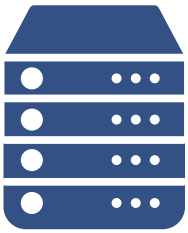
skyprep

SkyPrep Security Overview

Security Overview

Access to Information by Employees



SkyPrep adheres to the principle of least privilege when granting access to customer and personal data to employees. Only specific application developers, as well as designated account managers, have access to customer training data.

All SkyPrep employees must request permission from the customer before accessing their information. This request is either done over an established communication medium (email, Zendesk or phone).

All access to customer information is logged and recorded within the application backend and is auditable, including the time, location and person who access the data.

All employees must ensure confidentiality about both business information, trade secrets and customer and personal information. All employees and contractors agree to these requirements as part of their employment contract.

Application Updates

Updates to the application are first deployed to a staging environment hosting sample data to ensure the application is working correctly.

The application must be tested by designated testers to ensure they meet the product requirements and do not introduce bugs. Once this test is completed, the update is rolled out onto the production environment. Testing usually takes about 2 weeks and updates are pushed out to production once every month on average.

Source Code, Software Updates and Patches

Since SkyPrep is cloud-hosted, we develop, test and push changes of our product to the cloud on a continuous basis. We release minor version updates as often as once a week.

If bugs are reported by our customers and during testing, they are reported to our development and are prioritized by their level of impact and urgency. For example, any vulnerabilities related to security take precedence. We test changes to our product locally using sample data, then test it using staging data and finally roll out updates to our production environment.

Our development process includes continuous integration to ensure quality code. We follow an iterative development process and as such, do not have official version codes (e.g. V1, V2). However, we have internal Git SHA identifier.

Private keys, passwords and security credentials are stored separate from the sourcecode repository in an encrypted container and are manually merged into production servers at deployment time.

Our server infrastructure is updated and patched weekly using officially supported packages for the OS systems we utilize. Security patches are applied daily. Antivirus scanners are ran on servers daily. Security vulnerabilities and risks are addressed based on priority, from those with the highest risk and possible impact, to the lowest.

Data Security

All customer data is encrypted, both within transit (using TLS 1.2) and at rest (stored on AWS RDS database instances using AWS managed encryption keys). Similarly, database backups are encrypted as well. All encryption keys are managed by AWS. Access to the AWS management panel is secured using a strong password as well as MFA authentication.

All API keys using the AWS system are limited in their scope. No API key provides access to all services. This means that in the event of a compromised API key, they will only affect a certain portion of the application.

Any new API key issued must also be limited in scope using AWS IAM policies.This ensures that in the event of compromised API keys, the scope of the unauthorized access is limited.

Data deletion is not possible via APIs which ensures that our AWS-hosted backup data and AWS running instances can not be deleted by via compromised API keys. API keys and credentials are rotated every 6 months to minimize the impact of API key compromises.

Data Protection and Access Policy

SkyPrep takes the security of its service and customers very seriously. Our staff will never access the content and training content of our customers unless we are specifically asked to.

.We employ industry standard security practices including:

- Encryption and hashing of sensitive user data, including passwords and user data.
- Hourly and daily snapshots of our databases and file storage
- Protection of security access tokens and keys
- Use of 2FA tokens using TOTP devices
- Strong password requirements
- Off-site backup of data
- Storage of credit card and payment data on PCI compliant servers
- TLS 1.2 encryption for data transfer across the Internet
- Limiting access to privileged resources using expiring links and permissioned access.
- Private keys, credentials and passwords stored in password-protected encrypted containers or hardware-based KMS

All Internet ports on servers have limited access beyond ports 443 and 80. Access to servers is done via per-employee credentials for VPN. All servers have iptables enabled by default, as well as have AWS built-in port management with restricted access in each VPC.

Our service is hosted on Amazon AWS. Details about their security practices can be found at https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/.

Logical access to customer data is only provided by the authorization of customers upon request for support, which grants temporarily grants our customer service agents with elevated privileges to access your platform for the duration of the support request/ticket.

We follow the principle of least privilege. Only the minimum level of access is provided to SkyPrep employees as required for addressing the support inquiry.

No customer data resides on application servers. Customer data only resides on an AWS-key managed Amazon RDS database that is encrypted with AES-256. Physical security to our infrastructure is provided by Amazon, which follows leading industry standards.

Monitoring and Vulnerability Scanning

We monitor our application continuously for uptime. This information is available publicly at https://status.skyprep.com and our IT staff is notified upon any downtime events that occur. The monitoring interval is real-time and notifications are delivered within the minute.

The application is monitored for new vulnerabilities continuously using a third-party vulnerability scanning platform. SkyPrep also utilizes Sqreen and Snyk to monitor code and be alerted of new risks to either the application code, framework code, server code or OS patches.

Application Security

Application source code is continuously monitored using source-inspection tools for possible security holes. Source code must also be reviewed for possible security holes.

Third-party libraries and gems are also monitored and updated whenever a security hole or risk is identified. Both the head developer and the CTO review and monitor several security-related boards to identify new risks for publically available libraries.

The live application is also internally penetration tested for risks such as CSRF, XSS, bad server configurations, and malware using OWASP PenTesting tool, as well as third-party penetration testing services that report possible security risks to the corresponding IT personnel.

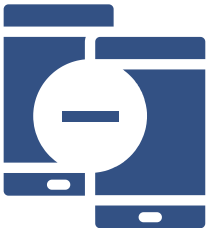
Certification: We are an ADP partner and participate in ADP's GSO Security Audit and do this every 6 months, which includes automated penetration testing, as well as manual security testing for attack vectors such as XSS, CSRF.

Data Breach Policy

In the event of a data breach that involves the personal or business information of a customer, or the personal or business information of individuals relevant to a customer, SkyPrep will notify the administrator(s) or designated IT contact of the customer about the event and reveal the relevant details pertaining to the breach including 1) time and place of the breach 2) scope and type of the data breach including the individuals and types of information affected 3) potential risks associated with the data breach, in accordance with applicable laws.

The client is responsible for disclosing any known data breaches that occur within and outside the confines of their own organization that may potentially affect the data security of any personal or business information that SkyPrep holds on behalf of the client. For example, if the client knows that the user credentials of an individual has been phished or stolen, or has been compromised in any way, the client must notify SkyPrep about the event to limit and mitigate any further potential data loss that may affect the customer, or may affect the customers personal and business information.

Customer Data Retention and Removal Policy



SkyPrep will retain customer data for a period of up to 180 days from the date of service cancellation in the live dataset that SkyPrep users.

If a customer or user requests to have their data removed for personal privacy reasons, such as a GDPR personal information removal request, SkyPrep will take the necessary steps to remove the personal information from within the primary instance of our data within 30 days. However, the customers data may still exist in cold backup archives that are in place in case of a disaster.

In the case that a restoration of the backup data must be put back into production due to disaster recovery, the original data removal request will be honored. The individual can be assured that their personal data will not be restored back to production systems (except in certain rare instances, e.g., the need to recover from a natural disaster or serious security breach).

In such cases, the user's personal data may be restored from backups, but SkyPrep will take the necessary steps to honor the initial request and erase the primary instance of the data again.

Training Smarter, Faster!

www.skyprep.com
hello@skyprep.com
1-855-SKY-PREP
1-855-759-7737

skyprep