Piton Investment Management

IT Protections

Firewall – The perimeter is protected by a Cisco ASA (Adaptive Security Appliance) 5506-X firewall.

Outside Access – Only SSL VPN is allowed from the New York office. Access to all other servers are locked down on the firewall.

Antivirus – Centrally managed, enterprise grade antivirus (ESET) protects all endpoints.

Web Filtering – All web DNS requests are filtered by OpenDNS. OpenDNS protects against malware and botnets.

Data Protection – USB drives are blocked.

Patching – An enterprise grade patch management system is in place. Patching is done on a regular schedule (daily for workstations with alerts for workstations pending a reboot, monthly for servers) via a pre-configured whitelist of acceptable patches. In addition, the system allows for expedited rollout of critical patches and the ability to quickly audit which machines have, or are lacking particular patches.

Password and Account Management – All users have unique user accounts. There is a minimum password length of eight characters, password complexity is required, password history is enforced and passwords must be changed every 90 days. Screen Saver lockout is configured for 15 minutes of idle time. Password and account policies are maintained centrally through Active Directory.

Administrator Remote Access – Remote access for administrators (Proactive Technologies) is done through a secure system with SSL encryption. All administrators have unique logins to the remote administration system and all remote administration access is logged and time stamped.

Monitoring Software – Monitoring software (Automate) is installed on all servers and workstations to monitor for software and hardware failure.

Backups – Multiple daily backups protect against ransomware and other corruptions. Full image backups are taken every 15 minutes and changes are sent offsite on a nightly basis. Multi-year retention is maintained both onsite and offsite. All backups are encrypted both onsite and offsite and the encryption keys are available only to Proactive Technologies. Backups are monitored daily by Proactive Technologies and tested periodically.

Messaging Retention – Email messages will be maintained in a searchable WORM format for 6 years by Global Relay.

Shares and Permissions – File permissions are maintained centrally through Active Directory.

Disaster Recovery – Files and Active Directory will be replicated in real time to Proactive's private cloud at a Sungard data center in Philadelphia, PA. Email is a full featured hosted Exchange hosted by

Intermedia. The Disaster Recovery plan is documented and is tested annually with documented test results.

Asset Management – Proactive's monitoring systems can produce on demand inventories of server and desktop hardware and software. Proactive manually maintains and inventory for other critical systems such as networking equipment and telecommunications services. Additionally, Proactive maintains a client runbook that includes a network diagram and inventories of critical systems and vendors.

Physical Security – Piton's office and IT room are protected by a keylock system. Access to the IT room requires a separate key from general office access. Circulation of this key is tightly controlled. The IT room door is locked at all times.

Wireless Network - Piton maintains a separate wireless network for guest access.