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

**Allegato 2**
**Misure di sicurezza tecnica e organizzativa**
**(Appendice 2 alle Clausole contrattuali tipo)**

| | |
|---|---|
| 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 ha implementato le seguenti misure tecniche e organizzative progettate per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati. OCLC può sostituire o modificare tali misure in qualsiasi momento, a condizione che le nuove misure servano sostanzialmente agli stessi scopi senza diminuire il livello di sicurezza applicabile ai dati personali. |
| **I. ORGANISATIONAL CONTROLS** | **I. CONTROLLI ORGANIZZATIVI** |
| • Full-time, dedicated Data Protection Officer | • Responsabile della protezione dei dati a tempo pieno e dedicato |
| • Full-time staff of information technology security professionals | • Personale a tempo pieno di professionisti preposti alla sicurezza delle tecnologie dell'informazione |
| • Data governance body reporting to executive management | • Organismo di gestione dei dati che riferisce alla direzione esecutiva |
| • Policies in place prohibiting the disclosure of confidential information | • Politiche in atto che vietano la divulgazione delle informazioni riservate |
| • Third-party independent security assessments are periodically conducted | • Vengono condotte valutazioni della sicurezza indipendenti e periodiche da parte di terzi |
| **II. PHYSICAL ACCESS CONTROLS** | **II. CONTROLLI DELL'ACCESSO FISICO** |
| • 24-hour staffed security at data centres | • Sicurezza 24 ore su 24 presso i data center |
| • Access to data centre controlled via proximity card and/or biometric devices | • Accesso al data center controllato tramite tessera di prossimità e/o dispositivi biometrici |
| • Computing equipment in access-controlled areas | • Apparecchiature informatiche in aree ad accesso controllato |
| • Video surveillance throughout facility and perimeter | • Videosorveglianza in tutta la struttura e il perimetro |
| **III. LOGICAL ACCESS CONTROLS** | **III. CONTROLLI DELL'ACCESSO LOGICO** |
| • Secure connections from customer browsers to our services accessing patron data stores | • Connessioni sicure dai browser dei clienti ai nostri servizi che accedono agli archivi dei dati degli utenti |
| • Regular network and system scanning for vulnerabilities | • Scansione regolare della rete e del sistema per rilevare le vulnerabilità |
| • Perimeter firewalls and edge routers block unused protocols | • Firewall perimetrali e router perimetrali bloccano i protocolli inutilizzati |

| | |
|---|---|
| • Internal firewalls segregate traffic between the application and database tiers | • I firewall interni segregano il traffico tra i livelli dell'applicazione e del database |
| • OCLC uses a variety of methods to prevent, detect, and eradicate malware | • OCLC utilizza diversi metodi per prevenire, rilevare e sradicare il malware |
| • OCLC's Information Security staff monitors notification from various sources and alerts from internal systems to identify and manage threats | • Lo staff di OCLC per la sicurezza informatica monitora le notifiche provenienti da varie sorgenti e avvisi dai sistemi interni per identificare e gestire le minacce |
| • Network vulnerability assessments conducted | • Vengono condotte le valutazioni della vulnerabilità della rete |
| • Selected penetration testing conducted | • Vengono condotti test di penetrazione selezionati |
| • OCLC tests code for security vulnerabilities | • OCLC esegue il test del codice per le vulnerabilità della sicurezza |
| **IV. ENVIRONMENTAL AND BUSINESS CONTINUITY CONTROLS** | **IV. CONTROLLI DI CONTINUITÀ AMBIENTALE E AZIENDALE** |
| • Fire suppression systems in our data centre facilities | • Sistemi antincendio nelle nostre strutture di data center |
| • Humidity and temperature control | • Controllo dell'umidità e della temperatura |
| • Raised flooring to facilitate continuous air circulation | • Pavimento sopraelevato per facilitare la circolazione continua dell'aria |
| • Connected to the Internet via redundant, diversely routed links from multiple Internet Service Providers served from multiple telecommunication provider Points of Presence | • Connessione a Internet tramite collegamenti ridondanti e diversificati da più fornitori di servizi Internet forniti da diversi provider di telecomunicazioni POP (Points of Presence) |
| • Underground utility power feed into each building | • Alimentazione elettrica sotterranea in ogni edificio |
| • Uninterruptible power systems (UPS) | • Gruppi di continuità (UPS) |
| • Redundant power distribution units (PDUs) | • Unità di distribuzione dell'alimentazione ridondanti (PDU) |
| • Diesel generators with on-site diesel fuel storage at each data centre location | • Generatori diesel con deposito di gasolio in loco presso ogni sede del data centre |
| • Nightly data backups | • Backup dei dati notturni |
| • Regular testing of restoration from backups | • Test regolari del ripristino da backup |
| • Disaster recovery solution for WorldShare Management Services | • Soluzione di ripristino di emergenza per WorldShare Management Services |
| **V. INCIDENT RESPONSE, NOTIFICATION, AND REMEDIATION** | **V. RISPOSTA, NOTIFICA E RIPARAZIONE DEGLI INCIDENTI** |
| • Incident response process for security events that may affect the confidentiality, integrity, or availability of its systems or data | • Processo di risposta agli incidenti per eventi di sicurezza che possono influire sulla riservatezza, l'integrità o la disponibilità dei sistemi o dati |
| • Incident Response Team trained in incident response and forensics | • Team di risposta agli incidenti preparato nella risposta agli incidenti e nell'informatica legale |