iCIMS, Inc. • 101 Crawfords Corner Road, Suite 3-100, Holmdel, NJ 07733 • www.icims.com • 1.888.299.0487

Updated March 19,

Overview

iCIMS maintains a fully cloud-hosted environment. Customer data storage is segregated from the application. Numerous security controls, detailed below, have been implemented in the cloud environment.

Locations

US

The private cloud used for primary hosting and disaster recovery in the United States is operated out of Virginia, with full capabilities to fail over to Oregon in the event of a major disaster.

EU

The private cloud used for primary hosting and disaster recovery in the European Union is operated out of Germany, with full capabilities to fail over to Ireland in the event of a major disaster.

Canada

The private cloud used for primary hosting and disaster recovery in Canada 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.

Availability & Connectivity

All locations offer a minimum 99.9% uptime and availability.

Monitoring & Security

All locations utilize the following monitoring and security measures:

- At rest AES 256-bit encryption of customer data.
- Physical access to the data center is limited to people with verified, justified business reasons. If access is granted, it is revoked once necessary work is completed.
- Controlled process for entering datacenter perimeter, including security personnel and cameras. All approved guests are given badges that require multi-factor authentication and limit access to pre-approved areas.
- Data center employees are granted specific permissions to relevant areas of the facility based on job function, which is regularly reviewed to ensure access to only appropriate areas.

- Multiple tools, such as video surveillance, intrusion detection, and access log monitoring systems, are leveraged to watch for unauthorized entry to the data center. Entrances are secured with devices that sound alarms if a door is forced or held open.
- Dedicated personnel are responsible for monitoring, triaging, and executing security programs for our data centers, including continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyze a potential security incident.

Compliance & Certifications

All locations maintain the following levels of compliance and certifications:

- SOC 1 (SSAE 16), SOC 2, and SOC 3 compliant
- ISO 27001, ISO 27017, ISO 27018 certified
- PCI DSS 3.2 certified
- GDPR ready

Environment, Power & Backup/Failover

All locations have the following environment, power and backup/failover precautions:

- Water, power, telecommunications, and internet connectivity are designed with redundancy, in order to maintain continuous operations in an emergency.
- Electrical power systems are designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility.
- People and systems monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.