How the ACET Portal Protects Your Information

General Provisions	
Data Stewardship	RCG protects Client data within the ACET Portal as if it was our own. The following items define some of the protections that are in place for each Client.
Information Security Policy	RCG's information security policies guide the software development, implementation, and operational support of the ACET portal. Our team puts security foremost.
External Party Access	RCG only uses data centers that have passed SSAE 16 audits and that secure client data to the most stringent standards. Data is secured inside of the Azure platform, and inside of the Virtual Strong Box secure data archive.
Legal Compliance	RCG's ensures full compliance with legal and regulatory requirements through on-going adherence to our information security policies.
Information Classification	RCG adheres to its formal asset management policy when classifying data and determining the protection level. Data contained within the ACET Portal is handled as if classified as Confidential and is encrypted.
Data Security Provisions	
Data Location	Your data is stored in private data centers which are rated highly for availability and durability and are located within the United States. RCG uses SSAE 16 Type II accredited datacenters to host our application and metadata.
Data Access Controls	The ACET system limits data access to members of your team and outside individuals your administrator has authorized to see the information. Our administrators have access to certain metadata needed to maintain the system, but do not have access to the data describing the security posture of your organization.
Data Visibility	The ACET Portal restricts users to view only access to files within the portal. File information is not downloaded to end user systems, instead users are provided with a temporary rendering of the information in the file. RCG disables copying, saving or printing of this information from inside of the ACET application.
Data Segregation	RCG maintains logical segregation of client data in separate databases, and in the file archive.
Encryption	Data are encrypted at rest and in motion using AES 256-bit encryption, a Federal Information Processing Standard (FIPS) encryption algorithm (FIPS 197). The ACET Portal employs TLS 1.2 for portal to browser communication.

Firewalls	Files are processed by systems protected by firewalls that effectively limit and control access to network segments
Network Ports	All Network Ports are under Firewall protection, using rules that only allow traffic from ports 80 and 443. This increases the protection of Customer data from external, unauthorized access to the data.
Redundant Data Storage	Data is stored redundantly in multiple locations within and across the data centers hosting the ACET portal. This ensures survivability of the data and facilitates continuity of operations.
Data Exchanges	All ACET Portal information communicated between RCG and its third parties is encrypted. Contractual agreements between RCG and the third parties ensure the proper handling and protection of shared information.
Data Deletion	When data is deleted, it is permanently deleted from our production and backup servers and is not recoverable. Deletion involves using a data wiping algorithm to overwrite the location of the data with a random pattern. Data deletion is under the control of the Client's Application Administrator.
Physical Security	RCG's data center providers adhere to best practices for securing physical access to information assets.
Data Ownership	Client data maintained within the ACET Portal remains the property of the Client. Clients may request return of their entire data set at the end of their contract.
Access Management	
Role-Based Access	Role based administration of access is inherent in the design of the ACET portal.
Multi-Factor Authentication	Clients may set up a multi-factor authentication process that requires the submission of the account password and a secondary authentication, such as SMS text message, to access their ACET Portal information.
Password Composition	Password length and composition are configurable by the Client application administrator. Options include length, composition rules, and lifetime. Default values are minimum 8 characters, one Upper, one Lower, one Numeric, and one Special, with a 90-day lifetime.
Account Lockout	After 3 failed logon attempts the ACET Portal locks users out of their individual account for 15 minutes.
Inactivity Logout	The ACET Portal will automatically log users out after 20 minutes of inactivity.

Access Logs	The ACET Portal maintains detailed Access logs on a Client specific basis. Access to these logs is restricted to the Client's Application Administrator. The logs are retained indefinitely, until purged by the Application Administrator.
Change Logs	The ACET Portal maintains detailed Change logs on a Client specific basis. Access to these logs is restricted to the Client's Application Administrator. The logs are retained indefinitely, until purged by the Application Administrator.
Audit Controls	Clients can use the tools provided within the ACET Portal to review account activity, such as account usage and access to information.
Operations Management	
Operational Processes	RCG's data center providers adhere to best practices for operating the computing infrastructure. RCG's operations team adheres to company established processes in managing the operations of the ACET Portal.
Patch Management	RCG monitors vulnerability data sources for new exploits and enforces timely patch management across the ACET infrastructure.
Updates	Except for patches, portal functionality will be updated on approximately a 90-day interval. Prior notice of updates will be published via the logon screen for the application.
Maintenance Window	RCG maintains a maintenance window for the application of routine changes to the system. The window is nominally set at 7-9PM Central time on Friday.
Monitoring	RCG leverages the capabilities of the Azure Security Center to monitor for and detect unauthorized information processing activities. Other Azure tools are used to detect and flag any degradations in performance or availability.
Continuity of Operations	
Incident Management	RCG leverages the Azure and Virtual StrongBox platform's incident response capabilities to address infrastructure related events. RCG's incident response plan addresses non-platform centered events.
Disaster Recovery	Data is backed up and replicated to another data center to ensure the ability to recover it following a data center event.
Business Continuity	The ACET Portal leverages the High Availability capabilities of the Azure and VSB platforms to ensure distribution across multiple data centers, thus ensuring timely resumption of services in the event of a system or data center loss.

DR/BCP Testing	RCG, as part of its Business Continuity Plan, conducts BCP and DR tests at least annually.
Outage Notification	RCG employs an H/A implementation and the elevated level of redundancies build into the RCG SaaS Platform to minimize outages. In the event of a network outage that would impact Customers' ability to access the SaaS application, RCG will publish a notification message on the logon screen.
RTO/RPO	In the event of a disaster, RCG's replication of Customer data and the application infrastructure across multiple Data Centers will assist with RTO and RPO objectives. The ACET Portal RTO is 12 hours. The RPO for the Portal is 1 hours.
Breach Notification	Federal and State Laws mandate notification in the event of loss of Personally Identifiable Information (PII) because of a breach. RCG's Incident Response practice includes proper notification of each Client potentially affected by a breach.
Configurable Settings	
Portal Customization	Clients may brand the ACET Portal through the application of their Logo and customization of the logon page messaging.
Terms and Conditions	Terms and Conditions are displayed when a Client's Application Administrator initially accesses the Portal. They remain accessible to the Application Administrator via a menu option off the administrator's settings menu.