



Data Security and Privacy Plan

Last updated: 16 October 2023

Data security and privacy plan	3
Kognity Data security and privacy plan	3
1. Purpose	3
2. General security assurance frameworks	3
3. Application	4
4. Hosting and data storage	4
5. Segmentation of production environment	4
6. Kognity’s disaster recovery and backup	4
7. Kognity’s business continuity plan	5
8. Access and authentication	5
8.1. Minimal access policy	5
8.2. Authentication	5
8.3. Password protection	5
8.4. Logs	5
8.5. Physical security	5
9. Encryption	5
9.1. Encryption at motion and rest	5
9.2. Encryption at file level	6
10. Vulnerability and penetration scans	6
10.1. SOC	6
10.2. End point detection	6
10.3. Network	6
11. Data de-identification and data destruction	6
12. Staff compliance	6
12.1. Training	6
12.2. Background checks	7
13. Subcontractor compliance	7
14. Privacy and security risk assessments and remediation	7
14.1. Platform	7
14.2. Organization	7
14.3. Governance	7

Data security and privacy plan

Kognity's Data security and privacy plan is a guiding document for security and privacy and the implementation and documentation of security frameworks and controls and compliance tracking with customers, third party vendors, independent auditors and regulatory agencies.

Kognity Data security and privacy plan

1. Purpose

The purpose and scope of this policy is to direct Kognity's design, implementation, and management of an effective information security program for all sensitive information on students, teachers, and other individuals received from customers of its education products and services in the United States.

Kognity's Information Security Policy provides an overall information security governance framework and describes management practices such as the responsibilities of the Head of Information Security. The responsibilities, amongst other thing, include:

- Implementing and ensuring information security at Kognity and providing leadership to the enterprise's information security organization
- Implementing and ensuring data privacy at Kognity
- Ensuring compliance with laws and regulations
- Raising awareness of risk management
- Monitoring all operations and infrastructure by reviewing alerts and logs to track the organization's digital security impact

Kognity's Incident Management Policy maintains the approach and responsibility of the Incident Management Team (IMT). IMT are responsible for logging, tracking, investigating, resolving and reporting incidents in the organization. The Incident Management Policy is available on request.

2. General security assurance frameworks

This information security policy describes the administrative, technical, and physical safeguards Kognity utilizes to protect sensitive education information. Kognity's information security program is based on and aligns with the following standards:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1
- The International Organization for Standardization (ISO) Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27001:2017
- Systems and Organization Controls (SOC) SOC2 Type 1 and SOC2 Type 2 - Security principles



Our commitment towards SOC2 has been independently audited and verified through our **SOC 2 type I attestation report**, which is available on request subject to customary non-confidentiality underwriting.

3. Application

Kognity leverages Salesforce Heroku (Heroku) as its platform hosting provider (Platform as a service, PaaS) which is hosted on top of Amazon Web Services (AWS) as its infrastructure hosting provider (Infrastructure as a service, IaaS).

4. Hosting and data storage

Kognity uses the benefits of the cloud and hosts its platform data in AWS and Heroku data centers, located in the US. In order to deliver the platform and a great user experience to customers, Kognity relies on these trusted subprocessors (subprocessor list is available [here](#)). Each subprocessor has been thoroughly evaluated for their information security and privacy program, and to always include legally valid transfer mechanisms (such as EU-US Data Privacy Shield or adopting the Standard Contractual Clauses). This is a recurring process on an annual basis which is a key principle for Kognity and the vetting team. This is maintained in a record of processing activities list.

Within Heroku, Kognity utilizes Customer Application Isolation, which provides an isolated cloud environment within Heroku, and cannot interact with other applications or areas of the system.

More information available at: [Heroku security](#) and [AWS security](#).

5. Segmentation of production environment

Production environments are **completely separate** from testing and development environments, applying different permission, logic, environment variables, data storage and network across the technology stack. Development environments and testing environments contain **no customer data**, only testing data, and are spun up as needed and destroyed once used.

6. Kognity's disaster recovery and backup

Kognity has adopted appropriate disaster recovery and backup policies and procedures, including, among other things, those described in this plan. In order to recover from a total system failure, Kognity will redeploy the platform code, and reconfigure proxy, caching and database settings depending on where the failure occurred.

Kognity is able to set up a new database instance from the daily database backups, and address the platform interface with the new database within 24 hours. Kognity's database is also running on High availability (HA) plan which means that the database cluster and management system is designed to increase database availability in the face of hardware or software failure that could potentially lead to downtime.



7. Kognity's business continuity plan

Kognity has adopted appropriate Business Continuity policies and processes including, among other things, those described in this plan. Kognity utilizes the power of cloud hosting, meaning that Kognity keeps the server instances as interchangeable commodities as far as possible. Kognity also notifies relevant staff of technology outages, as required, and provides them with recurring updates. Furthermore, Kognity will also notify other stakeholders and customers as required and appropriate in the event of an outage. Kognity is also to administer and convey a redundant backup plan, internally, if a hosting partner is unavailable.

8. Access and authentication

8.1. Minimal access policy

Kognity ensures internally that each user is assigned the minimum permission levels needed in order to perform job functions. This includes both the breadth of access (what data is available) and the depth of access (what actions the user is able to perform on that data), as per the principles of Privacy by Design.

8.2. Authentication

Kognity is internally enforcing multi-factor authentication (MFA) on email and corporation accounts, and single-sign-on (SSO) where MFA is not applicable.

8.3. Password protection

Internal privileged accounts require MFA authentication. All well-known infrastructure accounts are centrally managed by a digital vault, secure password manager, encrypted by AES-CBC-256. All privileged accounts used by third party applications are vaulted.

8.4. Logs

Kognity's customers have access to the platform audit log with basic information of students, classes and teachers added, removed or changed. The retention period for the audit log is one year.

8.5. Physical security

Kognity's office is protected 24/7 365 by a third party security firm. Additionally, Kognity office is protected by locked access, requiring badge access and enforcing a clean desk policy.

9. Encryption

9.1. Encryption at motion and rest

Kognity is encrypting data in both motion and at rest. Data in motion is encrypted by SSL and TLS protocol (TLS 1.2 or 1.3) and data at rest is encrypted by AES-256.

9.2. Encryption at file level

As Kognity is leveraging cloud first environment as its primary file and document hosting, all data is encrypted in motion and at rest.

10. Vulnerability and penetration scans

10.1. SOC

Kognity has a security operation center (SOC) monitoring any kind of threat, exploit or vulnerability tied to our different solutions. The platform is regularly checked for any known vulnerabilities or other threats by a third party, and is also subject to cyclic penetration tests.

10.2. End point detection

Kognity deploys an End-point Detection and Response (EDR) solution that helps protect Kognity computers against different cyber threats and exploits.

10.3. Network

Kognity is enforcing Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) at the highest level possible of security at the office network. These are monitored and maintained by a third party to always remain at the highest level of security.

Kognity is utilizing a network firewall monitoring all internet traffic. This is also monitored and maintained by a third party to ensure that all traffic is analyzed and remaining with the highest level of security.

11. Data de-identification and data destruction

Kognity does not retain data that have not been de-identified beyond the time period required to support a customer's utilization of Kognity's products. Kognity considers data as "de-identified" when all personal identifiers (such as name and email) have been removed or obscured such that the remaining information does not permit an individual's identity to be personally identifiable, taking into account all reasonably available information. Where data are de-identified, appropriate safeguards against re-identification are deployed. In addition, procedures are in place to delete data on customer requests (school or district).

Only de-identified data are used for Kognity's ongoing analysis and evaluation.

Sensitive data are manually removed from all devices prior to a full manufacturer reset to reset all devices to factory default settings in line with NIST 800-88.

12. Staff compliance

12.1. Training

Kognity has adopted an appropriate training program including, among other things, the following:

- New joiners: mandatory privacy and information security training for new joiners



- Annual trainings: mandatory privacy and information security training for all of staff (in addition to the new joiner training)
- Semiannual trainings: information security trainings is held twice a year for all of staff

12.2. Background checks

In addition to customary reference checks etc, criminal background checks are conducted in connection with employment in relation to staff that may have access to platform data.

13. Subcontractor compliance

Kognity will not share customer data to subcontractors or other third parties without customer consent or defined third parties in Kognity's subprocessor list.

14. Privacy and security risk assessments and remediation

14.1. Platform

When new platform functionality or features are introduced, it will be evaluated if it will impact personal data handling before progressing to our Continuous integration (CI) pipeline. The CI will trigger a test suite (backend, frontend and end-to-end). If the tests are passed and another developer has approved the code through an independent code review, that will continue to manual validation and testing. If that passes the tests, it can be merged with the rest of the code. This will trigger the test suite once more and if that passes the code will be merged into production and automatically redeployed on Kognity's hosting providers servers as part of Kognity's continuous deployment (CD) pipeline. The platform is also subjected to weekly automatic penetration testing and regular third party vulnerability scanning and alerts.

14.2. Organization

Kognity produces an annual report describing the security measures and initiatives taken throughout the year. This report states the current status of both the platform and the organization. An annual internal audit is conducted to describe how well the Information Security Management System is functioning and executing within the organization.

14.3. Governance

Penetration's executive summary report and Kognity's yearly security report can be shared with customers upon request subject to nondisclosure agreement.

We look forward to radically improving learning together with You!