Last Update: February 3, 2022

Redis Technical and Organizational Security Measures

This document contains the technical and organizational security measures (**"Measures"**) that are applicable to your use of the Redis Enterprise Cloud Services (the **"Cloud Services"**). These Measures are referenced and incorporated into the Redis Data Processing Addendum (DPA) that applies to the Cloud Services. In this document, the terms **"you"** or **"your"** refer to the Redis Enterprise Cloud Customer, while **"we"** or **"us"** refers to Redis. You agree to the following Measures, applicable to your Redis Enterprise Cloud Services, and form a part of your terms of service for the Redis Enterprise Cloud Services, or applicable signed agreement, or data processing agreement with Redis (the **"Agreement"**).

Important Note for On-Premises Software. If you are using another product, such as Redis Enterprise Software that you have deployed yourself, please consult with the applicable Redis Enterprise Software - Security Documentation, as the Measures contained in this document may not apply unless your organization also follows them, and you have enabled the proper security configuration(s) when deploying your Redis Enterprise Software.

1. Redis Measures

1.1. **Written Information Security Program.** Redis maintains a written information security program that is compliant with applicable data protection law. This program takes into account the appropriate administrative, technical, and physical safeguards and is designed to provide a level of security appropriate to the risk presented by the processing and the nature of the data to be protected.

1.2. **Audited Controls.** Redis uses independent third-party firm(s) to conduct audits related to security controls. At least annually, an independent, reputable, third-party firm will investigate and prepare a SSAE 18 Type II, specifically a SOC 2 Type II, compliance report and certification based on such investigations (**"SOC 2"**). The scope of the SOC 2 will cover attestations of availability, security, privacy, processing integrity, disaster recovery, backup, and contingency plans and systems, and confidentiality, as appropriate. Upon your written request, Redis will make a copy of this report available to you (please keep in mind that this report is confidential in nature).

1.3. **Access Controls.** Access to Cloud infrastructure is tightly controlled and periodically audited. Only authorized Redis team members have access to Cloud infrastructure on an as-needed basis, and access is controlled by multiple factors. Redis leverages industry standard measures such as logical and physical security access controls, role-based, least privilege, and strong authentication mechanisms designed to protect data and against unauthorized access.

1.4. **Software Development Life Cycle.** Redis manages information systems using industry standard Software Development Life Cycle (**"SDLC"**) that incorporates information security considerations, defines and documents information security roles and responsibilities throughout the SDLC, identifies individuals having such roles or responsibilities, and integrates Redis' information security risk management process into SDLC activities. The Redis SDLC policy includes internal security testing, third-party penetration testing, and processes for prioritizing identified issues found during testing based on the criticality of the risk, mitigation efforts, and likelihood of exploitation.

1.5. **Data Integrity.** For Redis Cloud Customers, logical separation is a measure used to keep data isolated and safe. Transport layer security (TLS) uses encryption to protect data from unauthorized access while

in transit. Redis strongly encourages you to enable TLS on all Redis databases. Additionally, Redis supports encryption at rest for all cloud providers, with persistence enabled. Redis leverages industry-standard encryption and native encryption key management service provided by the major cloud providers.

2. Monitoring and Notification.

2.1. **Breach Notification.** Redis leverages technology tools to help by alerting our security team of abnormal activity. In the event that Redis discovers or is notified of a security breach that has affected your data, or is likely to result in an exfiltration, unauthorized modification, or otherwise affect the integrity of your data, Redis will (i) notify you of the security breach in writing (generally via email for speed), promptly, but no later than 72 hours from the time Redis is able to reasonably identify and investigate the security breach, or 72 hours from the time that Redis is notified that the security breach has directly affected your data. Redis will work with you to provide applicable information regarding the outcome of its investigation, and such other information as you may reasonably request.

2.2. **Availability Monitoring.** Redis provides periodic updates regarding known outages pertaining to the Cloud Services. For high level availability information of the Cloud Services, please visit our Redis Operations Status page.

2.3. **Security Testing.** Different types of security testing are engaged to achieve different results. Our approach is to use the most suitable method to achieve the right result. Redis conducts a number of different activities including: penetration tests, red team tests, code reviews, and vulnerability scanning.

2.4. **Vulnerability Disclosure Program.** Redis believes that active collaboration with the security research community is a vital part of securing the software and infrastructure that powers our global community of Redis Geeks. Research by the Redis community plays a vital role in helping us spot unanticipated attack vectors or potential blind spots. Visit our vulnerability disclosure program on HackerOne and become an active participant.

2.5. **Supply Chain Monitoring.** We recognize supply chain risk is a threat and we have appropriate processes in place to ensure they meet the security standards we're committed to. Each of our third-party providers undergo thorough reviews to ensure the security of the services being provided.

3. Shared Responsibility; Security Documentation & Configuration

3.1. **Shared Responsibility.** Some aspects of the Cloud Services must be configured by you based on your organization's needs. For example, you as a customer are responsible for the security configurations in your Redis databases and the Cloud Services admin console. You agree that you have read, and understand the Cloud Services shared responsibility model document, available at https://docs.redis.com/latest/rc/security/shared-responsibility-model/.

3.2. **Security Documentation.** By using the Cloud Services, you agree to follow best practices when configuring and deploying the Cloud Services, and to follow the Cloud Services security best practices available at https://docs.redis.com/latest/rc/security/ (the **"Security Documentation"**).

End of Document