(k)Nudging

DATA SECURITY POLICY

(k)Nudging

Matthew D. Miko
matthew.miko@knudging.com
801.245.0579

www.knudging.com

VERSION 1.3

Version History			
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**
1.1	Matthew Miko	12Jan2021	-initial document created
1.2	Matthew Miko	27Feb2021	-updated data access controls
1.3	Matthew Miko	24Feb2022	-general revisions

Overview

(k)Nudging LLC (hereinafter referred to as "(k)Nudging," "we," "our," or "us") is committed to the privacy, protection, and security of data provided by our educational partners as it is related to our website, knudging.com, and our applications. This overview of knudging.com's information security program describes physical, technical, and administrative safeguards knudging.com implements to protect student personal information entrusted to us. While it is not possible to completely secure against all threats, we believe that by following the industry best practices, we provide appropriate protections for student personal information in our care.

Knudging.com leverages Digital Ocean (DO) as its cloud hosting provider. Within DO, knudging.com utilizes Virtual Private Clouds (VPCs) to provide isolated cloud environments within the DO infrastructure. External network traffic to a VPC is managed via gateway and firewall rules, which are maintained in source code control to ensure that the configuration remains in compliance with the (k)Nudging data security policy. In addition, the production VPCs and the development VPCs are isolated from each other.

Compliance/Certifications

Knudging.com is hosted using Digital Ocean data centers in the NYC1 location which conform to the highest standards of physical security and processes and have achieved **ISO 27001** and **SOC 2** certifications. See the Digital Ocean Trust Platform documentation and the individual **ISO-27001** and **SOC-2** certification reports.

The US. Family Educational Rights and Privacy Act (**FERPA**) is designed to protect student identity and academic information from unauthorized disclosure to third parties. Knudging.com complies with all relevant provisions as follows:

- Student account information is private in the system, viewable only by authorized faculty and IT administrators. Such permissions must be explicitly granted within knudging.com.

- Student grade information is accessible only to authorized instructors, reviewers, IT administrators, and to the individual student themselves.

- Authorized knudging.com staff may access the account information solely for the purpose of providing service and support to instructors and students. Such access is limited to authorized service and support staff only.

Knudging.com complies with the Children's Online Privacy Protection Act (**COPPA**) by obtaining consent through institutional customers, honoring requests for data deletion, and implementing appropriate data privacy and security safeguards. Key elements include:

- Users (teachers, administrators, etc.) who post videos that include children under 13, such as classroom observations, are required by our User Terms to obtain parent/guardian permission prior to posting.

- Parents may request removal of any video of their child by directly contacting knudging.com.

- Children under 13 years of age are expressly prohibited by our User Terms from creating their own account.

Knudging.com is compliant with the California Consumer Privacy Act (**CCPA**), including all applicable consumer rights in control of their personal data. Please see CCPA-specific rights and terms in our Privacy Policy.

Data Access Controls

Knudging.com's access control principles require all student personal information stored on behalf of customers is only accessible to institution-authorized users and to a limited set of internal knudging.com users who may only access the data for purposes authorized by the institution. Institutions maintain control over their internal users and may grant or revoke access at any time.

In limited circumstances and strictly for the purposes of supporting institutions and maintaining the functionality of systems, certain knudging.com users may access knudging.com systems with student personal information. All such access to student personal information by knudging.com technicians or customer support requires both authentication and authorization to view the information.

Knudging.com encrypts all student personal information in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes. Knudging.com encrypts student personal information at rest using the industry-standard AES-256

encryption algorithms. All database connections require SSL connections and a private SSL certificate to establish a connection.

Knudging.com follows the standard LTI specification. For more information on the required and recommended fields in this spec, see the IMS Global Learning Tools Interoperability® Implementation Guide. When the knudging.com tool is integrated, knudging.com receives the following user specific information:

- School ID (tool_consumer_instance_guid): Unique alphanumeric code sent from LMS
- School Name (tool_consumer_instance_name): Name of your school
- Course ID (context_id): Unique alphanumeric code sent from LMS
- Course Name (context_title): Name of your course
- Assignment ID (resource_link_id): Unique alphanumeric code sent from LMS
- Assignment Name (resource_link_title): As entered during assignment set up
- User Name (lis_person_name_full): Name in LMS
- User Email (lis_person_contact_email_primary): User's email sent from LMS
- User ID (user_id): Unique alphanumeric code sent from LMS
- User Role (roles): Role in LMS course

Knudging.com supports the latest LTI Version 1.3 specification and IMS Security Framework which includes OAuth 2.0, OpenId tokens, JSON Web Tokens, and other security measures.

Application Security

Permissions within knudging.com applications are designed on the principle that institutions control access to all student data. To facilitate this, knudging.com applications are designed so that roles and permissions flow from the institution to the individual user. Our developers follow the principle of least privilege which is a security best practice to only grant users and roles the minimum level of access needed to perform their tasks.

Security controls within applications are used to ensure that the desired privacy protections are technically enforced within the system. For example, if an instructor is supposed to see only the data related to his or her classes, knudging.com ensures that, throughout the design and development process, our products restrict instructors from seeing records for any students outside his or her classes.

To make sure knudging.com applications properly enforce permissions and roles, our development teams conduct reviews early in the design process to ensure roles and permissions are an essential component of the design of new applications.

Knudging.com applications are also developed to minimize security vulnerabilities and ensure industry-standard application security controls are in place.

As part of the development process, knudging.com has a set of application security standards that all applications handling student personal information are required to follow, including:

- Student personal information is secured using industry standard encryption when in transit between end-users and knudging.com systems.
- Applications are built with password brute-force attack prevention
- User sessions expire after a fixed period of time

Knudging.com conducts manual and automated static code analysis as well as dynamic application security testing to preemptively identify vulnerabilities published by industry leaders such as Open Web Application Security Project (OWASP) and SANS Common Weakness Enumeration (CWE).

Proactive Security

Knudging.com periodically conducts risk assessments, aimed at identifying and prioritizing security vulnerabilities. An information security team coordinates remediation of the vulnerabilities. The team also provides ongoing advice on current risks and advises on remediation of vulnerabilities and incident response. Our IT team monitors the Common Vulnerability and Exposure (CVE) reports to eliminate potential vulnerabilities as quickly as possible.

Knudging.com ensures that its systems are free of known vulnerabilities in several ways. Every production server runs vulnerability detection software that compares the installed software against a global database of known vulnerabilities. Secondly, we employ real time network monitoring that reports on any potentially malicious traffic. In addition, we continually review all our system logs for potential security breaches. Lastly, we continually test our applications against common malicious internet traffic. Violations in any of these areas will alert one of our teams, who are available around the clock.

Access to production systems at knudging.com is restricted to a limited set of internal staff to support technical infrastructure, troubleshoot customer issues, or other purposes authorized by the institution. Password based logins are disabled on production servers. Staff must use SSH keys to remotely access any host system. This prevents password guessing or brute force password attacks against our systems. Some systems, such as database clusters, restrict access to internal networks.

Knudging.com utilizes two-factor authentication methods for access to some systems. Two-factor authentication involves a combination of something only the user knows and something only the user can access. For example, two-factor authentication for administrative access could involve entering a password as well as entering a one-time pass code sent via text message to the administrator's mobile phone. The use of two-factor authentication reduces the possibility that an unauthorized individual could use a compromised password to access a system.

Network filtering technologies are used to ensure that production environments with student personal information are properly segmented from the rest of the network. Production environments only have limited external access to enable customers to use our web interfaces and other services. In addition, knudging.com uses firewalls to ensure that development servers have no access to production environments.

Other measures that knudging.com takes to secure its operational environment include system monitoring to detect anomalous activity that could indicate potential attacks and breaches.

At knudging.com, we believe that protecting student personal information is the responsibility of all employees. We provide comprehensive information security training program that all employees undergo upon initial hire, with an annual

refresher training. We also provide information security training for specific departments based on role.

Reactive Security

Knudging.com implemented intrusion detection and prevention systems (IDS/IPS) to monitor the network and report anomalous activity for appropriate resolution.

Knudging.com maintains a comprehensive Security Incident Response Policy Plan, which sets out roles, responsibilities and procedures for reporting, investigation, containment, remediation, and notification of security incidents.

Disaster Recovery

The knudging.com databases are fully managed, high performance database clusters to provide high availability to our customers. Our database clusters have automated failover, meaning they automatically detect and replace degraded or failing nodes. If a primary node fails, the service remains available. A standby node is immediately promoted to primary and begins serving requests while a replacement standby node is provisioned in the background. If there are no running nodes to copy data from, the database cluster re-provisions nodes using the most recent backup and the write-ahead log to recover the database to as close to the point of failure as possible.

Knudging.com provides point-in-time-recovery (PITR) to customers with full cluster backups taken on a daily basis and we maintain write-ahead-logs to allow us to restore a database to any point-in-time within the previous seven days. Additional backups are taken periodically to provide additional recovery options. All backups are stored in the cloud using redundant storage devices.

All knudging.com database engines and their operating systems are automatically updated every week to ensure they have the latest security patches and keep out applications stable. All data is encrypted at rest using LUKS and encrypted in transit using SSL. Every database node is automatically monitored, and our IT team is immediately alerted when certain metrics rise above or fall below various thresholds we have setup.

The knudging.com applications are run on multiple nodes using a load balancer to distribute the work evenly. Our IT team is immediately alerted if a node fails or any nodes experience performance related issues. Additional nodes can be added in

the event a node fails or more nodes are needed to maintain adequate performance.

Contact Information

We welcome your questions and comments about this policy. You can contact us at info@knudging.com.