Appleton Answers: How We Protect Your Data

APPLETON PARTNERS, INC.

Data Security Protocols

Data breaches that compromise individual and corporate data are an unfortunate reality of today's interconnected digital world. Cybercriminals are actively seeking to exploit vulnerabilities, and large-scale thefts of consumer information have repeatedly demonstrated the importance of data security. Natural disasters, power outages and other non-criminal activity can also put client data and systems stability at risk. Appleton Partners has taken many steps in consultation with outside experts to protect our clients' personal information, some of which are outlined below.

Email Protocol	• All incoming and outgoing emails are scanned through a spam filter to try and block phishing, malware, and viruses. • Employees are required to encrypt all outgoing emails containing Personal Identifiable Information to safeguard client data from falling into the wrong hands.
Password Policies	• All corporate system-level passwords must be changed at least annually. • All user passwords must be changed at least every 90 days. • All users have been trained on proper password protocol and all passwords must conform to established security guidelines.
IT Infrastructure	• To protect our network from cyberattacks and ransomware, Appleton has set up a 3rd party security system that includes 24x7 monitoring by a Security Operation Center (SOC). • Access to Appleton's network requires the use of multi-factor authentication (MFA). All external access to Appleton computer systems requires the use of a Virtual Private Network (VPN) and/or MFA. • Data is backed up several times daily and stored using secure, encrypted technology. • Appleton has a business continuity/disaster recovery plan that includes access to an offsite data center offering continuous data back-up and protection. This is aimed at maintaining full operations in the event of a power outage, or data security breach.
Network Security Control and Audit	• A comprehensive information security program overseen by our Security Officer is in place that includes monthly review of Appleton's computer network and its potential vulnerabilities. • To test network security, we have contracted with a 3rd party cybersecurity vendor to conduct systems audits and penetration tests.
Security Maintenance Patches and Updates	• All electronic devices connected to our network, such as servers, workstations, firewalls, network switches, routers, tablets, mobile devices, and cellular devices, periodically require vendor developed software patches, a process overseen by Information Technology.
Vendor Management/Third Party Services	• Appleton will only share personally identifiable client information with approved 3rd party service providers on a need-to-know basis and in accordance with established procedures. For example, this might involve transactions processing and custodial account maintenance. • Vendor due diligence reviews are conducted at least annually concerning matters such as cybersecurity, privacy policies, and business continuity. Compliance also conducts annual risk assessments on all vendors who access personally identifiable client information.
Employee Training	• Employees receive cybersecurity training at least annually that includes proper use of mobile devices. • Continuous phishing campaigns are conducted to test employee responses to staged email scams. Anyone falling for such test scams is required to undergo additional training.

How can we help you? Please contact:
Jim O'Neil, Managing Director, 617-338-0700 x775
privateclient@appletonpartners.com
www.appletonpartners.com