

Overview

The data center operations of Corporate iM are maintained by our internal partner, Aegis Information Systems, and managed primarily from here in CT by our combined staff, as well as our onsite data center staff. The highest quality of security and availability is constantly and consistently employed by our facilities and staff. The following gives a summary description of the physical environment of our data operations:

Power Supply

Our Internet Data Centers (IDC) are designed with true N+1 redundancy—at any time each component is connected with multiple power and networking connections. The IDC power design is based on multiple and fully divergent power substations, N+1 Uninterruptible Power Supply (UPS), N+1 generator back-up, and N+1 generator feeds to the building.

Network Connectivity

The data center has a highly scalable, fully redundant, secure network design that provides our application users with superior service and Internet connectivity to the DataLynx system. The facility is served by multiple carriers and Internet service providers for network connectivity redundancy. Divergent routes and multiple connections in networking cable plant, via multi-homed SONET rings, ensure true N+1 redundancy. Our self-healing wide area network and fully redundant, high-speed local area network infrastructure (Fast Ethernet/Gigabit Ethernet) provide our systems with a network solution that is secure, highly reliable and has virtually limitless scalability.

Physical Security

Our integrated security approach ensures that our equipment and your data are protected at all times. At the building's perimeter, security personnel monitor controlled access. Throughout the state-of-the-art facility, surveillance cameras, motion sensors and biometric identification systems create a fortress-like environment

Operations

Our data center staff and automated systems monitor your connectivity and performance, Internet and database server operations with state-of-the-art Network Operations Centers (NOC) 24 hours a day, 365 days a year. Our systems benefit from our advanced network management and reporting capabilities, as well as 24 x 365 onsite technical support. This high-touch care enables us to resolve system concerns before they become production issues.

Network Perimeter Security

Perimeter Security is provided by multiple redundant Cisco Firewalls, providing multiple layers of security to allow access to external systems while protecting core customer data.

Network Application Proxy

Access to customer data is delivered through our secure Application Layer Proxy. This redundant front-end environment provides a greater level of application performance over traditional WEB based systems. It also allows for a greater level of data security and is less subject to typical “web server” attacks.

Network Authentication Systems

Authentication to internal network systems is delivered through a single redundant directory service. This level of integration provides ease of administration while reducing the security risks associated with administering multiple systems.

Network Data Storage

Critical data files within our environment are stored on a true N+1 redundant storage infrastructure with security components integrated into the centralized management architecture. Backup of critical data is performed on an ongoing basis and ranges from constant “real time” backup to nightly backup, all performed to external media. After being backed up, the data is then moved to a secure off-site facility monthly for long-term storage.

Network Data Transmission

In order to provide a secure network, data must be protected at all times. This includes the protection of data while in transit and/or in the hands of authorized end users. Once in the system, data never leaves the network other than for long-term storage purposes or for secured, authorized transmission to external partners via our automated systems. Reporting data is made available to authorized, authenticated users only via the DataLynx online interface and via email (upon request).

Application Security

Access to the DataLynx system is only available to authorized and authenticated users. The DataLynx online system is secured via a 128-bit Secured Sockets Layer (SSL) connection. The data repositories of clients are logically and physically separated from each other based on the size and relationship of the logical groups of clients.

Customer Support

Support issues may be submitted by phone, online or email 24x7. Service Level Agreements (SLA) is as follows:

- Sev1 - Urgent issues affecting multiple users at multiple sites will be responded to within 1 hour from 9AM – 5PM ET Mon – Fri. On call support will respond within 4 hours outside of core business hours.
- Sev2 – Urgent issues affecting a single user are normally handled before end-of-day, however the SLA includes a response within 1 business day.
- Sev3 – Issues of a non-urgent nature will receive a response by email communication or by phone within 3 business days.

Contact Us

- **Phone:** An operator may be reached 24x7 at our toll-free number: (800) 730-4294
- **Email:** You may report a support issue by email to support@datalynxonline.com