

DATA SECURITY POLICY

(k)Nudging

Matthew D. Miko

matthew.miko@knudging.com

801.245.0579

www.knudging.com

VERSION 1.5

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
1.4	Matthew Miko	04Mar2024	-align to new product offering
1.5	Matthew Miko	11Jul2025	-minor verbiage changes

Overview

(k)Nudging (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 data 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 data in our care.

Knudging.com leverages Digital Ocean (DO) as its cloud hosting provider. Within DO, knudging.com utilizes the DO App Platform, Platform as a Service (PaaS) to provide isolated application environments within the DO infrastructure. External network traffic to the PaaS is managed via gateway and firewall rules and are in compliance with the (k)Nudging data security policy. In addition, the production PaaS and the development PaaS 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:

- Knudging.com does not store any student data. Data may appear in error logs for a limited amount of time.
- Student data is transmitted to the Knudging application server and then to the client’s AI server. The data is encrypted during transit using TLS/SSL.

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:

- 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 does not store any user data nor track users. Data may appear in error logs for a limited amount of 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 error logs with student data. All such access to student data by knudging.com technicians or customer support requires both authentication and authorization to view the information.

Knudging.com encrypts all student data in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes.

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 data are required to follow, including:

- Student data 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.

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 from an authenticator app or text message sent 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 data 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 data is the responsibility of all employees. We provide a 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 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 runs within the Digital Ocean App Platform platform as a service. Instances of the knudging application are created as needed to maintain performance. The instances are automatically built from tag released on our GitHub source code repository. In the event of a failure of one instance, a new

instance is automatically created. The Digital Ocean App Platform is similar to the Google App Engine platform.

Contact Information

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