

INFORMATION SECURITY CONTROLS OVERVIEW

The mission of eMoney Advisor, LLC (eMoney) is to revolutionize the way trusted advisors serve the needs of their clients and enable them to succeed; to provide 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 users’ information. eMoney has designed and implemented a robust information security program designed to ensure the confidentiality, availability and integrity of this information. This commitment to information security and privacy is one of our core values.

This document includes additional information on the following topics:

- **Corporate Governance, Oversight & Policies**
- **Application Development Process**
- **Human Resources and Change Management/Access Control**
- **Data Leakage Controls**
- **Infrastructure Controls**
- **Back Up Security and Business Continuity**
- **Physical Security - Data Centers**
- **Third Party Oversight**
- **Third-Party Audits**

This overview provides information regarding security practices and controls at eMoney to ensure that data is safe and secure.

Non-Transactional

eMoney360 Pro is a non-transactional application. Funds cannot be moved, withdrawn or accessed utilizing the software.

CORPORATE GOVERNANCE, OVERSIGHT & POLICIES

The Chief Technology Officer has the primary responsibility of ensuring that technology operations, security controls and policies are in place and function effectively to protect user information. eMoney maintains a robust and comprehensive IT Security policy. This policy addresses various areas, including, but not limited to:

- Roles and Responsibilities
- Account Termination
- Use of Passwords
- Access and Handling of Confidential Information
- Remote Access and Encryption
- Security Breach Handling
- Change Management
- Awareness and Education

These policies are reviewed by management on a regular basis to ensure that they are responsive to technological advances and trends and changes in the threat landscape.

APPLICATION DEVELOPMENT PRACTICES

eMoney maintains a robust set of practices around its application development process and various data environments. eMoney360/360 Pro is developed internally by eMoney application development professionals. Additional important elements of our development process include:

- Development, testing and production environments are physically separated from each other to avoid potential negative impacts to the production environment.
- Both manual and automated code reviews are in place to provide additional analysis and appraisal of new code or changes to existing code to minimize unintended consequences or coding errors.
- eMoney development professionals do not have general access to the production environment. Access to this environment is restricted with procedures in place for emergency access in the event an urgent situation arises where such access is required for a limited period of time.
- Audit reports of access rights to our production environment are produced and reviewed by appropriate management.
- A change management process is in place to effectively manage any required changes and/or updates to the production environment. Requests are placed into a change ticket requiring a description of the change, justification, back out plan, results of testing, proposed date of change, and other relevant information.
- Any changes or updates to our applications are tested by our Quality Assurance staff. This testing is performed as part of a comprehensive testing process that includes detailed use cases, testing procedures, expected outcomes, documentation requirements and formal acceptance and approval prior to implementation into the production environment.
- Administrative entitlements to production servers and databases are audited and reviewed by management on a regular basis.
- Shared and generic ID's are prohibited. Each individual is uniquely identified and accountable for actions that occur with their ID.
- eMoney's standard practice is to mask all user data in the test and development environments.
- All data at eMoney is encrypted while in transit and highly sensitive data is encrypted at rest within the database. eMoney utilizes 256-bit standard encryption.

HUMAN RESOURCES AND CHANGE MANAGEMENT/ACCESS CONTROL

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

- New hires, employee terminations and changes are tracked via a ticketing system. This system includes requests for the provisioning of office hardware and devices (ID, desktop computer, phones, etc.) and software access (email, CRM access, etc.) to ensure that employees maintain appropriate levels of access necessary for their specific roles within the organization.
- Every employee is required to participate in specialized training upon hire. This computer-based system includes Security Awareness, Customer Information Guidelines and Global Privacy training. Completion of this training is required and tracked until complete.
- All employees are provided unique ID's. Per policy and security training they are instructed never to share their passwords or write them down.
- All eMoney employees are required to confirm their understanding and acceptance of prohibited and appropriate uses of confidential information.
- As a requirement for employment all employees submit to a background check process. This process includes employment verification, criminal and credit checks and the right for eMoney to perform drug tests.

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 administer and control access to removable media such as USB's. Access is restricted by default with a robust request process for needs-based exceptions.
- Solutions to protect against sensitive user information being sent out via the eMoney corporate email system. Messages with potentially sensitive information are quarantined and alerts are provided to the original sender and/or appropriate management for message review.
- Remote desktop access into the eMoney corporate network is restricted to encrypted corporate-owned devices only. 2-factor authentication is required for remote access.
- Personal mobile devices are not allowed to connect to eMoney corporate email systems without installing a mobile application that secures this access with encryption and password protection.

INFRASTRUCTURE CONTROLS

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

- Infrastructure device and application patches are monitored via an automated process. Once new patches are made available, a standardized process is in place to assess, test, approve, apply and track their application within an appropriate timeframe.
- All data transmissions to and from eMoney servers are completed securely via SSL or other encryption.
- Data at eMoney is encrypted while in transit and highly sensitive data is encrypted at rest within the database. eMoney utilizes 256-bit standard encryption.
- eMoney laptops are encrypted using Checkpoint PGP encryption.
- Windows desktop systems and servers are secured with up-to-date enterprise anti-virus/malware protection. Systems are administered via an administrative console and signatures are updated regularly.
- Automated tools are in place to monitor for unauthorized wireless access points. This tool provides automated email alerts to appropriate management.
- The production network is monitored and policed for intrusion attempts 24 hours a day, 7 days a week. Any detected intrusion attempts are analyzed to determine the identity of the intruders and the extent of the intrusion.
- A robust security incident response plan is in place to respond appropriately to any suspected breach. This includes identification, assessment, remediation, resolution and, if necessary, notification. All eMoney staff are provided training in how to identify and properly report any suspected breach of confidential information.

BACK UP SECURITY AND BUSINESS CONTINUITY

- Secure, encrypted data back ups are completed electronically from our primary to our secondary data centers.
- A robust Business Continuity policy is in place and tested on an annual basis. This includes separate disaster recovery and business continuity testing.
- Specific RTO's and RPO's are in place.
- Iron Mountain is utilized for secure destruction of electronic assets. Hard copy paper assets are secured in locked bins and destroyed leveraging industry compliant 3rd party partners in the office environment utilizing cross-cut shredders.

PHYSICAL SECURITY - DATA CENTERS

- eMoney houses user data with SunGard Data Systems, a server hosting space offering the most secure environment in the industry. SunGard hosts 70% of all financial industry transactions.
- Physical access at SunGard's world-class hosting server centers is limited to authorized personnel, and requires multiple levels of authentication, including fingerprint scanning. SunGard Data Systems also makes use of fire protection, electronic shielding, database backups and more to ensure your data is protected.
- Security personnel monitor the system 24 hours a day. Access to servers requires multiple levels of authentication, including biometrics (finger print scanning) procedures to enter the production hosting facility.
- eMoney restricts physical access to its equipment to a very select group of authorized personnel.
- SunGard personnel do not have logical access to any user information. SunGard staff has physical access only in the event of an emergency.
- At no time is any user information stored in the "Cloud".

THIRD-PARTY OVERSIGHT

eMoney utilizes a very limited number of third-party vendors. These include:

- Iron Mountain – Secure electronic asset destruction
- DBSi – Data center
- SunGard – Data center
- Xtium – Disaster recovery platform and hosting partner
- CashEdge – Data aggregator

Security due diligence is performed on all third-parties who may physically handle or have access to sensitive information.

In the event a user requests to aggregate information from an organization for which eMoney does not yet have an electronic connection, eMoney may leverage the connection of another third-party data aggregator. In this event, security due diligence is performed on any of these potential third-parties prior to utilization.

THIRD-PARTY AUDITS

- Application and Network infrastructure penetration tests are completed regularly by reputable external third-parties. These tests also include physical and application infrastructure that supports mobile connectivity.
- eMoney's comprehensive Wealth Management System, which includes eMoney360 Pro, is VeriSign certified to be hacker safe. Vulnerability scans are also completed against the website.
- eMoney is currently in the process of completing a SSAE-16 audit overseen by PwC. The anticipated completion of this audit is scheduled for 2014.

Effective information security controls naturally evolve over time. With the layers of controls discussed in this document we feel confident that we can successfully meet 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.