Data Security Policies and Procedures

Table of Contents:

Overview

As part of our vision to ensure every child is served by inspiring and life-changing educators, KickUp's software collects comprehensive data about the professional growth and professional learning opportunities that teachers experience. We recognize that this data can be personal and sensitive. As the trusted guardians of this data, KickUp takes this responsibility seriously.

This document describes the techniques, technologies, policies, and procedures that KickUp uses to protect your data.

Data Center, Network, and Physical Security

Cloud Hosting and Physical Security

The KickUp application is a cloud-based web application hosted entirely in data centers provided by Amazon Web Services. All physical servers are hosted in an Amazon AWS data center, and benefit from Amazon's security and environmental controls.

AWS's security is regularly reviewed, and they hold an ISO 27001 certification. You can read more about Amazon's physical security here: https://aws.amazon.com/security/

Firewalls and Network Security

All KickUp services and databases are networked using VPCs, a private virtual network technology provided by AWS. KickUp uses VPCs in combination with firewalls to block all unnecessary ports from external traffic and isolate our infrastructure from the rest of the internet.

Hardware Maintenance and Vulnerability Management

System patching and third party vulnerability management

As part of its platform, KickUp relies on software created by other organizations: as part of its hosting infrastructure, in its server operating systems, and in other software dependencies that are bundled as part of the application.

KickUp reviews our software dependencies and server operating systems for available upgrades and security patches at least once per year. Upon learning about a critical patch to address security issues offered by any of its dependencies, KickUp will begin work to upgrade to that patch as soon as possible.

Server Decommissioning

All KickUp application services run in virtualized servers and containers that are provisioned and destroyed on demand.   KickUp does not store any data at rest on servers that execute application code, and the filesystems of these servers are treated as ephemeral.

Change Control and Review

KickUp continuously releases new software in a backwards compatible, low-risk manner. All changes to software and server configurations undergo an internal review prior to deployment, including changes to infrastructure and hosting configurations.

KickUp's engineering team uses source control, peer review of changes, and automated testing to ensure the reliability and quality of all updates to our application.

Employee Access, Assets, and Termination

Employee access to hosting infrastructure
Due to our usage of AWS, KickUp staff do not have physical access to any servers or databases used in the service of the KickUp application.

Electronic access to servers used in the KickUp application is available through a secure SSH terminal. All SSH terminal sessions are encrypted, and password-based access is not enabled. All SSH sessions are authenticated using public/private key pairs, and are logged.

KickUp staff also has access to the infrastructure through the AWS web console and client APIs. Access to these interfaces is differentiated based on role, and two-factor authentication is required to access the AWS web console.

Employee Data Access
KickUp staff may have access to client data, as it pertains to serving our clients.

When accessing client data, KickUp employees are required to only do so on equipment that is owned or furnished by KickUp and has disk encryption enabled.

Employee Termination, Asset Collection, and Access Removal
Upon termination, KickUp collects workstations, laptops, and any other assets from departing employees, and access to KickUp's platforms is terminated. Former KickUp employees are not permitted to retain access to KickUp intellectual property, platforms, or user data.

KickUp's Use of Client Data in Product Development
KickUp maintains a production-replica environment for testing, training, diagnostic, and quality assurance purposes. This environment is regularly loaded with clones of production data, and is secured to the same standards, controls, and techniques as the production environment.

Managing Third Party Service Providers and Vendors, and their Access to Sensitive Data

KickUp partners with third party platforms to provide its service, and these platforms may have access to sensitive user data, including personally identifying information (PII).

KickUp only shares sensitive data and PII with third party partners that have security postures similar to or stronger than KickUp's, including usage of secured data centers and encryption of data at rest. KickUp also maintains a list of third party platforms which have access to PII and sensitive data, and this list can be furnished upon request.

You can read more about how we might use your data in our privacy policy.

Access for Minors

KickUp does not create accounts for students or minors. KickUp will occasionally collect anonymous feedback from students and minors about their teachers, school, etc. When KickUp does collect data from students, it will not require students to create KickUp accounts, instead allowing students to respond anonymously.

Data Collection, Ownership, Export, and Removal

The data we collect
KickUp defines "data" as any data and content owned or controlled by the Client or a Permitted User that the Client or a Permitted User uploads, posts or submits.

The KickUp application collects first name, last name, email address, and IP address for all users who access KickUp.

The product has the ability to store arbitrary metadata, depending on how it is configured. The product could be configured to store any user data, including but not limited to address, phone number, employee id, years of professional experience, their role at their school, or other data. This is a matter of product configuration, and varies from client to client.

Data portability
Personnel (user list and metadata), PD events, form submissions, and event attendance data are all exportable from the KickUp application. Users with administrative privileges are capable of creating exports at will.

Other exports of user data from KickUp can be supplied upon request.

Data removal upon contract termination
Upon termination of the contract, KickUp will assist clients in exporting any data needed and will facilitate the removal of data from KickUp's system, unless otherwise mutually agreed upon.

Database Storage, Retention, Backups, and Encryption

Database Hosting and Network Security

All of our data is stored in AWS data storage solutions, such as their RDS databases and S3 file systems. These data storage solutions are protected as per AWS's standard procedures.

KickUp's RDS database lives in an Amazon Virtual Private Cloud (VPC) and is networked so as to prevent direct access from the public internet.   These services are only accessible from other servers inside of our VPC.

You can read more about Amazon's physical security here: https://aws.amazon.com/security/

Data Backups

Automated backups of our database are made nightly, stored online in multiple geographic locations.

Data Retention

As our backups are stored in our AWS data center, KickUp does not currently dispose of any backups, and does not have a specific policy to do so.

Data Encryption at Rest and in Transit

All user-contributed data and files stored by KickUp are encrypted at rest. Additionally, all user interactions with the KickUp application are done through an encrypted HTTPS channel.

Additionally, user passwords are salted and stored with a SHA256 hash.

Data Isolation / Logical Separation

KickUp uses a multi-tenant architecture, and logically separates data originating from different clients.

Data Residency

KickUp exclusively uses data centers located in the United States.

Intrusion Prevention and Incident Response

Intrusion Prevention

The KickUp application is a cloud-based web app hosted entirely in data centers provided by Amazon Web Services. As such, KickUp benefits from AWS's security protocols, including their internal vulnerability management and intrusion detection.

In addition to AWS's built-in security, KickUp adheres to the additional protocols:

- KickUp audits our server operating systems for available security patches yearly.
- KickUp staff does not have physical access to any servers or databases used in the service of the KickUp application.
- All SSH terminal sessions are encrypted, and password-based access is not enabled. All are authenticated using public/private key pairs. Additionally, all SSH sessions are logged, and trigger notifications that are sent at the start of every SSH session or login.

Denial-of-service attack prevention

The KickUp application uses redundant hardware components, and is able to scale up new hardware and service workers within minutes of increased scale.

KickUp monitors all services for resource utilization, availability, and stability. In the event that an unexpected uptick in requests jeopardizes the stability or availability of any service, KickUp engineering would be alerted immediately.

Incident Response

KickUp follows industry best practices to protect client data, and to ensure the reliability of our systems. Should KickUp become aware of an incident, such as data breach or unauthorized access, we will respond promptly. KickUp will first prioritize removing unauthorized access, protecting your data, and restoring services.   Once the system and data are secured, KickUp will then attempt to identify the root cause and impact of the incident.   Finally, KickUp will notify impacted clients of the nature of the incident, and information about its impact.

Supporting eDiscovery

In the case of a security investigation or e-discovery process, KickUp shall comply with all applicable laws and contractual obligations, as appropriate, under the supervision of KickUp's information security team.

Uptime Guarantee and Scheduled Maintenance

The KickUp application shall be available a minimum of 99.5% of the time during any calendar month, excluding any downtime scheduled in advance as part of planned maintenance.

Due to hardware redundancy, routine maintenance is typically performed without requiring an outage or other user impact. In the rare case in which routine maintenance would require an outage, users will be given at least one week’s notice.

KickUp’s uptime was 99.97% in 2022.

Disaster Recovery and System Resilience

System Scalability

Every layer of KickUp’s architecture is designed to allow for the seamless addition of additional hardware components. This allows us to scale linearly and elastically with demand.   With this strategy, KickUp is confident that it could scale up to accommodate increasing demand and data load within minutes.

System Resilience

KickUp maintains multiple instances of all critical hardware, to ensure automatic failover of individual components. KickUp is architected so that the failure of a single hardware component would not cause a user facing impact.

The simultaneous failure of multiple components of KickUp’s cloud architecture could have a temporary user impact. In the case of simultaneous failure of multiple hardware components, full access to KickUp would be restored within 12-24 hours.

Components of the KickUp application are deployed in multiple availability zones in AWS to ensure reliable levels of service, in case of a failure that is located in a specific availability zone.

Disaster Recovery

To protect against data corruption or data loss, KickUp creates a full database backup once a day, to ensure recovery from a catastrophic failure. These backups are replicated to multiple geographical regions.

Notification of Changes

KickUp shall use commercially reasonable efforts to notify the client in the case of any changes that affect security, storage, or related policies. This would typically involve email notification.