Enterprise Security Program

RPAG Technology

As a service provider it is essential to demonstrate adequate controls and safeguards are in place to protect data. RPAG recognizes this fact and as a result has made, and continues to make, significant investments into its technology infrastructure, processes, procedures and security.

RPAG performs regular audits to ensure compliance with a variety of business and regulatory requirements including an outside public entity auditing and ensuring RPAG's Sarbanes-Oxley compliance. In addition, RPAG regularly engages the services of independent third parties to perform security evaluations of our network, web/mobile applications, and login system.

At RPAG, we take data security seriously. We want you to feel comfortable that your data is secure. We welcome a follow up discussion with your IT team to further answer any questions or concerns you may have.

Human Resources Security

All RPAG staff certify their compliance with the RPAG IT Policy, which governs appropriate usage and affirms the importance of the confidentiality, integrity and availability of RPAG IT Systems. RPAG ensures all employees or third party contractors' access to information assets are suitable for their roles and that they understand their responsibilities at onboarding, during employment, while under contract and after termination. Controls include background checks, non-disclosure agreements, periodic access control reviews, audits, formal and informal training and an orderly termination process that includes return of assets and removal of access to information systems.

Information & Data Security

Mobile Device Full Disk Encryption

Full disk, BIOS level encryption is employed for all laptops and desktops.

PDA Security

All mobile devices connected to RPAG's Enterprise Email Platform are centrally managed via security policy. RPAG's mobile device security policy requires device encryption, password reset rotation and remote data wiping capabilities at minimum. RPAG's mobile device policy forces a locked screen after a period of inactivity and access is explicitly granted upon correctly entered request and device compliance verification.

Securing Documents and File Server

All file and document repositories are strictly secured by logical access control policies.

FTP transfers between RPAG and external firms are handled via SFTP or FTPS depending on the requirements of the firms themselves. Key management for these protocols is handled by internal RPAG staff.

Software Development Security

RPAG software development practices adhere to industry best practices and Sarbanes Oxley controls. RPAG's internal software development controls are audited by internal and third party auditors. RPAG staff employs industry leading tools for the development, issue tracking and resolution, testing, segregation of duties and source code integrity & control.

All changes to RPAG's websites and applications have penetration testing performed by internal developers prior to release to a production environment. In addition, all applications are tested by a third party to ensure code is secure from common hacking strategies.

Email Encryption

RPAG employs industry leading products and services for the encryption of emails in transit. RPAG employs automatic encryption and data leak prevention engines that screen and enforce security policy and the protection of Personally Identifiable Information.

Web Identity and Access Management & Dual Factor Authentication

RPAG employs an industry leading roles based Identity & Access Management suite of products along with Dual-Factor authentication for secured web-based control. Along with Dual-Factor authentication, RPAG employs a secure and robust self-service password reset mechanism. Password strength and expiration rules are managed centrally and adhere to RPAG's IT policy (NOTE: RPAG maintains and has a third party audit/review of the IT policy. It is overseen and enforced by RPAG's CIO and Chief Auditor).

User activity and access are logged and monitored per RPAG's IT Policy.

Redundancy and Disaster Recovery

RPAG engages a multi-step approach to achieving redundancy as well as disaster recovery. Critical systems are run in a high availability environment with no single points of failure. Data is stored securely and is backed up between the primary and secondary geographically disperse locations. In addition, backups are taken regularly and stored at an offsite secure location.

Both locations have remote work facilities established so that in the event of a disaster, employees have a secondary work location to continue to work and process business.

Database Security

System administration and database security is managed by internal RPAG staff. Applications requiring database access are given a SQL user account with limited access rights to the necessary databases. SQL accounts are bound by the same password policy as the Active Directory domain. Access to individual client data in a database is restricted by application role based security. Sensitive client data in the database is encrypted.

Encryption is utilized when needed to secure and access to these account credentials and keys is restricted to internal RPAG employees only.

Network Security

Intrusion Detection

RPAG leverages real-time threat and intrusion prevention services to monitor communication points on our webservers, externally facing applications and networks. Event management and monitoring is handled by a 24/7 offsite monitoring hosted service. The system monitors data transmission along the primary subnets. The sensors act as a vulnerability scanner that evaluates the current level of exposure associated with each device on the network.

The system's alarm monitoring uses threat-modeling which quantifies the type of attack by the potential vulnerability to determine the overall risk. If an alarm is generated, it will be investigated

by the operations center immediately to determine if the alarm is credible based on human intelligence. The responses to a positive alarm can include automatically shutting down the attack source switch port.

Internet Usage Monitoring & Control

All RPAG web based traffic is monitored, logged and filtered by a category based filtering device. Malicious and harmful sites are explicitly blocked.

Denial of Service Response (DoS)

DoS attacks are detected and prevented by use of RPAG's Intrusion Detection hosted service.

Wired Network Access Security

Physical and logical access controls are employed to restrict wired network access. All physical network device provisioning is governed by RPAG's IT Policy.

Password Management

RPAG complies with industry best practices for password complexity, expiration and rotation rules. Password management is handled centrally by approved administrative personnel for all accounts and adheres to RPAG's IT Policy.

Network Port Blocking Gateway

RPAG firewalls restrict data transmission to specific ports. Port and firewall rules are audited and follow a strict change control process for any approved updates. RPAG port and firewall security position is reviewed periodically by internal and third party auditors.

On an annual basis, RPAG goes through penetration testing by an outside security firm that leverages leading edge security and practical organizational defense mechanisms. The firm leverages both automated security tools as well as expert human assessments. All externally facing surfaces are tested for vulnerabilities. Material findings are reviewed by RPAG's executive team and issues are remediated immediately

Spam Filtering

RPAG's Spam filtering solution is consistent with the industry leaders within the financial services industry and has proven to be successful at providing filtering and control. This filtering monitors all incoming/outgoing emails to/from the organization.

Wireless Network Access Security

RPAG has several tiers of wireless access. All are encrypted and restricted to authorized users.

Physical & Environmental Security

Asset Management

Asset management is handled across multiple systems. RPAG has indexes of all hardware, software, replications and backups. RPAG's disaster recovery planning accounts for each of these areas.

Secure Equipment Disposal

All storage devices disposed of by RPAG are subject to a low level wipe to ensure the non-recoverability of the data. This includes drives and tapes.

Building Access

RPAG's buildings are accessible only with access badges or employee escort. In addition, data centers and network areas are only accessible with additional access badge checks or keys. All entrances are tracked into log files and reviewed as necessary.

Office Access

Offices that contain sensitive information are locked with individual keys. Individuals that access sensitive information have lockable file cabinets for document storage.

Office Surveillance

RPAG's offices are monitored by motion detector cameras. All ingress and egress locations are recorded.

Secure Office Areas

Certain areas that require additional security are within locked areas and are accessible only by those specific employees assigned to that department.