iCIMS Backup and Disaster Recovery Overview

Last Updated 3/19/2021

Overview

iCIMS maintains a comprehensive disaster recovery plan to ensure full availability of our customers' critical data in the event of a disaster. iCIMS tests this recovery plan at least annually.

iCIMS' primary hosting environments provide first-level protection for disaster recovery through redundancy at all levels of the operation.

- The United States hosting environment is operated on the East Coast with primary disaster recovery across multiple availability zones and the capability to fail over to an alternate region within the US in the event of a complete disaster.
- The European Union hosting environment is operated out of Germany with primary disaster recovery across multiple availability zones and the capability to fail over to an alternate region within Europe in the event of a complete disaster.
- The Canadian hosting environment is operated out of the province of Québec, with full capabilities to fail over to the province of Ontario in the event of a major disaster.

For details about these locations, see https://www.icims.com/gc-it.

All proprietary customer data is backed up nightly using AES 256-bit encryption and iCIMS currently commits to a 24/24 RTO/RPO or 8/8 RTO/RPO.

Preventative Measures and Provisions

Servers

iCIMS makes use of clustering, load-balancing, and failover technologies within its architecture. This serves to minimize, if not eliminate, any noticeable impact because of the failure of a specific server.

Internet Connectivity

iCIMS solutions are connected to the Internet backbone via multiple ultra-high-speed fiber optic connections. State-of-the-art routers provide autonomous load-balancing and failover. These routers instantly fail over if and when any given connection goes down. Each connection follows a different path (or route) to the Internet backbone. The result is that even in the event of catastrophic failure of the primary route, the data center automatically fails over to the best available connection.

This is augmented by a strategic partnership with a top-tier content delivery network (CDN), with a network of over 100,000 servers located in over 71 countries used to deliver certain static content (such as images, style sheets, JavaScript, etc.) directly to end users. No sensitive customer data is ever hosted or delivered by our CDN.

Data Backups

iCIMS performs backups of all customer data every night. AES 256-bit encrypted copies of data backups are stored locally on servers and remotely

in a secured cloud environment. Should the need arise, iCIMS can restore the previous night's data quickly, which is tested and has proven reliable.

Monitoring

iCIMS monitors its systems 24 hours a day, 7 days a week, 365 days a year through a combination of third-party and proprietary partners and tools. iCIMS' technical personnel are quickly alerted when there is a problem. The monitoring solution implemented by iCIMS also provides certain early detection and notification of potential problems. As a result, many potential problems are detected and resolved long before they may impact availability or become visible to our customers.

Recovering from a Disaster

The majority of iCIMS' technical infrastructure has been architected for the cloud and leverages best practices such as high availability and replication of services across multiple locations.

In the event of a partial disaster (e.g., failure of infrastructure, service, or hardware within a hosting environment), iCIMS and/or iCIMS' hosting providers will be notified of the disaster and will take steps to address any affected infrastructure/service or hardware, if applicable. Should a partial disaster affect any component of iCIMS' cloud infrastructure, iCIMS technical personnel will be notified by internal and external monitoring software. iCIMS technical personnel will review the affected infrastructure/service and will take necessary action. Should a partial disaster affect one of iCIMS' hosting environments, iCIMS will be notified by the hosting provider as to the arrangements being made to replace or fix the affected system. The clustering, load-balancing, and failover technologies used by iCIMS help to

mitigate the visible effects that certain partial disasters might have otherwise had on iCIMS solutions. iCIMS solutions will often remain fully functional while the partial disaster is addressed.

In the event of a complete disaster (e.g., earthquakes, explosions, fires, other natural disasters that result in complete physical destruction of a primary region), iCIMS will be notified by hosting provider as to the extent of the disaster. Based on this information, iCIMS will begin to leverage the appropriate disaster recovery environment. Customer data will then be restored from backups, as necessary. Once the systems are back online, iCIMS will conduct testing to ensure everything was properly recovered to the expected state.