OCLC® The world's libraries. Connected.™

Security Whitepaper: *OCLC's Commitment to Secure Library Services*

Contents

Executive Summary

OCLC is a worldwide library cooperative, owned, governed and sustained by members since 1967. Our public purpose is a statement of commitment to each other—that we will work together. OCLC's partnership extends to preserving the confidentiality, integrity and availability of our library partner's and their patron's data. OCLC is committed to industry-leading security and interoperability principles, including open connections and support for standards and data portability that meet the needs of the library community and its patrons. OCLC delivers layered security based on International Standards Organization (ISO) 27001:2005, Standard for Information Security Management. OCLC's ISO 27001 information security management system (ISMS) is aligned with our ISO 9001:2000 certified quality processes.

Information Security and Enterprise Risk Management

- Implemented an Information Security Management System in accordance with ISO/IEC 27001:2005.
- Professional staff of certified information security and information technology audit professionals and a full-time dedicated specialist in Business Continuity Planning and Disaster Recovery.

Physical and Environmental Controls

- 24-hour manned security
- Restricted access via proximity cards
- Computing equipment in access-controlled cages
- Video surveillance throughout facility and perimeter
- Humidity and temperature control
- Raised flooring to facilitate continuous air circulation
- Underground utility power feed
- Interruptible power systems (UPS)
- Redundant power distribution units (PDUs)
- Diesel generators with on-site diesel fuel storage
- Smoke and fire detection sensors throughout the data centers
- The Dublin Service Delivery Center (DSDC) is protected by a Halon system with sufficient reserves for multiple discharges
- The Columbus Service Delivery Center (CSDC) is protected by a DuPont FM-200 fire suppression system
- The data centers are also protected by wet-pipe sprinkler systems
- There are fire extinguishers maintained throughout the DSDC and CSDC

Logical Access Controls

- User identification and access management
  * Connections to patron data via SSL 3.0/TLS 1.0, using global step-up certificates from Thawte, ensuring that our users have a secure connection from their browsers to our service
  * Individual user sessions are identified and re-verified with each transaction, using XML-encrypted security assertions via SAML 3.0

* Depending on the specific services utilized

Operational Security Controls

- Connected to the Internet via redundant, diversely routed links from multiple Internet Service Providers served from multiple telecommunication provider Points of Presence
- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers

- Load balancers provide proxies for internal traffic
- OCLC uses a variety of methods to prevent, detect, and eradicate malware
- Third-party independent security assessments are also periodically conducted
- All data are backed up daily to tape at each data center
- The backups are cloned over secure links to a secure tape archive
- Tapes are transported offsite and are securely destroyed when retired
- Our Information Security staff monitors notification from various sources and alerts from internal systems to identify and manage threats

Systems Development and Maintenance

- OCLC tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities
- Network vulnerability assessments
- Selected penetration testing and code review
- Security control framework review and testing

Business Continuity and Disaster Recovery

- The OCLC service performs real-time replication to disk at each data center, and near real-time data replication between the production data center and the disaster recovery site
- Sensitive data are transmitted across dedicated links
- Disaster recovery tests verify our projected recovery times and the integrity of the customer data

Incident Response, Notification, and Remediation

- Incident management process for security events that may affect the confidentiality, integrity, or availability of its systems or data
- Information Security Team is trained in forensics and handling evidence in preparation for an event, including the use of third party and proprietary tools

Compliance

- Information can only be obtained by third parties through legal processes such as search warrants, court orders, subpoenas, through a statutory exemption, or through user consent
- OCLC maintains a strong privacy policy to help protect customer and patron data. This policy is detailed at http://www.oclc.org/policies/privacy/

Information Security and Enterprise Risk Management

OCLC's Information Security Management System (ISMS) defines our commitment to our customers. The information security program is based on ISO/IEC 27001:2005, recommendations of the Cloud Security Alliance, and Generally Accepted System Security Principles. The Information Security Program organizes security requirements into three top-level domains: Administrative, Technical, and Physical. The criteria in these domains represent the basis from which security and compliance risks are managed. Starting with the safeguards and controls identified in the domains and their subcategories, the Information Security Program follows the ISO/IEC27001:2005 framework of "Plan, Do, Check, Act." OCLC's security program is formed around a multi-layered security strategy that provides a combination of preventative and detective controls at various levels of data access, storage, and transfer. Our strategy includes:

- OCLC's corporate policies
- Data classification and control
- Personnel security
- Physical and environmental security
- Logical access control
- Operational security controls
- Systems development and maintenance
- Disaster recovery and business continuity
- Incident Response, notification and remediation
- Compliance

To meet internal and external regulatory requirements, OCLC has implemented a number of control and security procedures. These procedures require transparency and validation for security tools, including vulnerability, logging, anti-malware and anti-spam. OCLC recognizes that corporate governance and compliance requirements are complex, and differ by country, library types, and other variables. Therefore, we harmonize these requirements to create a coherent security strategy based on the strictest of standards.

OCLC employs a full-time Information Security Team, embedded in the OCLC Systems Management Division, which is comprised of experienced and certified security, audit, and compliance professionals with deep knowledge in security architecture, applications, and network security. This team is responsible for monitoring the company's perimeter defense systems, developing security review processes, and advising OCLC's leaders for a customized security infrastructure. The OCLC Security Team has a key role in the development, documentation, and implementation of security policies and standards. Its responsibilities include:

- Reviews security plans for OCLC's networks, systems, and services using industry standards from the Center for Internet Security, ISACA, and the Institute of Internal Auditors

- Conducts security design reviews
- Provides ongoing consultation on security risks associated with a given project and possible solutions to security concerns
- Drives compliance with established policies through routine security evaluations and internal audits
- Engages outside security experts to conduct regular security assessments of its infrastructure and applications
- Executes a vulnerability management program to help discover problem areas on the networks, systems, and applications, and monitors remediation
- Monitors for suspicious activity on OCLC’s networks, and follows formal incident response processes to quickly recognize, analyze, and remediate information security threats

OCLC's Corporate Policies

OCLC is committed to the security of all information stored or transiting its information systems. This commitment is reinforced in OCLC's Code of Conduct. The foundation of OCLC’s commitment to security is established in its keystone corporate policies, procedures, and guidelines that cover physical, account, data, corporate services, network and computer systems, applications services, and systems services. These policies are reviewed on a regular basis to help ensure their continued relevancy, effectiveness, and accuracy.

OCLC employees are required to conduct themselves in a manner consistent with the company’s guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Upon hire, OCLC verifies an individual’s education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, OCLC may also conduct criminal, credit, and security checks. The extent of background checks is dependent on the individual’s roles and responsibilities. All employees are required to execute a confidentiality agreement and must acknowledge receipt of and compliance with policies in OCLC's Standard's Manual or local Employee Handbook. The confidentiality and privacy of customer information and data is emphasized in OCLC's employee guidelines and during new employee orientation. Employees are provided with security training as part of new hire orientation.

Data Classification and Control

To assist our library customers, OCLC's services environment must meet numerous government-mandated and industry-specific security requirements in addition to OCLC management's rigorous objectives. As OCLC's offerings continue to grow and evolve into the OCLC cloud, such as the Web-scale Management Services (WMS), additional requirements are expected that could include regional and country-specific data security standards. The OCLC Security Team works across operation, product, and service delivery teams to ensure OCLC complies with relevant laws, standards and regulatory requirements. These include, but are not limited to:

- Payment Card Industry Data Security Standard
- Health Insurance Portability and Accountability Act
- Family Educational Rights and Privacy Act
- Federal Information Security Management Act (National Institute of Standards and Technology (NIST) Special Publication 800-53)
- Children's Online Privacy Protection Act
- Commission of the Sponsoring Organizations of the Treadway Commission - Internal Control over Financial Reporting
- Applicable Regional and Country Privacy Laws, such as the EU Privacy Directive, Australian Privacy Principles, Canadian Personal Information Protection and Electronic Documents Act, etc...

Physical and Environmental Controls

OCLC's data centers employ a variety of physical security measures. The standard physical security controls implemented at each OCLC data center are composed of well-known technologies and follow generally accepted industry good practices: custom designed electronic card access control systems, CCTV monitoring and recording, and security guards. Access to areas where systems, or system components, are installed or stored are segregated from general office and public areas.

Access to all data center facilities is restricted to authorized OCLC employees, approved visitors, and approved third parties whose job it is to operate the data center. OCLC audits who has access to its data centers on a quarterly basis to help ensure that only appropriate personnel have access to the data centers. OCLC's data centers have been designed to be robust, fault tolerant, and concurrently maintainable.

Power to support OCLC's continuous operations is provided by redundant electrical power systems. A primary and alternate power source, each with equal capacity, is provided for every critical component in the data center. An uninterruptible power supply (UPS) is intended to provide power until the backup generators can take over. The backup generators are capable of providing enough emergency electrical power to run the data center at full capacity for a period of time.

The OCLC data centers use raised-floors to promote continuous air circulation. Air cooling is required to maintain a constant operating temperature for servers and other computing hardware. Cooling prevents overheating and reduces the possibility of service outage. Computer room air conditioning units are powered by both normal and emergency electrical systems.

Automatic fire detection and suppression equipment helps prevent damage to computing hardware. The fire detection systems utilize heat, smoke, and water sensors located in the data center. In the event of fire or smoke, the detection system triggers audible and visible alarms. Manually operated fire extinguishers are also located throughout the data centers. Data center technicians receive training on fire prevention and incipient fire extinguishment, including the use of fire extinguishers.

Logical Access Controls

OCLC has extensive controls and processes to protect the security of patron information[1]. Library staff and patron access can be defined by most institutions using federated models, such as Shibboleth, or the institution's LDAP. For authenticated access, OCLC's cloud offerings employs Security Assertion Markup Language (SAML) 2.0 XML-based standard for exchanging authentication and authorization data between security domains via the Identity Management (IDM) Module. Access to sensitive data is protected through secure HTTP (HTTPS) and Secure Socket Layer (SSL) 3.0/Transport Layer Security (TLS) 1.0 encryption. OCLC applications provide institutional customers with options for defining permissions and privileges based on roles and local policies for separation of duties.

Many legacy OCLC hosted systems have physically separated servers and databases that isolate a specific institutions data; however, OCLC's cloud applications run in a multi-tenant, distributed environment with logical access controls to restrict access between clients. Access by OCLC's staff to production environments is similarly controlled. A centralized group is used to define and control administrator's access to production services. OCLC employs a need-to-know and least-privilege model to manage access to resources and services. Where feasible, role-based access controls are used to allocate logical access to specific job functions or areas of responsibility, rather than to an individual. Individuals who are authorized to access any asset must use the appropriate measures to gain access. Highly sensitive assets require multifactor authentication, including such measures as password and hardware tokens. Reconciliation of user accounts against authorizations for access occurs on an ongoing basis to ensure that use of an asset is appropriate and needed to complete assigned duties. Accounts no longer needing access to a given asset are disabled.

[1] *"Patron Data" means all data related to a Patron, including item check-out, holds, profiles, and library account information.*

Operational Security Controls

Having a defense-in-depth approach is fundamental to how OCLC provides a trustworthy computing infrastructure. Employing a defense-in-depth approach improves our capacity to prevent breaches or to lessen the impact of a security incident.   Applying controls at multiple layers involves employing preventative and detective controls, developing risk mitigation strategies, and being capable of identifying and responding to attacks when they occur. Consequently our information security efforts focus on risks closer to the application level, such as objects, the static or dynamic data storage containers, the virtual machine objects, the run-time environments in which transactions occur. Risk management and corresponding reviews are adapted to this dynamic environment. OCLC uses processes based on its long-term experience delivering services on the Internet for managing these new risks.

OCLC's Information Security Program establishes the standard processes and documentation requirements for performing continuous risk-based decision making. The OCLC Information Security Team works with system developers, operations, and customer support staff to evaluate vulnerabilities to systems and services. Risk assessments occur at a variety of levels and inform OCLC's management of prioritization in areas such as product release plans, policy maintenance, and resource allocation. Each product has a comprehensive assessment of threats and leads to additional reviews throughout the year. This ongoing work focuses on those threats that could affect the availability, integrity, and confidentiality of services and data. Through this process, OCLC prioritizes and guides development of security controls and related activities.

Network Security

OCLC employs multiple layers of defense to help protect the network perimeter from external attacks. OCLC's network team executes systematic management of the network firewalls and ACL rules that employs change management, peer review, and testing. Only authorized services and protocols that meet OCLC's security requirements are permitted to traverse the company's networks.

OCLC uses multiple systems to monitor system, application, web page and web service status, and to inform operations and support staff of problems in an attempt to resolve issues before they are noticeable to users of OCLC systems. When problems are encountered, the systems send notifications out to administrative contacts in a variety of different ways. The systems provide operators with detailed status information, historical logs and reports. This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing. Network analysis is supplemented by examining system logs to identify unusual behavior, such as unexpected activity in former employees' accounts or attempted access of customer data.

Operating System Security

OCLC's production servers are built on a standard of hardened Windows and Linux operating systems (OS), and security patches are uniformly deployed to OCLC's infrastructure. The Security Team evaluates builds against industry standards, such as the Center for Internet Security, using automated vulnerability scanners to identify and remediate security issues prior to deployment in the production environment. OCLC uses a change management system to identify, test, and deploy critical security patches and updates to maintain the integrity of OSs. OCLC has a change management system to minimize the risks associated with making unauthorized modifications to the production OS builds.

Application Security

Application security is a key element in OCLC's approach to securing its cloud computing environment. The OCLC Security Team plays a key role in ensuring that security requirements are defined, application threats are identified against the Open Web Application Security Project (OWASP), the Web Application Security Consortium (WASC) Threat Classification and Common Weakness Enumeration. Additionally, applications undergo security test and evaluation with remediation of identified exceptions.

Malware Prevention

Malware poses a significant risk to today's information system environments. OCLC recognizes that a malware attack can lead to account compromise, data theft, and possibly additional access to a network. Therefore, we take these threats to its networks and its customers seriously and use a variety of methods to prevent, detect, and eradicate malware, including the deployment of professional anti-malware solutions for both servers and end-users.

Backup

OCLC employs a formalized, automated backup strategy that includes incremental backups to tape every 24 hours. Additionally, OCLC's backups are shipped off-site to a secure facility for storage.

Sensitive Data Disposal

When retired from OCLC's systems, disks containing sensitive information are subjected to a data destruction process before leaving OCLC's control. Where practical the disk to be logically wiped by authorized individuals. The erasure consists of a full write of the drive with all zeroes followed by a full read of the drive to ensure that the drive is blank. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be destroyed.

Systems Development and Maintenance

The rigorous security practices employed by development teams are formalized in OCLC's Product Management Life Cycle (PMLC). OCLC's PMLC is fully integrated with the product development lifecycle from design to response. OCLC's senior leadership continues to support the mandate that the PMLC be applied during the development process of OCLC products, including delivery of online cloud services.

OCLC maintains separate environments for development, quality assurance/test, and production. Application changes are thoroughly tested prior to being installed in the production environment to ensure the quality of service, as well as prevent any service disruption. OCLC’s change management for networks, operating systems, applications, and databases ensures that changes are evaluated, approved by management, and scheduled to prevent service disruptions.

Incident Response, Notification and Remediation

OCLC has an incident management process for security events that may affect the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. OCLC’s computer security incident handling procedures are structured around the NIST guidance on handling incidents (NIST Special Publication 800-51). Security breaches[2] are investigated quickly and the Legal Team provides notification to the affected institutions in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

The Information Security Team is trained in forensics and handling evidence in preparation for an event, including the use of third party and proprietary tools. To help ensure the swift resolution of security incidents, the OCLC Security Team is available 24x7 to all employees. When an information security incident occurs, OCLC's Security Team responds by logging and prioritizing the incident according to its severity. Events that directly impact customers are treated with the highest priority. OCLC's Security Team consults on post-mortem investigations when necessary to determine the root cause for single events, trends spanning multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.

[2] *“Security Breach” means an unauthorized access, use or disclosure of personally identifiable information (PII) that compromises the security, confidentiality or integrity of such information, such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. The following are not be considered a Security Breach: (i) the unintentional but unauthorized acquisition, access, or use of PII by an OCLC employee, contactor or agent acting under the authority of OCLC; or (ii) a good faith belief by OCLC that the unauthorized individual to whom the impermissible disclosure was made, would not have been able to use the PII.*

Disaster Recovery and Business Continuity

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, OCLC implements a disaster recovery program at its data centers. This program includes multiple components to minimize the risk of any single point of failure. To help ensure availability in the event of a disaster, OCLC data is replicated to a secondary data center. High-speed connections between the data centers help ensure minimal data loss. In addition to the redundancy of data and applications, OCLC also has a business continuity plan for key operational processes. The Business Continuity Plan addresses major disasters, such as a weather event or other crisis, and it assumes people and services may be unavailable for up to 30 days. This plan is designed to enable continued operations of our services for our customers. OCLC conducts periodic testing of our Disaster Recovery Plan.

Compliance

Legal Information Access

OCLC follows standard legal processes in responding to third party requests for information. Information can only be obtained by third parties through legal processes such as search warrants, court orders, subpoenas, through a statutory exemption, or through user consent. Upon receipt of a request for information disclosure, OCLC's Legal team reviews the request for compliance with applicable law. If the request is legally valid, it is OCLC's policy to notify the individual user or organization whose information is being requested except in an emergency or where prohibited by law.

Privacy

OCLC maintains a strong privacy policy to help protect customer and patron data. This policy is detailed at http://www.oclc.org/policies/privacy/

Conclusion

OCLC is committed to keeping the information stored on its computer systems safe and secure. OCLC provides controls at each level of data storage, access, and transfer. With OCLC, libraries and their patrons can be assured that OCLC values the privacy, confidentiality, integrity, and availability of their data.