DATA SECURITY ADDENDUM

This Data Security Addendum details the technical and organizational measures that Flooid implements to protect Customer Data in its processing of Customer Data pursuant to the Master Subscription Agreement ("Agreement") and/or Personal Data pursuant to the Data Processing Addendum ("Data Processing Addendum") by and between Flooid and Customer. All capitalized terms not defined herein have the meaning ascribed to them in the Agreement and/or Data Processing Addendum.

1. Encryption of Customer Data

Customer Data is encrypted at rest and in-transit using industry standard encryption technologies within the cloud platform, currently at rest using AES 256-bit encryption and In-transit via Transport Layer Security (TLS) 1.2+ protocol.

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Flooid is ISO 27001:2022 certified, ensuring that it maintains and enforces appropriate administrative, physical and technical safeguards to protect the integrity, availability and confidentially of Customer Data.

3. Measures for ensuring the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident

Flooid has BCPs for all critical systems as identified in our BIA (Business Impact Analysis). These Disaster Recovery and Business Continuity Plans are reviewed, updated and tested at a minimum annually. We have a full cloud DR procedure, more details on this can be provided on request.

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Flooid completes vulnerability testing in line with our Asset Management Policy and annual penetration testing of our infrastructure including cloud.

5. Measures for user identification and authorisation

Access is governed by Flooid's Access Control Policy. Access to Customer Data is provided only to personnel as strictly necessary for the sole purpose of satisfying instructions and as per their role within the company. Other types of relevant controls are password requirements in line with the Flooid Password Policy and multi factor authentication implemented at the corporate level.

6. Measures for the protection of data during transmission

Customer Data is encrypted in transit within the cloud using industry standard encryption technologies, currently via Transport Layer Security (TLS) 1.2+ protocol. Flooid's provisioned secure sharing tool Send Safely enables secure end to end encrypted sharing of data during transmission outside of the cloud platform.

7. Measures for the protection of data during storage

© 2025 Flooid Inc. All rights reserved
Flooid Inc. Protected Information

Customer Data is encrypted at rest using industry standard encryption technologies within the cloud platform, currently AES 256-bit encryption.

8. **Measures for ensuring physical security of locations at which Customer Data is processed**

Flooid relies on cloud service providers for some of its data storage requirements. All cloud data centers hold ISO 27001 and SOC 2 Type 2 certifications. With respect to Flooid's facilities, all physical offices require badge access and utilize video surveillance with secure areas only being made available to authorized individuals.

9. **Measures for ensuring events logging**

Flooid performs logging and monitoring of internal servers that are centrally collected and normalized within SIEM tooling.

10. **Measures for ensuring system configuration, including default configuration**

Flooid has standard gold build processes for internal end user devices and for customer infrastructure using Reference Architecture. These ensure that systems are commissioned and built to a standardized level.

11. **Measures for internal IT and IT security governance and management**

Flooid maintains a robust information security management system governed by the Information Security Team.

12. **Measures for certification / assurance of processes and products**

Flooid maintains both the ISO 27001 & 9001 certification.

13. **Measures for ensuring data minimization**

Any Customer Data collected and processed will not be held or used unless necessary to provide the Subscription in compliance with Flooid's policies.

14. **Measures for ensuring data quality**

Automated processing is used whenever technically or operationally feasible to ensure data quality.

15. **Measures for ensuring limited data retention**

Customer Data is purged in line with the Agreement which is usually ninety (90) days post project closure or upon termination of the Agreement. Data retention is also agreed as part of the solution design with suitable automated procedures for the purging of data to ensure it is only stored for agreed timescales. In some instances it may be the Customer's responsibility to retain data in line with agreed retention periods subject to agreement from both parties.

16. **Measures for ensuring accountability**

Activity logging within the cloud platform is immutable. We use named user accounts within Flooid to ensure accountability. Personnel complete training and acknowledge compliance with Flooid's policies annually or when changes are made.

© 2025 Flooid Inc. All rights reserved
Flooid Inc. Protected Information

17. **Measures for allowing data portability and ensuring erasure**

Flooid may store or process Customer Data as part of provision of services on Google cloud servers which may be transferred to other locations within the cloud platform, upon request.

18. **For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

Flooid maintains a Vendor Security Standard that details minimum vendor security requirements necessary to store, process or transmit Customer Data that provides a baseline of control expectations for the evaluation of each vendor, conformance and risk acceptance based on the nature of the vendor relationship. Suitable transfer agreements such as IDTAs (International Data Transfer Agreements) are also implemented when necessary.

© 2025 Flooid Inc. All rights reserved
Flooid Inc. Protected Information