

Data Security

Database Design

At the core of iLumen's integrated business client solution is a relational database architecture designed to track, audit, route, and store financial data. Identifying information relating to a specific company's financial records is stored in an isolated database repository.

By encrypting the company's identity, as well as separating the physical storage of the data, we further ensure that no unauthorized party can interpret, decipher, or decode financial records maintained within the database, even if the data were accessed directly from an authorized domain account on the server itself.

Industry-leading security measures within the application, network, and physical premises of the data center are designed to prevent any possible physical access to the data. iLumen goes one step further by making that data unintelligible to an unauthorized party. iLumen has never had any security breaches or data compromised.

Data Storage

As a standard policy, no customer data is managed or stored at iLumen. All production client data is managed at our off site production data center, DataReturn, which recently was acquired by Terremark.

During a customer implementation, customer data may be processed using storage media provided to iLumen directly by our customer; however, this only occurs at the customer's request with express written permission.

Any incidental customer data stored in connection with this type of request resides temporarily on a dedicated server in our secure server room.

When the data transfer is completed to DataReturn/Terremark, iLumen either removes the data from our on-site server or archives it in a secure off-site location, as necessary and as directed by the customer. The initial source CDs and data files are returned in its initial form to the customer or destroyed.

Confidentiality

iLumen requires each employee and independent contractor to enter into a written agreement that states all Confidential Information, and all embodiments thereof received or developed by them while employed by iLumen, in trust and in the strictest confidence.

Each employee and/or independent contractor must further agree in writing not to disclose to anyone or use any Confidential Information outside iLumen without the written authority of iLumen's management. This confidentiality obligation continues for a period of three (3) years after the end of the employment or the independent contractor relationship.

In addition, each of iLumen's customer contracts contains mutual non-disclosure provisions that include not only confidential information, but also trade secret information.

Network Security

Test and QA data resides on dedicated servers in our secure server room. Access to these data stores is limited to System Administrator (SA) privileges only. Manual access to these data stores is limited to our Senior Database Administrator (DBA) and the Director of Product Development who have all executed a standard Employee Contract.

The test and QA regions contain no live customer data. Actual financial data is sometimes used to derive testing data, but it is impossible to trace a customer's data through the test and/or development region.

All our databases and critical data files are backed up every night to removable media device. The removable media device is then stored, on a rotating basis, in an off-site secure location.

Hosting Provider

iLumen utilizes DataReturn/Terremark as its hosting provider for the data and applications that power Portfolio Connection and Client Connection. From best-in-class physical infrastructure and server platforms to an ITIL-based operations model certified to deliver under today's demanding regulatory requirements, DataReturn/Terremark is an unmatched service infrastructure to bring enterprise class managed services to mid-market companies and the leading online applications.

A pioneer in the industry and acknowledged expert in running complex transaction-intensive, business-critical applications, DataReturn/Terremark has been providing a higher standard of managed hosting for more than a decade. The company has handled billions of transactions for hundreds of clients around the world. In addition to iLumen, DataReturn/Terremark hosts sensitive company financial information for online service providers such as HR Block and QuickBooks Online.

DataReturn/Terremark offers a full Managed Hosting service for all customers with applications running at its facilities. DataReturn/Terremark manages ongoing security matters such as daily back-ups, network updates, security patches, intrusion detection, hardware failures, and other network operations. To perform these services at the contracted SLA levels, DataReturn/Terremark requires administrative level access to all application servers running in their environment.

DataReturn/Terremark has very stringent policies and controls to insure that customer data is never jeopardized. DataReturn/Terremark does not have any level of access to any iLumen networks or systems other than those physically located at DataReturn/Terremark.

