# Technical and Organizational Security Measures

***Last updated:*** April 16, 2024

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 Gateway Enterprise**: Kong's customer self-managed (on-premises) API gateway management software.
- **Kong Mesh**: Kong's customer self-managed (on-premises) service mesh.
- **Kong Konnect**: Kong's hosted SaaS API management platform. The Customer may use Kong Konnect as (i) a control plane for Kong software instances self-managed by the Customer in the Customer Network Environment, also referred to as Kong Konnect Hybrid, or (ii) a control plane for single tenant Kong Gateway Enterprise instances managed by Kong if the Customer purchases Kong Konnect Dedicated Cloud Gateways.

## 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 Gateway Enterprise, Kong Mesh and Kong Konnect are certified against SOC 2 Type II, Kong Gateway Enterprise is attested against the NIST 800-218 and SLSA level 3 (hardened build) standards, and Kong Konnect is assessed against Cloud Security Alliance (CSA) Security, Trust,

Assurance, and Risk (STAR) Level 1. Further information on Kong's information security certifications and attestations is available at konghq.com/compliance.

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 access to Kong offices is controlled by passcodes unique to each staff member. 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 and Supply Chain Security.** 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 software 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. Our software supply chain practices for Kong Gateway Enterprise are attested against the NIST 800-218 and SLSA Level 3 (hardened build) standards.

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. For our downloadable software, 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 products 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 platform. Kong conducts application-level security testing using a standard application assessment methodology (e.g., OWASP).

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

3.6 **Customer Responsibilities.** Kong products and services enable the Customer to develop, test 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 **Certain Definitions**. The following terms have the following meanings when used in this Section or elsewhere in these Security Measures:

6.1.1. "**AWS**" means Amazon Web Services, Inc.

6.1.2. "**Cloud Gateway Nodes**" means instances of Kong Gateway Enterprise hosted by Kong in AWS as part of the Dedicated Cloud Gateways product. Cloud Gateway Nodes are in the Data Plane for Dedicated Cloud Gateways.

6.1.3. "**Control Plane**" means the part of Kong Konnect used to configure and manage instances of Kong software in the Data Plane.

6.1.4. "**Data Plane**" means the Kong software instances that process the Customer's network traffic including Customer Payload Data. With Kong Konnect Hybrid, the Data Plane runs within the Customer Network Environment. With Kong Konnect Dedicated Cloud Gateways, the Data Plane is hosted and managed by Kong in AWS.

6.1.5. **"Kong Konnect Hybrid"** means a hybrid SaaS and on-premises deployment where the Customer uses Kong Konnect as the Control Plane for Kong software instances self-managed by the Customer in the Customer Network Environment.

6.1.6. **"Kong Konnect Dedicated Cloud Gateways"** or **"Dedicated Cloud Gateways"** means Kong's fully-hosted (SaaS) API lifecycle management product. The Customer uses Kong Konnect as the Control Plane for Cloud Gateway Nodes hosted and managed by Kong in single tenant deployments in the AWS region of the Customer's choice.

6.2. **Kong Konnect Data Center Security.**

Kong Konnect 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.

6.3. **Konnect Data Center Locations.**

6.3.1. **Kong Konnect Control Plane.** Kong currently offers hosting of Kong Konnect Control Planes in AWS regions in the United States, Europe and Australia, with other regions expected to follow. Please refer to the Kong Konnect documentation for current hosting options. The Customer may elect the region in which they wish their Kong Konnect Control Planes 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 platform is hosted in the United States.

6.3.2. **Kong Konnect Hybrid Data Plane**. With Kong Konnect Hybrid, the Kong software in the Data Plane is self-managed by the Customer and runs within the Customer Network Environment. As a result, the Customer decides where to deploy the software, which may include on the Customer's own servers, servers of third party cloud providers or some combination of on-premises and cloud provider deployment.

6.3.3. **Dedicated Cloud Gateways Data Plane**. The Customer controls the AWS region where its Cloud Gateway Nodes are deployed. The region or regions will be selected by the Customer in the Kong Konnect portal. Please refer to the Kong Konnect documentation for current hosting options.

6.4. **Encryption.**

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

6.4.2. **Encryption in Transit to and from the Data Plane.** The Customer controls whether network traffic to and from clients and the Customer's upstream services to the Data Plane is encrypted, and the Customer is responsible for their own configuration. Both http and https are supported. Incoming encrypted traffic is decrypted when the TLS handshake is completed and re-encrypted upon egress. For Dedicated Cloud Gateways, if the Customer uses AWS for its upstream services and has configured its AWS account to attach an AWS Transit Gateway, network traffic may egress from the Cloud Gateway Nodes unencrypted to the Customer's upstream services without going to the public internet.

6.4.3. **Encryption at Rest.** Customer Content is encrypted at rest in the Kong Konnect Control Plane using AES-256 to secure all volume (disk) data. With Dedicated Cloud Gateways, the Customer's network traffic, including Customer Payload Data, is proxied and not at rest.

6.5. **Kong Konnect Access Controls.**

6.5.1. **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.

6.5.1.1 **Authentication and Authorization for Communications between the Control Plane and Data Plane.** Authentication control for communication between the Data Plane and the Control Plane is enabled by default with mTLS. With Kong Konnect Hybrid, the Customer provides the public key for the authentication and authorization for the connection between their Data Planes and the Control Plane.

6.5.1.2 **Kong Konnect Authentication.** User credentials for Kong Konnect are stored using industry standard encryption and audited user accounts, and one-way password hashes. Kong Konnect supports multi-factor authentication (MFA)

through the Customer's identity provider SSO. Kong Konnect 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.

6.5.1.3 **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 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 users. Administrative users can review, limit, and revoke user access at any time.

6.5.1.4 **Customer Logs and Auditing.** Kong Konnect offers auditing that monitors actions in the Customer's Kong Konnect account and is designed to 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.

6.5.2 **Kong Personnel Access.**

6.5.2.1 **Privileged User Access.** As a general matter, Kong personnel do not have authorization to access the Customer's Kong Konnect account. Only a small group of privileged users are authorized to access your Kong Konnect account in rare cases, or, for Dedicated Cloud Gateways Data Plane, 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.

6.5.2.2 **Customer Permission-Based Personnel Access.** Kong's technical support team does not have access to the Customer's Kong Konnect account. 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 to the Customer's Kong Konnect account. All access is logged and subject to audit.

6.5.2.3 **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.

6.5.2.4 **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 Kong Konnect account or, for Dedicated Cloud Gateways, to the Customer's Data Plane. Audit logs are retained by Kong for at least 1 year, and include a timestamp, actor, action, and output. Logs for the Customer's Kong Konnect account are also available to the Customer if they have enabled the audit logging feature.

## 6.6 Systems Security.

6.6.1 **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 production environment and Kong's internal network.

6.6.2 **Systems Configuration.** Kong maintains configuration baselines for its systems supporting the production environment aligned with industry best practices such as the Center for Internet Security (CIS) Level 1 and Level 2 benchmarks. Changes to baselines are limited to a small number of authorized Kong personnel and must follow change control processes. Changes must be auditable and checked regularly to detect deviations from baseline configurations.

6.6.3 **Monitoring.** Kong maintains a centralized log management system for the collection, storage, and analysis of log data for our Kong Konnect and Dedicated Cloud Gateways production environment. We use this information for health monitoring, troubleshooting, and security purposes. We maintain our log data for at least one year, and we use a combination of automated scanning, automated alerting, and human review to monitor the data.

## 6.7 Contingency Planning.

### 6.7.1 Availability and Failover.

6.7.1.1 **Kong Konnect.** Kong Konnect is a multi-tenant application. It is hosted by Kong in AWS regions in the United States, Europe and Australia, 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.

6.7.1.2 **Dedicated Cloud Gateways**. The Dedicated Cloud Gateway Data Planes are single tenant deployments of Cloud Gateway Nodes within the cloud provider region or regions designated by the Customer. If the Customer elects the “autopilot” mode in Dedicated Cloud Gateways, then Kong will scale down to a minimum of two Cloud Gateway Nodes per region to help ensure high availability. If the Customer does not elect “autopilot” mode, then the Customer decides the number of Cloud Gateway Nodes deployed per region.

6.7.2 **Backups.**

6.7.2.1 **Kong Konnect.** 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.

6.7.2.2 **Dedicated Cloud Gateways.** With Dedicated Cloud Gateways, the Customer’s network traffic, including Customer Payload Data, is proxied and not at rest. Kong does not store or backup the Customer’s network traffic or Customer Payload Data that transits through the Cloud Gateway Nodes.