SECURITY POLICY OVERVIEW

At J. J. Keller & Associates, Inc. (J. J. Keller) we recognize that protecting customer data is critical and that security is crucial to our customers. Therefore, security in J. J. Keller web-based applications is our top priority. We devote significant resources to continually improving our robust security infrastructure. Our information systems policies and controls have been designed with the ISO 27001 and NIST Cybersecurity frameworks in mind. DQS, Inc. has certified our Information Security Management System (ISMS) as compliant with the ISO 27001:2013 standard.

It is the policy and practice of J. J. Keller that we will:

- Maintain an ISMS that is independently certified to be compliant with ISO 27001.
- Make information accessible only to those authorized to have access.
- Safeguard the accuracy and completeness of information and processing methods.
- Continuously improve the security of our services, identify risks, and implement and document appropriate controls.
- Promote security awareness and provide appropriate information security training to our associates and consultants using our information systems.
- Require all associates, contractors, third parties, and vendors working on behalf of J. J. Keller to understand and comply with the confidentiality, integrity and availability requirements included in J. J. Keller's service offering.
- Prepare and test incident response plans so that incidents are timely detected, contained and corrected, and impacted customers are timely notified according to contractual and regulatory requirements.
- Plan business continuity practices to help prevent disruption of services, achieve our RTO and RPO objectives, and maintain continuity of information security during adverse events.

These policy objectives are achieved through the implementation of information technology and security policies, which include procedures and guidelines developed in accordance with industry best practices. To provide assurance that we are achieving our security objectives, we undergo annual audits by a certified registrar to maintain certification to the ISO 27001 standard, commission a third-party to conduct annual penetration tests against our systems, and contract with a Managed Security Service Provider (MSSP) to provide 24x7x365 monitoring of our network.