Last Revised on May 23, 2022

Upstash Technical and Organizational Security Measures

These Technical and Organizational Security Measures ("**Security Measures**") are incorporated into and form part of your applicable agreement with Upstash with respect to your use of Upstash (the "**Agreement**"). The Security Measures set out the security features, processes, and controls applicable to Upstash, including configurable options available to Customer, which employ industry standard information security best practices.

1. Definitions

The following terms have the following meanings when used in the Security Measures. Any capitalized terms that are not defined in the Security Measures have the meaning provided in your Agreement.

1.1. "Cloud Provider" means Amazon Web Services (AWS) or Google Cloud Platform (GCP), as selected by Customer.
1.2. "Customer Data" means any data you or your end users upload into Upstash.
1.3. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.
1.4. "Information Security Program" means Upstash's written security program, policies, and procedures that set forth the administrative, technical, and physical safeguards designed to protect Customer Data.
1.5. "Upstash Cluster" means each replica of data-bearing nodes running the Upstash software that is managed by Upstash, subject to your selected configurations.
1.6. "Upstash Systems" means Upstash's internal infrastructure, including development, testing, and production environments, for Upstash.
1.7. "Privileged User" means a select Upstash employee or third-party contractor who has been granted unique authority to access Customer Data or Upstash Systems as required to perform their job function.
1.8. "Security Incident Response Plan" means Upstash's documented protocols for evaluating suspected security threats and responding to confirmed Data Breaches and other security incidents.

2. Information Security Program Overview.

2.1. General. Upstash maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond to, and recover from security incidents. Upstash's Information Security Program complies with applicable Data Protection Law and is aligned with the NIST Cyber Security Framework (NIST). Additionally, Upstash is in the process of being

certified against SOC 2 Type II.
2.2. Maintenance and Compliance. Upstash's Information Security Program is maintained by a dedicated security team, led by our Chief Cloud Officer. Upstash monitors compliance with its Information Security Program, and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated at least annually to reflect changes to our organization, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Information Security Program in a way that materially weakens or compromises the effectiveness of its security controls.
2.3. Upstash Personnel Controls.

2.3.1. Background Checks. Upstash performs industry standard background checks on all Upstash employees as well as any third-party contractor with access to Customer Data or Upstash Systems.
2.3.2. Personnel Obligations. Any Privileged User authorized to access Customer Data is required to commit in writing to information security and confidentiality obligations that survive termination and change of employment. Upstash maintains a formal disciplinary procedure for violations by Upstash personnel of its security policies and procedures.
2.3.3. Training. Upon hire and subsequently at least once per year, Privileged Users authorized to access Customer Data undergo required training on specific security topics, including phishing, secure coding, insider threats, and the secure handling of Customer Data and personally identifiable information. Further, Upstash implements mandatory, role-specific training for Privileged Users who are authorized to access Customer Data. Upstash maintains records of training occurrence and content. In addition to these mandatory trainings, Upstash offers employees additional training resources, such as internal security reading groups and hackathons.
2.4. Third Parties. Upstash maintains and adheres to a documented process for the evaluation and approval of third-party service providers prior to onboarding, which includes appropriate due diligence regarding each third party's security processes and controls. We require third parties to contractually commit to confidentiality, security responsibilities, security controls, and data reporting obligations.
2.5. Security Contact. If you have security concerns or questions, you may contact us via your normal support channels or by emailing support@upstash.com.

3. Upstash Security Controls.

3.1. Data Centers and Physical Storage. Upstash runs on AWS, and GCP, and you control which Cloud Provider to use for deploying your Upstash Clusters. Each Cloud Provider is responsible for the security of its data centers, which are compliant with a number of physical security and information security standards detailed at the Cloud Provider's respective websites:

- ○ https://aws.amazon.com/security/
- ○ https://cloud.google.com/security/

At least once a year, Upstash performs due diligence of each Cloud Provider, which includes reviewing security compliance certifications.

In addition to selecting which Cloud Provider to use, you also control the region where your Upstash Clusters are deployed. This gives you the flexibility to decide where your Customer Data is physically stored, and you may choose to deploy your Customer Data in a specific geographic region (for example, only within the European Union or only within the United States).

3.2. Encryption.

3.2.1. Encryption in Transit. Upstash network traffic is protected by Transport Layer Security (TLS), which can be enabled by the customer. Customer Data transmitted between nodes of your Upstash Cluster, is isolated inside Cloud Provider's network. You can select which TLS version to use for your Upstash Clusters, with TLS 1.2 being the recommended default and a minimum key length of 128 bits.

3.2.1.1. Key Management Procedures for Encryption in Transit. All encryption in transit is supported by the use of OpenSSL FIPS Object Module. We maintain documented cryptography and key management guidelines for the secure transmission of Customer Data, and we configure our TLS encryption key protocols and parameters accordingly. Upstash's key management procedures include: (i) generation of keys with approved key length; (ii) secure distribution, activation and storage, recovery and replacement, and update of keys; (iii) recovery of keys that are lost, corrupted, or expired; (iv) backup/archive of keys; (v) maintenance of key history; (vi) allocation of defined key activation and deactivation dates; (vii) restriction of key access to authorized individuals; and (viii) compliance with legal and regulatory requirements. When a key is compromised, it is revoked, retired, and replaced to prevent further use (except for limited use of that compromised key to remove or verify protections). Keys are protected in storage by encryption and are stored separately from encrypted data. TLS certificates are obtained from a major, widely trusted third-party public certificate authority. In the course of standard TLS key negotiation for active sessions, ephemeral session keys are generated which are never persisted to disk, as per the design of the TLS protocol.

3.2.2. Encryption at Rest. Upon request of the customer, Customer Data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of your selected Cloud Provider, and the Cloud Provider fully manages the encryption keys.

3.3. Network Connectivity Options.

3.3.1. Network Isolation. Upon request, the customer may choose to deploy Upstash Clusters in a dedicated virtual environment or a shared multi-tenant system. Dedicated Upstash Clusters are deployed in a VPC (for AWS and GCP) that fully isolates your Customer Data and is configured to prevent inbound network access from the internet. Each such Upstash VPC utilizes security groups that act as a virtual firewall for your dedicated Upstash Clusters.

3.3.2. IP Access List. In order to allow inbound network access to your Upstash VPC, you must configure an IP Access List to enable specific networks to connect to the Upstash Clusters within the Upstash Account. Unless the IP Access List for an Upstash Account includes a specific network's IP addresses, network traffic is prevented from accessing your Upstash

Clusters in that Upstash Account.
3.3.3. Virtual Private Cloud Peering. You may enable peering between your Upstash VPC to your own dedicated application tier virtual private network with the Cloud Provider of your choice (VPC). Peering permits you to route encrypted traffic between your Upstash VPC and your own application tier VPC privately, rather than traversing the public internet. Subject to the capabilities of your selected Cloud Provider, you may also choose to peer your Upstash VPC to your application tier VPC across regions.
3.3.4. Private Endpoints. Upstash also supports private endpoints on AWS using the AWS PrivateLink feature. If you enable this feature for any Upstash Cluster, that Upstash Cluster will only allow a one-way connection from your AWS VPC to the Upstash Cluster and that Upstash Cluster cannot initiate connections back to your AWS VPC. Private endpoints also enable you to reach your Upstash Cluster transitively over the network from other application tier AWS VPCs that you have peered with the private endpoint, or through your own self-managed virtual private network including via AWS DirectConnect.
3.4. Configuration Management. The Upstash environment, including our production environment and your Upstash Clusters, leverages configuration management systems to fully automate configuration based on one-time decisions that are securely applied to new and existing environments to ensure consistency every time. Our production environment and your Upstash Clusters use in-house built docker images with secure configuration management applied via industry standard automation software, which includes hardening steps.

4. Access Controls.

4.1. Customer Access. Upstash supports multiple authentication and authorization options and methods to give you the flexibility to meet your individualized requirements and needs. You are responsible for understanding the security configuration options available to you and the impact of your selected configurations on your Upstash environment, which consists of a web application administrative interface ("**Upstash Console**") and any Upstash Cluster you deploy. Upstash provides you with configurable authentication and authorization options for both the Upstash Console and your Upstash Clusters.

4.1.1. Upstash Console Authentication and Authorization. Upstash uses Auth0 as identity management provider. User credentials for the Upstash Console are stored using industry standard and audited one-way hashes. The Upstash Console supports Single Sign-On (SSO).
4.1.2. Upstash Cluster Authentication and Authorization. Upstash follows the Redis and Apache Kafka protocols to provide Authentication and Authorization to the Upstash Clusters. Authentication control for Apache Kafka clusters is enabled by default with the Salted Challenge Response Authentication Mechanism (SCRAM). The customer is able to create credentials with different privileges to access Apache Kafka clusters. The customer can use the Redis ACLs to configure the authorization of different credentials. You can review, limit, and revoke user access to your Upstash Clusters at any time by resetting password.

4.2. Upstash Personnel Access to Upstash Clusters.

4.2.1. Privileged User Access. As a general matter, Upstash personnel do not have authorization to access your Upstash Clusters. Only a small group of Privileged Users are authorized to access your Upstash Clusters in rare cases where required to investigate and restore critical services. Upstash adheres to the principle of “least privilege” with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue. Privileged Users may only access your Upstash Clusters by adding their IP addresses to the IP allowance list, requiring MFA both to log in to our Cloud Providers’ Systems.

4.2.2. Restricting Upstash Personnel Access. Upstash provides customers who have a dedicated virtual environment (3.3.1 in this document) the option to entirely restrict access by all Upstash personnel, including Privileged Users, to your Upstash Clusters. If you choose to restrict such access and Upstash determines that access is necessary to resolve a particular support issue, Upstash must first request your permission and you may then decide whether to temporarily restore Privileged User access for 24 hours. Enabling this restriction may result in increased time for the response and resolution of support issues and, as a result, may negatively impact the availability of your Upstash Clusters. If you enable client-side field level encryption, even Privileged Users will be unable to access Customer Data within your Upstash Clusters in the clear unless you provide Upstash with the encryption keys.

4.2.3. Credential Requirements. Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

4.2.4. Access Review and Auditing. Upstash reviews Privileged User access authorization on a quarterly basis. Additionally, we revoke a Privileged User’s access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by Upstash personnel to your Upstash Clusters. Audit logs are retained including a timestamp, actor, action, and output.

4.3. Upstash Personnel Access to Upstash Systems.

4.3.1. General. Upstash’s policies and procedures regarding access to Upstash Systems adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to Upstash, Upstash developers are only granted access to our development environments, and access to our production environment is limited to Privileged Users with appropriate authorizations. We review access authorizations to Upstash Systems on a quarterly basis. As part of the employee off-boarding process, access to Upstash Systems is revoked within 24 hours of an employee’s departure.

4.3.2. Access to Upstash Production Environment. Our backend production environment that runs Upstash is only accessible by a dedicated group of Privileged Users whose privileges must be approved by senior management. Privileged Users may only access our backend production environment via an allowed IP address both to log in and to establish a SSH.

4.3.3. Credential Requirements. All Upstash personnel passwords must be at least eight characters, including at least one lower case letter, upper case letter, number, and symbol. Passwords may not contain part of a username or the person’s first or last name. Additionally, MFA is mandatory for all Upstash personnel.

4.4. Physical Controls at Upstash Offices. As noted in Section 3.1, Customer Data is deployed at the data centers of your selected Cloud Provider, and not at facilities owned or operated by Upstash. At Upstash offices, we follow industry best practices to employ physical security controls that are appropriate to the level of risk posed by the information stored and the nature of operations at our offices.

4.5. Secure Deletion of Customer Data. If you terminate an Upstash Cluster, it will become unavailable to you immediately and any Cloud Backup associated with that Upstash Cluster will be terminated. Upstash may retain a copy of the Customer Data of the terminated cluster in the backup system for at most 4 weeks.

5. Upstash Systems Security.

5.1. Separation of Production and Non-Production Environments. Upstash has strict separation between production and non-production environments. Our Upstash production environment, your Upstash Clusters, and your Customer Data are never utilized for non-production purposes. Our non-production environments are utilized for development, testing, and staging. Upstash also maintains strict separation of our Upstash production environment and Upstash's development environment using separate cloud accounts.

5.2. Software Development Lifecycle. Upstash has a dedicated security team, reporting to the Chief Cloud Officer, that leads security initiatives in the software development lifecycle (SDLC). We develop new products and features in a multistage process using industry standard methodologies that include defined security acceptance criteria and align with NIST and OWASP guidance. The SDLC includes regular code reviews, documented policies and procedures for tracking and managing all changes to our code, continuous integration of source code commits, code versioning, static and dynamic code analysis, vulnerability management, as well as automated and manual source code analysis.

5.3. Monitoring and Alerting. Upstash monitors the health and performance of Upstash without needing to access your Upstash Clusters. Upstash maintains a centralized log management system for the collection, storage, and analysis of log data for our Upstash production environment and your Upstash Clusters. We use this information for health monitoring, troubleshooting, and security purposes, including intrusion detection. We maintain our log data, and we utilize a combination of automated scanning, automated alerting, and human review to monitor the data.

5.4. Vulnerability Management.

5.4.1. Upstash Vulnerability Scanning. Upstash maintains a documented vulnerability enumeration and management program that identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk, and tracks issue remediation. We conduct quarterly scans of both the underlying systems upon which Upstash is deployed, as well as all third-party code integrated into our products. Upstash's vulnerability management policy requires individual engineering teams to identify known vulnerabilities in system components, and develop remediation timeframes commensurate to the severity of an identified issue. We also utilize automated tooling in conjunction with monitoring security bulletins for relevant software and libraries, and implement patches if security issues are discovered.

5.4.2. Vulnerability Remediation. Upstash uses a central company-wide ticketing system to track all security issues until remediation. We implement patches to our operating system and applications on a need-to-update basis.

5.5. Testing and Internal Risk Assessments. Upstash undergoes regular reviews from security teams. Internally, Upstash undergoes periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns. The Upstash security team is also routinely involved in source code review, architecture review, code commit peer review.

6. Contingency Planning.

6.1. High Availability and Failover. Except the single zone ones, every Upstash Cluster is deployed as a self-healing replica set that provides automatic failover in the event of a failure. Replica set members are automatically provisioned by Upstash across multiple availability zones within a region, providing resilience to localized site failures. All replica set members are full data-bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery. Concurrent writes across replica sets occur in real time. Upstash also offers multi-region deployment options.

6.2. Backups. Upstash utilizes Cloud Backups, which use the native snapshot functionality of your selected Cloud Provider to locally back up your Customer Data. Cloud Backup snapshots are stored with your selected Cloud Provider in the same region as your Upstash Cluster.

7. Incident Response and Communications.

7.1. Security Incident Response Plan. As part of the Information Security Program, Upstash maintains an established Security Incident Response Plan that aligns with NIST and ISO/IEC 27001:2013. In the event that Upstash becomes aware of a Data Breach or other security incident, Upstash will follow the Security Incident Response Plan, which includes: (i) clearly defined roles and responsibilities, including designation of a security incident task force; (ii) reporting mechanisms; (iii) procedures for assessing, classifying, containing, eradicating, and recovering from security incidents; (iv) procedures and timeframes for required notifications to relevant authorities and customers; (v) procedures for forensic investigation and preservation of event and system log data; and (vi) a process for post-incident and resolution analysis designed to prevent future similar incidents. The Security Incident Response Plan is reviewed, updated, and tested annually, including a security tabletop exercise at least once per year.

7.2. Customer Communications. Upstash will notify you without undue delay if we become aware of any Data Breach. Taking into account the information available to us, such notice will include a description of the nature and cause of the Data Breach and the expected resolution time. To the extent possible, we will subsequently update you with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

8. Audit Reporting.

8.1. Third-Party Certifications and Audit Reports. Upon request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor) information regarding Upstash's compliance with the security obligations set forth in these Security Measures in the form of third-party certifications and audit reports.

8.2. Security Questionnaires. No more than once per year, we will complete a written security questionnaire provided by you regarding the controls outlined in these Security Measures.