney staff are trained to identify and properly report any suspected breach of confidential information.

eMoney

Data leakage control

eMoney has several controls in place to mitigate the potential for sensitive data leakage from the corporate environment. These include:

- Solutions to control and prevent unauthorized access, enforce restriction of removable media such as USBs, and to detect or prevent the transmission of sensitive data.
- Data is encrypted at rest and in transit, as well as encryption of all end-point devices using the AES 256-bit standard encryption.

Vendor oversight

We conduct security due diligence on all third parties. Third parties that have access to sensitive information are considered high-risk and are assessed annually.

Third-party validation

- We use third-party providers to validate security controls. eMoney Advisor conducts annual penetration testing as well as annual Web/ Application Security Assessments.
- eMoney completes an annual SOC2:Type2 Assessment and received a clean opinion for this testing period (since 2014).

Infrastructure controls

Infrastructure devices are the backbone of any corporate network, and we have controls in place to help protect this vital part of our network.

- The eMoney platform offers a 99.5% availability with a 24 hour Recovery Time Objective (RTO) and a 4 hour Recovery Point Objective (RPO).
- eMoney maintains a formal Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). eMoney's DRP and BCP are validated by management and tested annually.
- The eMoney platform is continuously monitored for security and availability.

Effective information security controls naturally evolve over time. With the layers of controls discussed in this document, we feel confident that we successfully address today's threat landscape.

Good security is a shared responsibility and often involves coordination and cooperation among organizations. We look forward to working with other organizations and customers as we strive to grow our business and fulfill our mission.