Kong

Technical and Organizational Security Measures

Last updated: March 31, 2023

These Technical and Organizational Security Measures ("**Security Measures**") are incorporated into and form part of the Customer's applicable agreement with Kong with respect to its use of Kong products (the "**Agreement"**). Any capitalized terms that are not defined in the Security Measures have the meaning provided in the Customer's Agreement.

The Security Measures set out the security features, processes, and controls applicable to Kong products, including configurable options available to the Customer, which employ industry standard information security best practices.

Except where indicated, these Security Measures apply to the following Kong products:

- **Kong Enterprise:** Kong's customer self-hosted (on-premises) API gateway management software.
- **Kong Mesh:** Kong's customer self-hosted (on-premises) service mesh.
- **Kong Konnect:** Kong's hybrid SaaS and software API lifecycle management platform. The Customer uses the SaaS portion – also sometimes referred to as the "Control Plane" – to configure and monitor the Kong software instances – also sometimes referred to as the "Data Plane" – running in the Customer Network Environment.

1. Information Security Program Overview.

1.1. **General.** Kong maintains a comprehensive written information security program to establish effective administrative and technical safeguards for development of its products and data under its custody or control, and to identify, detect, protect against, respond to, and recover from security incidents. Kong's information security program complies with applicable data protection law and the SSAE / SOC 2 information security frameworks. Additionally, Kong Enterprise, Kong Mesh and Kong Konnect are certified against SOC 2 Type II, and Kong Konnect is assessed against Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 1.

1.2. **Maintenance and Compliance.** Kong's information security program is maintained by a dedicated security engineering team, led by our Senior Vice President, Engineering, and a dedicated Compliance team led by our Vice President, Legal and Compliance. Kong 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 our security controls.

1.3. **Kong Personnel Controls.**

1.3.1. **Background Checks**. Kong performs industry standard background checks on all Kong personnel as well as any third-party contractor with access to Kong systems.

1.3.2. **Personnel Obligations.** All Kong staff are required to commit in writing to confidentiality obligations that survive termination and change of employment and to formally acknowledge adherence to Kong's security and privacy policies. Kong maintains a formal disciplinary procedure for violations by Kong personnel of its policies and procedures.

1.3.3. **Training.** All employees and contractors with access to Kong's systems are required to complete Kong's security awareness and privacy training during onboarding. In addition to the initial training during onboarding, all employees and contractors with system access are required to undergo recertification training annually, as a refresher to the content and re-acknowledgement of compliance with our most current security and privacy policies. Kong maintains records of training occurrence and content.

1.4. **Third Parties.** Kong 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 and security responsibilities and we perform ongoing targeted due diligence on at least an annual basis.

1.5. **Business Continuity and Disaster Recovery.** Kong maintains a documented business continuity and disaster recovery ("**BCDR**") plan to enable the restoration of business operations and ensures availability of information to our customers following the interruption or failure of critical business processes. The BCDR includes clearly defined roles and responsibilities. For Kong Konnect, the BCDR also includes recovery point objectives (RPOs), recovery time objectives (RTOs) and backup and restoration procedures. We review, update, and test our BCDR plan at least annually.

1.6. **Security Contact.** If you have security concerns or questions, you may contact us via your normal Support channels, via support.konqhq.com, or by emailing security@konghq.com.

2. Kong Personnel Access to Kong Systems.

2.1. **General.** Kong's policies and procedures regarding access to Kong's internal infrastructure, including development and testing of Kong products and, for Kong Konnect, production environments, adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to Kong Konnect, Kong developers are only granted access to our development environments, and access to our production environment is limited to a limited number of users with appropriate authorizations. We review access authorizations to Kong systems on a quarterly basis and we review any changes to authorizations for users with privileged access to production environments promptly. As part of the employee off-boarding process, access to Kong systems is revoked within 24 hours of an employee's departure.

2.2. **Credential Requirements.** All Kong personnel passwords must conform to industry-standard complexity rules. Access to Kong internal network resources is controlled by a centralized directory service utilizing single sign-on via our SSO gateway and enforces a multi-factor authentication (MFA) requirement. Role-based access restrictions to specific applications, or other areas are controlled using the directory service framework. Privileged administrative staff have separate, distinct administrative accounts and separate personal work accounts for their daily use, in accordance with industry best-practices.

2.3. **Physical Controls at Kong Offices.** Kong maintains policies and procedures for secure areas and protection. Kong's headquarters office is in a secured building with 24/7 front desk staffing with closed-circuit cameras. All staff are issued a badge by the building's reception and these are tied to specific Kong floors, so that only Kong-issued badges may access Kong floors. The building management has audit trails of access linked to individual staff. All visitors are logged by the front desk and escorted to the applicable areas. We revoke personnel access within 24 hours of termination.

3. Kong Product Security.

3.1. **Software Development Lifecycle.** Kong has a dedicated engineering security team, reporting to the Senior Vice President, Engineering, 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 criteria and align with NIST and OWASP guidance. Kong conducts static code analysis on its releases. In addition, all new code is scanned by Kong’s codebase provider automatically against known CVE vulnerabilities and OWASP Top Ten best practices and is regularly peer-reviewed.

3.2. **Vulnerability Management.** Kong maintains a documented vulnerability reporting and management program. We provide multiple ways in which potential vulnerabilities may be reported to Kong. We conduct vulnerability scans of our releases as well as all third-party code integrated into our products. We also use automated tooling to monitor relevant software and libraries and implement patches if security issues are discovered. We track security issues through remediation using a company-wide ticketing system.

3.3. **Vulnerability Remediation.** We maintain a documented vulnerability remediation program to address confirmed vulnerabilities. We assess vulnerabilities in Kong products using the risk-based FAIR Methodology for Quantifying and Managing Risk [fairinstitute.org]. If a vulnerability is found, Kong determines the severity with the Common Vulnerability Scoring System (CVSS). Critical vulnerabilities are addressed as soon as possible. Development tasks for less severe vulnerabilities are defined as issues for specific patch or other releases in accordance with their severity. Kong 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.

3.4. **Penetration Testing.** The internet-facing components of Kong Enterprise and Kong Mesh, as well as the Kong Konnect production environment, are subject to an external penetration test by a nationally recognized security firm at least once per calendar year. Upon request, Kong will provide the Customer with a summary of the penetration test results and remediation status if applicable. Kong does not allow external testing of its Kong Konnect production platform. Kong conducts application-level security testing using a standard application assessment methodology (e.g., OWASP).

3.5. **Internal Risk Assessment.** Internally, Kong Enterprise, Kong Mesh and Kong Konnect undergo periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns.

3.6 **Customer Responsibilities.** Kong Enterprise and Kong Mesh are self-hosted software applications that run within the Customer's Network Environment. Kong Konnect is a hybrid SaaS and Customer self-hosted product. These Kong products and services enable the Customer to manage, configure and secure their APIs and applications. The Customer is responsible for properly configuring and using the Kong products and services and taking its own steps to maintain appropriate security, protection and backup of its data, including Customer Payload Data.

4. Incident Response and Communications.

4.1. **Security Incident Response Plan**. As part of Kong's information security program, Kong maintains a security incident response plan that aligns with NIST and ISO/IEC 27001:2013. If Kong becomes aware of a security breach for Customer data under its custody or control ("**Data Breach**") or other security incident, Kong 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.

4.2. **Customer Communications.** Kong will notify the Customer in accordance with applicable law 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 the Customer with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

5. Audit Reporting.

5.1. **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 Kong's compliance with the security obligations set forth in these Security Measures in the form of third-party certifications and audit reports.

6. Kong Konnect Security Controls

6.1. **Konnect Data Center Security.** Kong Konnect is a hybrid SaaS and customer self-hosted software solution. The SaaS portion (the "**Control Plane**") is hosted by Kong on AWS. AWS is compliant with a number of physical security and information security standards detailed at the following website: https://aws.amazon.com/security/

At least annually, AWS is subject to due diligence performed by Kong or third-party auditors, which includes obtaining and reviewing security compliance certifications.

6.2 **Konnect Data Center Locations.** Kong currently offers hosting of Kong Konnect in AWS regions in either the United States or Europe. The Customer may elect the region in which they wish their Customer Content to be hosted. They may also limit access to users in the region. This will be at the Customer's discretion and will be selected by the Customer in the Kong Konnect portal. Identity management and authentication to the Kong Konnect service is hosted in the United States.

The Kong software data plane component of Kong Konnect (the "**Data Plane**") runs within the Customer Network Environment, and so in what regions, and in what third-party cloud providers, the Customer chooses to deploy Kong software used with Kong Konnect is the Customer's decision.

6.3. **Kong Konnect Encryption.**

6.3.1. **Encryption in Transit.** All network traffic between the Control Plane and the Data Plane in Kong Konnect is protected by Transport Layer Security (TLS), which is enabled by default and cannot be disabled.

6.3.2. **Encryption at Rest.** Customer Content is encrypted at rest in the Control Plane using AES-256 to secure all volume (disk) data.

6.4. **Kong Konnect Access Controls.**

6.4.1. **Customer Access.** Kong Konnect supports multiple authentication and authorization options and methods to give the Customer the flexibility to meet its individualized requirements. The Customer is responsible for understanding the security configuration options available to it and the impact of the Customer's selected configurations on its Kong Konnect deployment, including the Kong Data Plane software instances in the Customer Network Environment.

6.4.1.1 **Authentication and Authorization for Communications between the Control Plane and Data Plane.** Authentication control for communication between the Kong software runtime instances in the Data Plane in the Customer Network Environment and the Control Plane is enabled by default with mTLS. The Customer provides the public key for the authentication and authorization for the connection between their Data Planes and the Control Plane.

6.4.1.2 **Kong Konnect SaaS Control Plane Authentication.** User credentials for the Kong Konnect Control Plane are stored using industry standard encryption and audited user accounts, and one-way password hashes. The Control Plane supports multi-factor authentication (MFA) through the Customer's identity provider SSO. The Control Plane also supports federated authentication functionality for Single Sign-On (SSO) using OpenID Connect (OIDC). The Customer may establish minimum password requirements (e.g., length, complexity) through its identity provider. The developer portal included with the Control Plane similarly supports authentication through SSO and OIDC and industry standard encryption and audited one-way hashes.

6.4.1.3. **Kong Konnect Authorization**. Kong Konnect allows the Customer to define permissions for individual users or API services managed through Kong Konnect in order to restrict Customer Payload Data and API services that are accessible. The Kong Konnect Control Plane allows the Customer to tailor access controls by combining multiple roles and privileges for particular -9

6.4.1.4. **Customer Logs and Auditing.** Kong Konnect offers auditing that monitors actions in the Customer's Kong Konnect deployment and is designed to prevent and detect any unauthorized access to Customer Content, including create, read, update, and delete (CRUD) operations, encryption key management, and role-based access controls. The Customer is responsible for enabling auditing and selecting the endpoint for the logs.

6.4.2. **Kong Personnel Access to the Kong Konnect Control Plane.**

6.4.2.1. **Privileged User Access.** As a general matter, Kong personnel do not have authorization to access the Customer's Kong Konnect Control Plane. Only a small group of privileged users are authorized to access your Kong Konnect Control Plane in rare cases, where required, to investigate and restore critical services. Access to Kong's systems are based on the least privilege principle. All access is logged and subject to audit.

To further reduce the risk of unauthorized access to systems or data, Kong enforces multi-factor authentication for access to internal systems. Additionally, Kong uses a Privileged Access Management (PAM) solution to control access to our production environments.

6.4.2.2. **Customer Permission-Based Personnel Access.** Kong's technical support team does not have access to the Customer's Control Plane. If Kong determines that access is necessary to resolve a particular support issue, Kong must first request the Customer's permission from authorized Customer personnel. The Customer may then decide whether to provide access. All access is logged and subject to audit.

6.4.2.3. **Credential Requirements.** Kong 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 2.2 also apply to privileged user accounts.

6.4.2.4. **Access Review and Auditing**. Kong 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 Kong personnel to the Customer's Konnect Control Plane. Audit logs are retained by Kong for at least 2 years, and include a timestamp, actor, action, and output. Logs are also available to the Customer if they have enabled the audit logging feature.

6.5. **Kong Konnect Systems Security.**

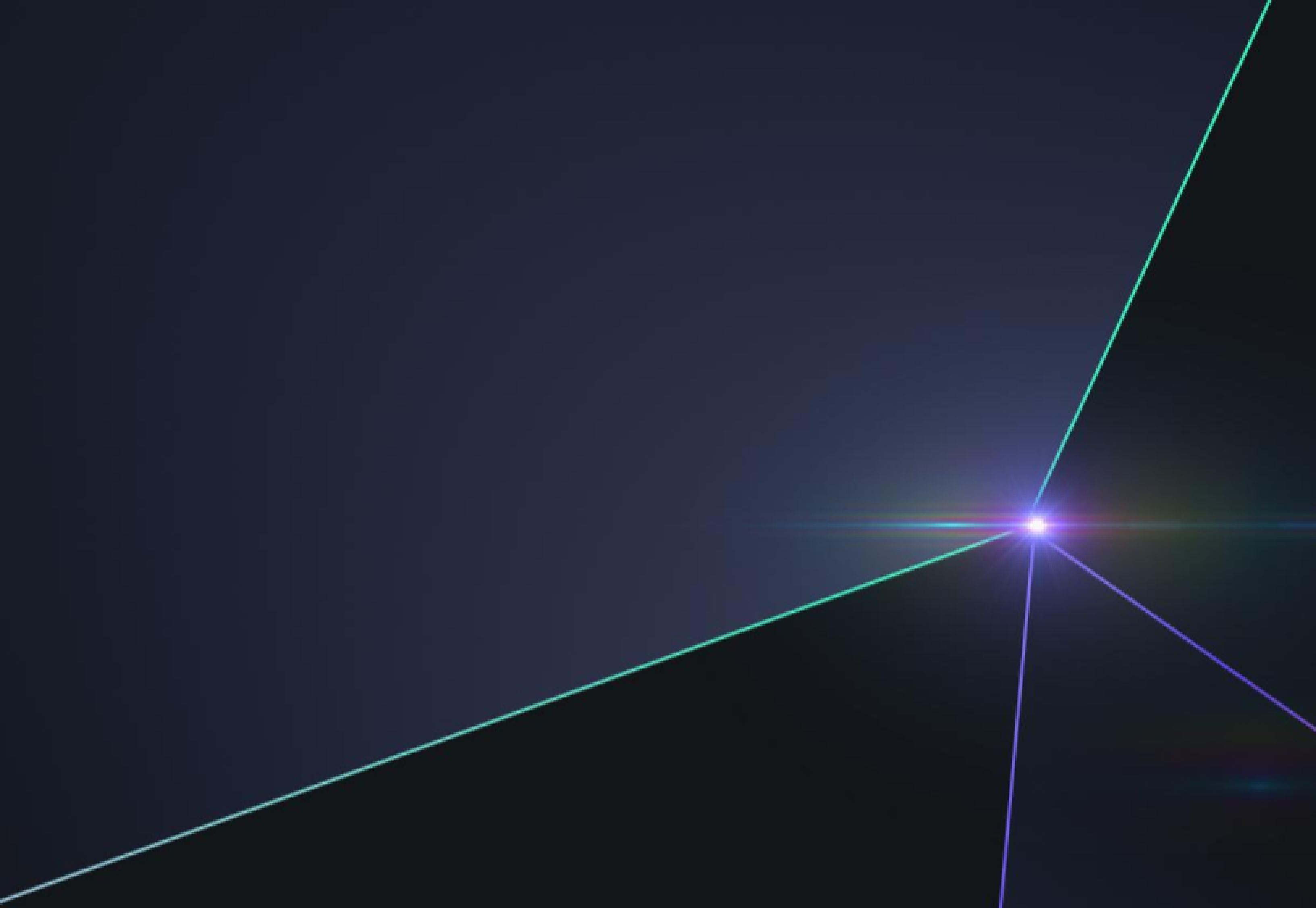
6.5.1. **Separation of Production and Non-Production Environments.** Kong has strict separation between production and non-production environments. Our non-production environments are used for development, testing, and staging. Kong also maintains firewalls to achieve separation of our Kong Konnect SaaS production environment and Kong's internal network.

6.5.2. **Monitoring and Alerting.** Kong maintains a centralized log management system for the collection, storage, and analysis of log data for our Kong Konnect SaaS production environment. We use this information for health monitoring, troubleshooting, and security purposes, including intrusion detection. We maintain our log data for at least two years, and we use a combination of automated scanning, automated alerting, and human review to monitor the data.

6.6. **Kong Konnect Contingency Planning.**

6.6.1. **Availability and Failover.** The SaaS portion of Kong Konnect is a multi-tenant application. It is hosted by Kong in AWS regions in the United States and Europe, with primary / secondary regions and multiple availability zones within a region, providing resilience to localized site failures. Kong Konnect uses redundant servers, load balancing, and other techniques to help ensure that the Kong Konnect service remains available even during hardware or software failures. Concurrent writes across replica sets occur in real time.

6.6.2. **Backups.** Kong Konnect supports replication of databases, clusters and other infrastructure to ensure that data is continuously backed up and that failover systems are ready to take over if the primary system fails. The backups are encrypted at rest.



Konghq.com

Kong Inc.
contact@konghq.com

150 Spear Street, Suite 1600
San Francisco, CA 94105
USA