CLUMIO SECURITY POLICY

Clumio and Customer agree that this Security Policy is hereby incorporated into and made a part of their written agreement that references this policy (the "**Agreement**"). Capitalized terms not specifically defined in this Security Policy will have the same meaning as in the Agreement. To the extent there is a conflict between the Agreement and the terms of this Security Policy, the terms of the Agreement will prevail unless otherwise expressly set forth therein.

Clumio maintains an information security program and a privacy information management program that contain technical, physical, and organizational measures designed to protect data of any type that is uploaded by or on behalf of Customer to the Service for the purpose of storage and retrieval ("**Customer Data**"). This Security Policy describes safety measures that Clumio has in place to protect the security of Customer Data. Clumio may review and update this Security Policy from time to time, provided that such updates shall be designed to enhance and not materially diminish the overall level of protection for Customer Data.

1. Information Security Policies and Procedures. Clumio's information security program includes policies and procedures designed to: (i) maintain the confidentiality, integrity, and availability of Customer Data in Clumio's possession or control; (ii) protect such Customer Data against unauthorized access, use, disclosure, alteration, or destruction; and (iii) identify and mitigate potential threats or hazards to the security of Customer Data.

2. Third Party Management Policy. The security of information assets and information processing facilities will not be reduced by an introduction of third-party products or services. Clumio will align the security of information assets and information processing facilities accessed or managed by third party business partners with security standards no less protective than Clumio's information security program.

3. Physical Security. Clumio utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "**Cloud Provider**") and utilizes such Cloud Provider's data center infrastructure to provide the Service to Customer. To ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Service, Clumio regularly reviews those controls as audited under the Cloud Provider's third-party audits and certifications.

4. Technical Security. Clumio maintains technical security controls designed to: (i) restrict access to its information systems, including firewalls, intrusion detection and prevention systems, access control lists, and routing protocols; (ii) safeguard data on Clumio laptops or other mobile devices or removable storage devices; and (iii) encrypt and protect Customer Data from unauthorized access during electronic transmission, transport, or storage by Clumio. Clumio conducts regular penetration testing or other appropriate security testing and security audits, including third party certifications and audits under ISO 27001, ISO 27701, and SSAE 18 (SOC 2), and is HIPAA- and PCI DSS-compliant.

5. Organizational Security. Clumio maintains policies, procedures, and technical controls to limit access to Customer Data to authorized persons, and to remove access rights promptly in the event of a change in job status. Clumio requires Clumio personnel to comply with its information security program. Clumio maintains a security awareness program to train personnel about their security obligations.

6. Business Continuity and Disaster Recovery. Clumio maintains, implements, and invokes when needed, disaster recovery and business continuity plans to mitigate the effects of natural disasters, emergencies, acts of God, or similar events on Clumio's information systems and the sites that house them ("**BCDR Plan**"). The BCDR Plan incorporates Clumio's contingency plans, recovery plans (including recovery point objective and recovery time objective) and risk controls designed to enable Clumio's continued performance under the Agreement consistent with any applicable recovery time objective specified therein. Clumio regularly reviews and updates these plans.

Last Updated: October 28, 2020