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

Bijlage 2
Technische en organisatorische beveiligingsmaatregelen
(Bijlage 2 bij de Modelcontractbepalingen)

OCLC has implemented the following technical and organizational 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.	OCLC heeft de volgende technische en organisatorische maatregelen geïmplementeerd om de beschikbaarheid, integriteit, vertrouwelijkheid en veerkracht van gegevensverwerkingssystemen en - diensten te waarborgen. OCLC kan deze maatregelen vervangen of wijzigen, op voorwaarde dat nieuwe maatregelen hoofdzakelijk hetzelfde doel dienen en zonder dat dit ten koste gaat van het beveiligingsniveau dat van toepassing is op de beveiliging van Persoonsgegevens.
I. Organisational Controls	**I. Organisatorische controle**
• Data Protection Officer	• Functionaris voor gegevensbescherming
• Full-time staff of information technology security professionals	• Voltijdse IT security professionals
• Data governance body reporting to executive management	• Data governance afdeling die rapporteert aan het management
• Policies in place prohibiting the disclosure of confidential information	• Beleid aanwezig dat de openbaarmaking van vertrouwelijke informatie verbiedt
• Third-party independent security assessments are periodically conducted.	• Externe onafhankelijke beveiligingsbeoordelingen worden periodiek uitgevoerd
II. Physical Access Controls	**II. Fysieke toegangscontrole**
• 24-hour staffed security at data centres	• 24-uurs bemande beveiliging bij datacenter
• Access to data centre controlled via proximity card and/or biometric devices	• Toegang tot het datacenter door middel van een proximity kaart en/of biometrische apparaten
• Computing equipment in access- controlled areas	• Computerapparatuur staat in zones met gecontroleerde toegang
• Video surveillance throughout facility and perimeter	• Videobewaking aanwezig, zowel in het datacenter als de omgeving ervan
III. Logical Access Controls	**III. Logische toegangscontrole**
• Secure connections from customer browsers to our services accessing patron data stores	• Veilige verbindingen van de browsers bij klanten tot onze diensten met toegang tot eindgebruikergegevens
• Regular network and system scanning for vulnerabilities	• Regelmatig scannen van netwerken en systemen op kwetsbaarheden
• Perimeter firewalls and edge routers block unused protocols	• Perimeterfirewalls en routers blokkeren onbekende/niet-gebruikte protocollen
• Internal firewalls segregate traffic between the application and database tiers	• Interne firewalls scheiden verkeer tussen de applicatie en databaselagen

• OCLC uses a variety of methods to prevent, detect, and eradicate malware	• OCLC gebruikt verschillende methoden om malware te voorkomen, op te sporen en uit te roeien
• OCLC's Information Security staff monitors notification from various sources and alerts from internal systems to identify and manage threats	• De Information Security medewerkers van OCLC monitoren meldingen van verschillende bronnen en waarschuwingen van interne systemen om bedreigingen te identificeren en te beheren
• Network vulnerability assessments conducted	• Er worden kwetsbaarheidsonderzoeken op het netwerk uitgevoerd
• Selected penetration testing conducted	• Er worden geselecteerde penetratietests uitgevoerd
• OCLC tests code for security vulnerabilities	• OCLC test code op beveiligingskwetsbaarhede
IV. Environmental and Business Continuity Controls	**IV. Controle op milieu- en bedrijfscontinuïteit**
• Fire suppression systems in our data centre facilities	• Brandbestrijdingssystemen in onze datacenters
• Humidity and temperature control	• Vocht- en temperatuurregeling
• Raised flooring to facilitate continuous air circulation	• Verhoogde vloer om een continue luchtcirculatie mogelijk te maken
• Connected to the Internet via redundant, diversely routed links from multiple Internet Service Providers served from multiple telecommunication provider Points of Presence	• Verbonden met internet via redundante, divers gerouteerde koppelingen van meerdere internetproviders die worden bediend vanuit meerdere Points of Presence van de aanbieder van telecommunicatie.
• Underground utility power feed into each building	• Ondergrondse stroomvoorziening voor nutsvoorzieningen in elk gebouw
• Uninterruptible power systems (UPS)	• Niet verstoorbare elektriciteit ssystemen (UPS)
• Redundant power distribution units (PDUs)	• Redundante stroomdistributie eenheden (PDU's)
• Diesel generators with on-site diesel fuel storage at each data centre location	• Dieselgeneratoren met on-site opslag van dieselbrandstof op elke locatie van het datacenter
• Nightly data backups	• Nachtelijke gegevensback-ups
• Regular testing of restoration from backups	• Regelmatig testen van herstel van back-ups
• Disaster recovery solution for WorldShare Management Services	• Disaster Recovery voor WorldShare Management Services
V. Incident Response, Notification, and Remediation	**V. Incidentrespons, melding en remediëring**
• Incident response process for security events that may affect the confidentiality, integrity, or availability of its systems or data	• Incident-responsproces voor beveiligingsgebeurtenissen die de beschikbaarheid, integriteit of vertrouwelijkheid van de systemen of gegevens kunnen beïnvloeden
• Incident Response Team trained in incident response and forensics	• Incident Response Team getraind in incident respons en forensisch onderzoek