DyKnow Cloud Security, Privacy and Architecture Documentation

DyKnow understands that the confidentiality, integrity, and availability of our customers' information are vital to their operations and our own success. We use a multi-layered approach to protect that information, constantly monitoring and improving our application, systems, and processes to meet the changing demands and challenges of privacy and security.

DyKnow Cloud is a SaaS product that runs and stores data in the Amazon Web Services “cloud.” The software runs locally as an installed client on student devices and is accessed via a web browser on teacher devices. This documentation describes the security and privacy-related information and architecture of services branded as DyKnow Cloud.

Data Collection

DyKnow requires customers to provide, and therefore DyKnow stores, the following for product setup:

- Unique SIS (student information system) ID for each teacher and student user
- First name
- Last name
- Username
- Password (optional)
- Email (optional)
- Role (either “student” or “teacher” or “administrator”)
- Unique SIS ID for each course
- Course name
- Course start and end dates

DyKnow collects the following information related to product features[1]:

- URLs visited and applications used by students during a DyKnow class session
- Desktop screenshots of student devices during a DyKnow class session
- Student responses to assessment questions prompted by teacher or self-reported during a DyKnow class session

- [1] DyKnow Cloud “sessions” are started and ended by users with a “teacher” or “administrator” role type.

Third-Party Infrastructure

- DyKnow follows a strict no-sell policy on all customer information
- DyKnow does not use or partner with any 3rd party advertising services
- DyKnow leverages Google Analytics to measure product usage and optimize product performance. Google Analytics reports the geographical region and external IP address of customers actively using DyKnow class sessions
- DyKnow passes error logs, including access tokens, to a 3rd party tool called Loggly. Loggly is used to help DyKnow identify the cause of and aid in the resolution of product errors.

Product Usage Restrictions

DyKnow customers configure when the DyKnow Cloud product can and cannot be accessed and run by their users. This includes limiting use by day/time as well as by IP address. The most common use of limiting user access is to prevent student devices from being monitored by DyKnow Cloud teacher users outside of school hours and campus Internet boundaries. Restricting usage includes preventing the collection of URLs visited and applications used, desktop screenshots and student responses to assessment questions.

Network Operations Center Management and Security

- DyKnow performs regular penetration testing, vulnerability management, and intrusion prevention. This is done via DyKnow's service provider Amazon Web Services. See Amazon's documentation here for additional information.

Are all network devices located in secure facilities and under controlled circumstances?

- Yes, see the above link.

Are backups performed and tested regularly and stored off-site?

- Yes, see the above link.

How are these backups secured? Disposed of?

- See the above link.

Are software vulnerabilities patched routinely or automatically on all servers?

- Yes.

Data Storage and Access

Will any data be stored outside the United States?

- No.

Is all or some data at rest encrypted?

- DyKnow user passwords are hashed.

How will the information be stored?

- DyKnow's platform is multi-tenant, but each customer is assigned its own silo or "vanity" which identifies a specific customer and requires specific login credentials. Customers cannot access data between silos.

Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry or theft?

- Yes, see Amazon Web Services security practices.

How does the provider protect data in transit?

- All data is sent via securely via HTTPS. There is no multicast or P2P data transfer.

Who has access to information stored or processed by the provider?

- Customer users with the role type of "Administrator" can always access and manage the data they provided that has been imported into DyKnow. DyKnow does not access customer information except in the events of: maintaining service, preventing or responding to technical service problems, and/or at the customers' request in connection with a customer support issue. DyKnow Product Architects and Developers and Customer Success Managers have access to all customer data. Customers have access to their own data.

Does the provider subcontract any functions, such as analytics?

- DyKnow development operations are partially supported by a third party consulting firm. This firm has access to product usage analytics. In the event DyKnow chooses to outsource other product development, consultants do not have access to customer data.

What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?

- DyKnow creates an account with administrator role privileges for the individual listed on the sales purchase order. This provides administrator role access to their school silo/vanity only. Customer access privileges are per account type. DyKnow contacts the agreed upon or established customer project lead(s) to verify inbound requests from users DyKnow has no record of. DyKnow maintains an internal account with administrator role privileges that has access to all customer data for the purposes of account management and product troubleshooting.

How is student data transferred/uploaded to the provider?

- DyKnow requires student data be transferred via Secure File Transfer Protocol (FTPs or sFTP).

Data and Metadata Retention

Can a customer access raw data?

- Upon customers' written request, DyKnow may deliver a delimited file containing all data originally provided by the customer. This may include but is not limited to user first name, user last name, username, email addresses, course numbers, course names, Student Information System (SIS) unique identifier numbers, etc.

How and when is data deleted?

- To maintain user privacy and keep customer costs low, data is de-identified at the written request of individual customers. De-identified data is defined as "information that has been stripped of information that is unique to and could be used to identify a particular individual, facility, or client."

How long does the provider keep data?

- DyKnow may keep de-identified data forever.

Development and Change Management Process

DyKnow follows standardized and documented procedures for coding, configuration management, patch installation and change management for all servers involved in delivery of contracted services.

DyKnow notifies customers about any changes that will affect the security, storage, usage or disposal of any information received or collected directly from the customer.

Availability

Does the provider offer a guaranteed service level?

- DyKnow reports real-time uptime status as well as historical uptime statistics at status.dyknow.com.

What is the backup-and-restore process in case of a disaster?

- DyKnow completes daily backups and in the case of a disaster, will restore data to the most recent product backup.

What is the provider's protection against denial-of-service attack?

- See AWS security practices.

Data Breach, Incident Investigation and Response

What happens if the provider has a data breach?

- DyKnow will promptly notify impacted customer(s) of any actual or reasonably suspected unauthorized disclosure of their respective data to the extent permitted by law.

Will the provider assist you in investigation? For example, does the provider log end user, administrative and maintenance activity and are these logs available to the customer?

- Upon customers' written request, DyKnow may provide a log of end-user, administrative and maintenance activity

Parents

DyKnow Cloud is sold and licensed exclusively to schools. Access to the DyKnow Cloud platform is neither sold nor distributed to parents. DyKnow Cloud does not require students to disclose any information to the platform. To request details on a child's personal information, parents must request details via the purchaser, their child's school administrator.

Notice

In the event of changes to this Privacy Policy, DyKnow will update users by email using the email address provided in product data imports. Notice will take place prior to changes taking effect.