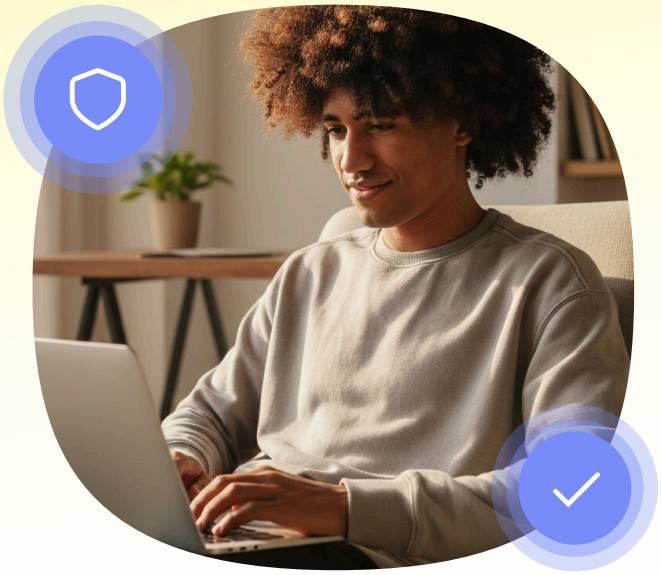
kustomer

Kustomer Security

This document outlines the comprehensive security and confidentiality measures implemented by our organization to safeguard sensitive information and ensure robust system operations. It serves as a testament to our commitment to maintaining the highest standards of data protection and operational integrity for our stakeholders.



Highlights at a Glance

Encryption

AES-256 encryption at rest;
TLS 1.2 encryption in transit

Access Security

Role-Based Access Control (RBAC) + SCIM Provisioning,
IP-based Allow listing, MFA via SSO
(Microsoft, Google, SAML such as Okta or other providers)

Uptime & DR

99.9% uptime SLA; annual DR/BCP tests;
multi-region failover capabilities

Data Masking

PCI-compliant by design: PAN is removed pre-ingestion;
supports manual and automated masking

Org Access Controls

Centralize IP allow listing to access Kustomer, and also restrict Kustomer support from accessing without authorization

Audit Logging

Rich tamper-protected audit logs
to provide assurance

Choose Your Region

Choose your region at onboarding
(U.S., E.U. or India)

Secure API Keys

API keys with role-based permissions, rate limiting,
and expiration dates

Attribute-Level Permissions

Field-level access controls for both standard and custom objects, including masked attributes

Transparency

Real-time status page with historical uptime metrics; audit reports/ certs available under NDA via Kustomer's Trust Center

©2025 Kustomer

Internal Kustomer Security & Privacy Practices

Security Commitments

Compliance

- SOC 2 Type II
- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- GDPR
- HIPAA
- CCPA
- EU-U.S. Data Privacy Framework (DPF)

Kustomer Internal Access Security Controls

Kustomer's internal security systems and configurations enforce role-appropriate access, granting only the permissions required for each role and preventing out-of-scope access. and are implemented through:

- SSO + MFA enforced for all workforce apps
- RBAC & least privilege, with audit logs covering all administrator access
- Quarterly access reviews plus JML (joiner/mover/leaver) deprovisioning SLAs
- Production access via VPN + IP allow listing; no shared creds ensures non-repudiation
- Managed devices via MDM with CIS Level 1 macOS baseline, full-disk encryption, EDR, and patching
- Centralized access logging & anomaly alerting for authentication and privilege changes

Intrusion Detection

We deploy advanced intrusion detection and prevention systems that:

- Detect unauthorized access attempts in real time
- Alert the security team to potential breaches
- Maintain tamper-evident audit logs to ensure integrity and non-repudiation

Vulnerability Management

Our proactive approach includes:

- Continuous vulnerability scanning across the platform, including infrastructure, containers, and application components
- Application security testing built into the SDLC, including Static (SAST) and Dynamic (DAST) analysis
- Responsible disclosure and bug bounty programs
- Cloud-Native Application Protection (CNAPP) for cloud posture management and workload scanning
- Annual internal & external penetration testing of the Kustomer application and APIs
- Responsible disclosure / bug bounty program to enable safe reporting and coordinated remediation
- Defined, enforced vulnerability SLAs with severity-based, time-bound remediation

Incident Management

We have rigorous procedures for managing security incidents:

- Defined incident response protocols (containment, eradication, recovery)
- SLA-driven response times for detection and customer notification
- Breach notification aligned with regulatory requirements

©2025 Kustomer

Data Retention and Disposal

We enforce strict retention and disposal policies:

- Data deletion SLAs are enforced; Policy defined data retention periods
- Secure deletion processes aligned with GDPR and CCPA
- Data lifecycle practices consistent with legal and operational needs

Employee Education and Awareness

- All employees complete annual security awareness training
- Role-based training for staff handling sensitive information
- Regular phishing simulations to maintain awareness

Integrated Management System

Kustomer operates an Integrated Management System (IMS) to manage risks and objectives for security, privacy, and AI. The IMS Committee meets monthly to review risks and track objectives.

Confidentiality Commitments

Data Use

Confidential information is strictly used for contractually agreed purposes. All use is monitored and logged. Employees receive regular training on proper handling of sensitive data.

Vendor Management Processes

Kustomer operates a risk-based vendor management program. We expect vendors and sub-processors that handle Kustomer data or critical services to protect information in line with our security and privacy standards and applicable regulations. Kustomer maintains an up-to-date inventory of all sub-processor DPAs.

High-level expectations:

- Safeguard Kustomer data and use it only to deliver the service.
- Provide reasonable assurance of controls (e.g., recognized reports or a Kustomer assessment).
- Communicate material security/privacy incidents and significant changes.
- Ensure any sub-processors follow equivalent protections.

Privacy Commitments

Data Collection and Use

Personal information is collected and processed solely for purposes defined in privacy notices and agreements. Access is restricted by role, and all processing is logged. Customers have rights to access, correct, or delete data.

Vendor and Incident Management

All vendors with access to personal data are contractually bound to privacy requirements. We conduct regular compliance reviews, DPIAs, and AI/LLM vendor evaluations. Privacy incidents are managed through a documented response process with notification and remediation.

©2025 Kustomer

Availability Commitments

System Resilience

Kustomer ensures availability through redundant infrastructure, load balancing, and automated failover. We provide a 99.9% uptime SLA, with disaster recovery and business continuity tested annually.

Monitoring and Transparency

We continuously monitor system performance and capacity. Customers can access real-time uptime at https://status.kustomer.com and additional resources via our Trust Center.

Tested Business Continuity and Disaster Recovery

We maintain defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for core platform services and test our business continuity and disaster recovery program at least annually. Details are available to customers under NDA via the Kustomer Trust Center.

Infrastructure, Sub-Processors & System Components

Infrastructure & Architecture

Kustomer operates its production environment in Amazon Web Services (AWS). We do not run our own physical data centers; AWS is responsible for the physical and environmental controls, while Kustomer owns the logical, application, and data layers. Traffic enters through HTTPS endpoints into AWS networking components, with infrastructure provisioning and scaling automated to maintain reliability and consistency.

Sub-Processors & Key System Components

Kustomer uses a small number of vetted sub-processors to deliver the service. The list of Kustomer sub-processors is maintained on the Kustomer Trust Center. Kustomer maintains a formal vendor management program, including an inventory of data processed by critical vendors, contractual controls, and periodic risk reviews.

Compliance, Privacy & AI Future-Proofing Roadmap

Kustomer maintains compliance with SOC 2 Type II; ISO/IEC 27001:2022; ISO/IEC 27701:2019; GDPR; HIPAA; CCPA; and the U.S.-E.U. Data Privacy Framework. Audit reports and certifications can be accessed under NDA at https://trust.kustomer.com/. For PCI DSS, we keep scope minimal by preventing cardholder data from entering our systems through edge redaction; i.e., redacting the PAN at the network boundary (ingress).

We do not use customer data to train AI models without explicit agreement. To future-proof our controls and governance, we track NIST post-quantum cryptography standards for readiness, and are actively pursuing compliance and certification with ISO/IEC 42001.

©2025 Kustomer