Annex 2
Technical and Organisational Security Measures
(Appendix 2 to the Standard Contractual Clauses)

OCLC has implemented the following technical and organisational measures designed to ensure the confidentiality, integrity, availability and resilience of data processing systems and services. 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.

. **Organisational Controls**

- Full-time, dedicated Data Protection Officer
- Full-time staff of information technology security professionals
- Data governance body reporting to executive management
- Policies in place prohibiting the disclosure of confidential information
- Third-party independent security assessments are periodically conducted

. **Physical Access Controls**

- 24-hour staffed security at data centres
- Access to data centre controlled via proximity card and/or biometric devices
- Computing equipment in access-controlled areas
- Video surveillance throughout facility and perimeter

. **Logical Access Controls**

- Secure connections from customer browsers to our services accessing patron data stores
- Regular network and system scanning for vulnerabilities
- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers
- OCLC uses a variety of methods to prevent, detect, and eradicate malware
- OCLC's Information Security staff monitors notification from various sources and alerts from internal systems to identify and manage threats
- Network vulnerability assessments conducted
- Selected penetration testing conducted
- OCLC tests code for security vulnerabilities

. **Environmental and Business Continuity Controls**

- Fire suppression systems in our data centre facilities
- Humidity and temperature control
- Raised flooring to facilitate continuous air circulation
- Connected to the Internet via redundant, diversely routed links from multiple Internet Service Providers served from multiple telecommunication provider Points of Presence

- Underground utility power feed into each building
- Uninterruptible power systems (UPS)
- Redundant power distribution units (PDUs)
- Diesel generators with on-site diesel fuel storage at each data centre location
- Nightly data backups
- Regular testing of restoration from backups
- Disaster recovery solution for WorldShare Management Services

V. Incident Response, Notification, and Remediation

- Incident response process for security events that may affect the confidentiality, integrity, or availability of its systems or data
- Incident Response Team trained in incident response and forensics