Learn how physical facility and systems security as well as operations center and server operating environments play a role in OCLC ILLiad hosting operations.

Physical facility security

OCLC systems for hosted ILLiad are housed in a data center in Dublin, Ohio. Access to this location is granted on an as needed basis. Persons wishing to enter this restricted area must use a badge reader system. System Operators staff the Network Operations Center (NOC) 24x7, monitoring all hosts and subnets. Security guards are present after standard business hours. The OCLC data center is also monitored via a CCTV system. The CC feeds display in the NOC.

Visitors, 3rd party contractors, and vendors of the Dublin campus of OCLC are given guest badges identifying them as non-OCLC employees. These badges allow access to only non-secure sections of the campus. Visitors of the OCLC data center are only allowed access to an observation deck unless there is a specific need for them to have access to the datacenter floor.

Systems security

OCLC is proud to employ a permanent team dedicated to Information Security. The evaluation of all areas traditionally associated with computer security fall under this group's auspices. Reviews of applications, systems, and procedures are part of an ongoing process. Continuous evaluation of our program rather than semi-annual or annual audits significantly enhance our ability to prevent or detect security events. Ongoing staff development is key tool we use to help retain staff and to ensure they are able to do their jobs in an efficient manner. Compliance is monitored by the Information Security (InfoSec) team.

Operations center environment

Our datacenter pulls power from two grid segments. They are connected to the electrical room from two feeders originating on separate substations. During normal operation, one feeder supplies power to the UPS modules (Uninterruptible Power Source), with the other feed as backup. The UPS is made up of two 1000KVA parallel redundant systems. These units supply power to the three computer rooms and telco equipment. Currently the system is at 20% of rated capacity. During a failure of commercial power and during the start-up of emergency backup power, the UPS batteries will carry the critical load.

During a failure of the primary feeder, OCLC has the ability through high voltage switching gear to supply power from the remaining feeder. This mode can be sustained until the power company returns the down feeder back to operation status. During the failure of both feeders, OCLC can sustain critical operations by bringing both banks of emergency generators on-line. Each bank consists of two 1000-Megawatt diesel generators. One bank feeds the UPS modules and
the other feeds the life safety equipment. One 20,000 gallon in ground fuel tank supplies fuel for both banks and monitoring equipment tracks gallons per hour used and remaining fuel in the tank.

We have a state of the art fire suppressant system consisting of Halon under the floor and water sprinkler heads in the ceiling; all of which are monitored 24x7. Intelligent smoke detectors are installed and it takes two adjacent smoke detectors to activate to release the Halon. Zoned water sensors are also placed under the raised flooring.

**Server operating environment**

OCLC ILLiad servers run on Windows 2012 Server and MS SQL 2017. All servers are under patch management from the Windows systems and database administration support groups. OCLC has an extensive hardening policy that is integral with the rollout of systems. These policies cover network, host, and application settings, configurations, and standard operations. Periodic security audits are conducted by the InfoSec team to review and ensure compliance with these standards. All hardware purchases are backed by three-year service plans. Software licensing is kept current with the manufacturer.

The InfoSec team at OCLC as well as the Windows systems and database administration groups monitor security advisories and patch notifications from Microsoft as well as other notification lists like Flexera. Before patches are applied to a production system, they are rolled out to a test environment to determine if there are any negative changes to system functionality. If the patch has no detrimental side effects, it is deployed on the production nodes during a maintenance window.

OCLC makes use of an agent-based monitoring system to ensure ILLiad hosts are up and running within SLA parameters. All servers are protected by CrowdStrike Falcon, a next-gen anti-virus service that works on AI and Machine learning to better detect and protect against malicious threats.

OCLC also employs a stringent backup policy. The ILLiad MS SQL database is backed up in hourly increments and additional backups are run nightly on the SQL Database, ILLiad files, and Web pages (including Odyssey PDF files). These backups are sent to an offsite backup facility. All database and web server backups are on 45-day rotation. Backup restoration tests are performed during disaster recovery exercises that are held several times throughout the year.

https://help.oclc.org/Resource_Sharing/ILLiad/Get_started/OCLC_ILLiad_hosting_operations

Printed: Mon, 19 Sep 2022 14:48:21 GMT