ANNEX 2. SERVICE PROVIDER TECHNICAL AND ORGANIZATIONAL MEASURES

Service Provider represents and warrants that it implements and maintains the following technical and organizational measures. Each measure applies to the maximum extent applicable to the nature of the Services and Service Provider's processing of Canva Personal Data. Where Service Provider considers that a specific measure is not applicable to the Services, Service Provider shall: (i) notify Canva in writing, identifying the measure and the basis for its inapplicability; and (ii) implement an alternative measure that provides materially equivalent protection, unless the risk the measure addresses is not present in Service Provider's processing of Canva Personal Data.

Information Security Program

Security Personnel: Service Provider employs qualified information security personnel responsible for developing, implementing and maintaining an information security program that protects against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data processed within the Services.

Security Risk Assessment: Service Provider reviews and assesses potential security threats, risks and vulnerabilities at least annually.

Security Policies: Service Provider maintains information security policies covering business continuity, access management, vulnerability management, operational security, incident response, asset management and vendor management.

Personnel Management

Confidentiality: Personnel must sign a written confidentiality or non-disclosure agreement.

Contractors: Before providing a service, Service Provider's service providers and contractors must sign an agreement with appropriate confidentiality terms and, where appropriate, are bound by security policies no less protective than this Annex.

Training: Service Provider provides employees with security and privacy training.

Termination: On termination, Service Provider disables the employee's access to critical and non-critical systems, including physical facilities.

Networks and Transmission

Network Controls: Service Provider implements network access controls that detect and prevent unauthorized access to networks containing systems that process personal data.

Encryption in Transit: Service Provider requires HTTPS (TLS 1.2+ with a secure cipher suite) for transfers of personal data over public networks.

Data Centers and Data Management.

Data Center Controls: The Services run on infrastructure protected by appropriate physical security and environmental controls. Where this infrastructure is outsourced, Service Provider performs periodic security assessments of that vendor.

Data Segregation: Service Provider separates each customer's data logically and/or physically.

Environment Separation: Service Provider operates independent development, test and production environments, and does not use production data in development or test.

Encryption at Rest: Service Provider encrypts personal data at rest in the Services' systems using AES 256-bit encryption or stronger.

Access Controls and Logging

Access to Customer Data: Service Provider manages access to customer data using Role-Based Access Controls, restricting users to the least privilege necessary. Access to customer data uses unique user accounts. Access is centrally managed through an enterprise identity management solution.
Administrative Access: Administrative access to production servers and databases is restricted to personnel accountable for system availability and those with a legitimate business need.
Access Reviews: Service Provider conducts access reviews at least annually to confirm that personnel still require their access.
Authentication: Access to customer data requires multi-factor authentication, and password complexity rules are enforced where passwords are used.
Accounts and Credentials: User access to customer data uses unique user accounts
Offboarding: Service Provider's centralized offboarding process promptly disables user credentials.
Event logging: Service Provider's systems forward security events and audit logs to a central Security Information and Event Management (SIEM) solution for monitoring and investigation. Logs are encrypted and log integrity shipping is in place.

Security Assessments
Vulnerability Scans: Service Provider conducts routine vulnerability scans of the Services' systems.
Penetration testing: Service Provider engages independent third parties to conduct annual penetration tests of the Services.
Customer Assessments: Service Provider reasonably cooperates with periodic security assessments carried out by customers.

Business Continuity and Availability
Resiliency: Service Provider takes technological and process measures to ensure the resiliency of the Services.
Continuity Plans: Service Provider maintains and periodically tests appropriate business continuity and disaster recovery plans.

Incident Response
Response Plan: Service Provider maintains an up-to-date incident response plan setting out responsibilities, how information security events are assessed and classified as incidents, and the applicable response procedures.