Annex 2

Technical and Organisational Security Measures

(Appendix 2 to the Standard Contractual Clauses)

(LAST REVISION: 1 MARCH 2024)

Founded in 1967 as a non-profit, member-driven library community, OCLC is a global library cooperative that provides shared technology services, original research and community, and community programs for its membership and the library community at large. OCLC consists of 30,000 library members in over 100 countries.

OCLC has implemented the following technical and organisational measures designed to ensure the confidentiality, integrity, availability, and resilience of its data processing systems and services in accordance with industry standards. OCLC may replace or change these measures at any time, provided that new measures serve substantially the same purpose(s) without diminishing the level of security applicable to Personal Data. More information about OCLC's audit certifications is available in the OCLC Trust Center.

Information Security Program and Risk Assessments

OCLC maintains a worldwide information security and privacy program, with a full-time staff of security professionals and a dedicated data protection officer. Its information security and privacy teams are supported by a data governance body reporting to OCLC's executive management. Comprehensive internal policies are established and enforced to manage the classification and proper handling of data, and to prohibit the improper disclosure of confidential information.

All employees worldwide are required to perform information security awareness and privacy awareness training on an annual basis. Every employee undergoes a background check prior to employment.

OCLC undergoes annual information security risk assessments by third-party assessors, to validate its technical, administrative, and procedural controls. These assessments include ISO 27001, ISO 27018, ISO 27701, SOC 2, and U.S. FedRAMP certifications.

Physical and Environmental Controls

OCLC maintains data worldwide in its own data centres located in Dublin (USA), Amsterdam, Toronto, and Sydney. These data centres maintain suitable environmental protections, including fire suppression systems, humidity and temperature control, raised flooring for continuous air circulation. OCLC utilises uninterruptible power systems and redundant power distribution units, together with diesel back-up generators and on-site diesel fuel storage.

Its data centres are physically secured against unauthorised access, with 24-hour staffed security, all computing equipment in access-controlled areas, and video surveillance throughout the facility and its perimeter. Access is controlled with proximity cards and/or biometric control devices.

Data Controls

All data is stored encrypted at rest and in transit using current and industry standard encryption mechanisms. Administrative access to production systems containing customer data is restricted to necessary roles, requires multi-factor authentication, and is secured by encrypted virtual private network (VPN).

OCLC's systems utilise internal firewalls to segregate traffic between its application and database tiers. Perimeter firewalls and edge routers block unused protocols and manage incoming traffic to ensure availability. External penetration testing is performed annually by a third party, and periodic network vulnerability assessments are conducted to identify and remediate potential areas of risk.

Application Security

OCLC follows a software development process based on industry best practices. Logically separate environments are maintained for development, testing, and production, and source code management and deployment follow separation of duties principles. A formal change control process is followed, and code is evaluated and tested for security vulnerabilities. Developers do not have the ability to deploy software changes, as this is restricted to separate operations personnel with elevated privileges.

Incident Response and Business Continuity

OCLC maintains full disaster recovery, incident response, and business continuity plans. Its data centres utilise redundant, diversely routed links from multiple Internet service providers served from multiple telecommunication points of presence. Disaster recovery processes, including backup media restores, are tested at least annually.

Incidents are managed by a dedicated global Computer Security Incident Response Team (CSIRT) trained in incident response and forensic analysis. OCLC has multiple automated and manual incident detection systems, including an intrusion prevention system and unusual network traffic flow analysis. When incidents are identified, they are assigned a severity level by CSIRT and managed through resolution (including postmortem root cause analysis). CSIRT coordinates with OCLC's global privacy team and other relevant stakeholders across the organisation to evaluate privacy and business continuity impact, devise remediation plans, and provide information to potentially affected customers.