

Security and Privacy Safeguards

The Business Connection Web-Based Tool

RSM McGladrey provides the Business Connection to its business clients. The tool is accessed through a secure data portal within the RSM McGladrey corporate web site. It provides a simplified method for clients to electronically submit financial information to RSM McGladrey, and provides clients with secured, password-protected access to their financial performance trends.

Confidentiality

RSM McGladrey is committed to safeguarding the confidentiality of its clients' financial information. Each employee that uses or accesses the tool, and each independent contractor that provides support for the tool, is legally bound to hold all client information confidential and is legally prevented from disclosing the information to any unauthorized person or entity.

Information Security

All information transmitted by this on-line system is carefully managed, with leading technology practices employed to enforce data privacy. Physical, electronic and procedural practices employed meet or exceed federal standards regarding the protection of customer information. Client information is not sold to or shared with outside parties that may wish to market their products.

Network Security

Data servers containing client information are equipped with secure firewalls to prevent outside attacks. 128-bit Secure Socket Layer (SSL) Data Encryption ensures that if the data were intercepted during transmission, it would be unintelligible and unidentifiable.

Application Security

Application users must enter 3-component security credentials (a login name, password and client code), which are then authenticated against internal database, and either granted or denied access to internal application space. No client data is stored or cached on a browser.

Storage of Client Data

Production equipment for this system is located at a managed hosting services facility that maintains 24-hour security. The hosting facility's physical security practices include 24 x 7 x 365 on-premise security monitoring of all servers and data stores, and unapproved data center staff are prevented from accessing system resources. This facility manages ongoing security matters such as daily back-ups, network updates, security patches, intrusion detection, hardware failures, and other network operations, and employs stringent controls to ensure that client data is never jeopardized.