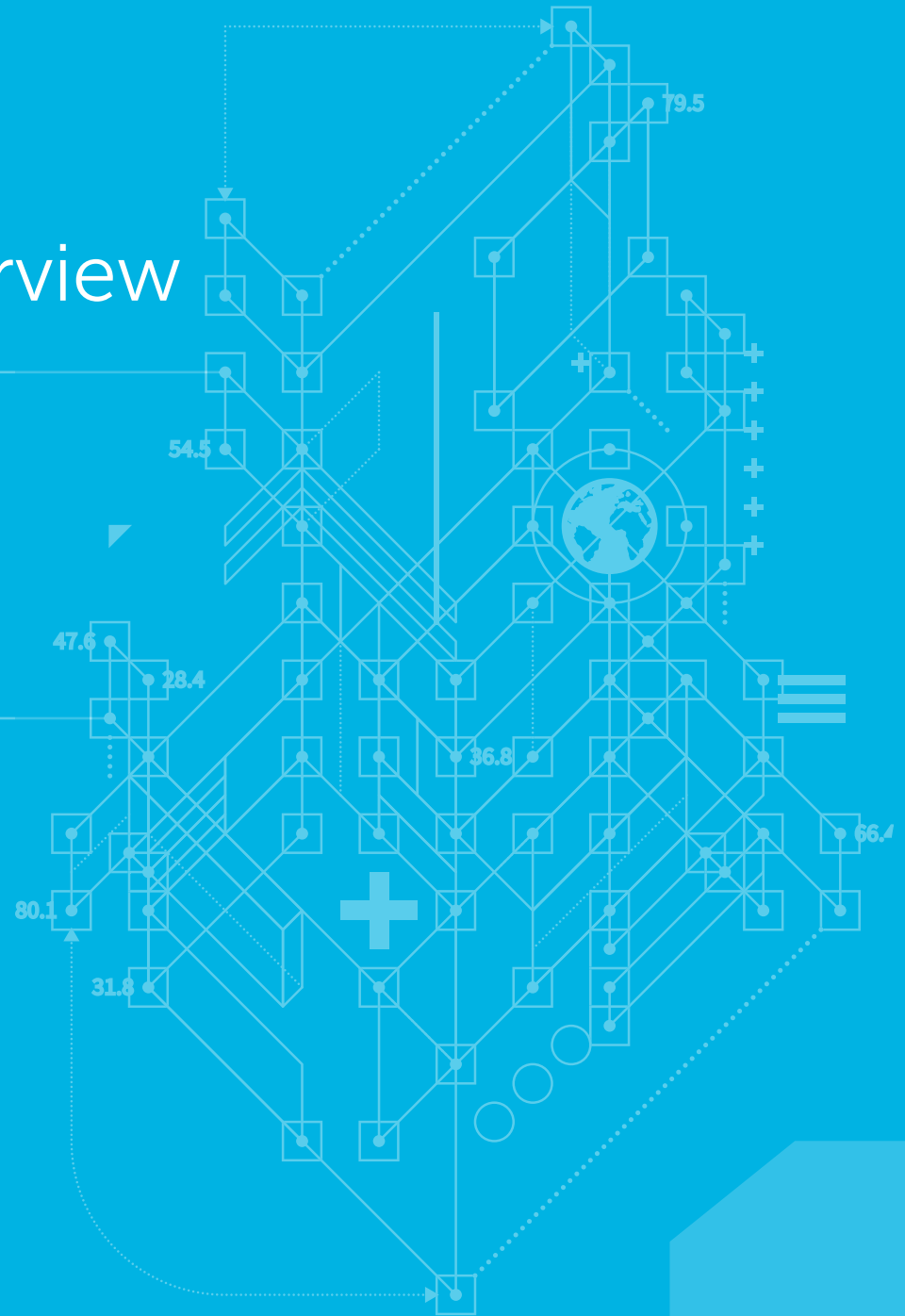




# Technical Security Overview

Matt Jaeh, CTO  
mjaeh@proctoru.com  
(205) 267-6987

2200 Riverchase Center #600,  
Birmingham, AL 35244



ProctorU is an online proctoring platform that enables students and professionals to take exams from their home. Replicated after the physical testing center, ProctorU monitors examinees using remote screen-sharing technology and webcams. We currently offer a robust suite with industry-leading features included automated proctoring with artificial intelligence, live proctoring and identity management services.

This document is meant to provide an overview of ProctorU's security, privacy, processes and controls. Its intention is not to document every single aspect of the business but rather, give I.T. professionals a look in to how we conduct our business and protect user information. These sections are outlined in much more detail in our official Security Policy that is available upon request.

## Quick Facts:



Founded in 2008



Over 5 million  
exams proctored



Users in 125+  
countries



1,000+ partners

| <p>Automated proctoring with artificial intelligence &amp; premium options</p>   | <p>Live+ proctoring with proactive detection and intervention</p>   | <p>Identity management-only platform with continuous authentication</p>  |
|--|---|--|
| <ul style="list-style-type: none"> <li>▶ Fully-automated user experience</li> <li>▶ End-to-end exam recording</li> <li>▶ AI-backed breach detection</li> <li>▶ Industry leading identity authentication</li> <li>▶ Option for live proctor launch &amp; ProctorU recording review</li> </ul> | <ul style="list-style-type: none"> <li>▶ Monitored by our proctors at a ProctorU facility</li> <li>▶ End-to-end exam recording</li> <li>▶ Industry leading identity authentication</li> <li>▶ AI-backed breach detection</li> </ul> | <ul style="list-style-type: none"> <li>▶ KBA Challenge</li> <li>▶ Keystroke biometrics</li> <li>▶ User photo capture</li> <li>▶ ID scan</li> </ul> |

Our Users Include:



# Certification & Compliance



Our infrastructure is built upon Amazon Web Services (AWS) and Google Cloud for all application hosting and data storage. All servers operate in the United States and feature industry-leading digital and physical security. These servers are in full compliance with:

- ▶ ISO 9001, ISO 27001, ISO 27017, ISO 27018
- ▶ SOC 1, SOC 2, SOC 3
- ▶ FERPA
- ▶ GDPR
- ▶ EU-US Privacy Shield
- ▶ EU Protection Directive, EU Model Clauses

**Other tools include but not limited to the following:**

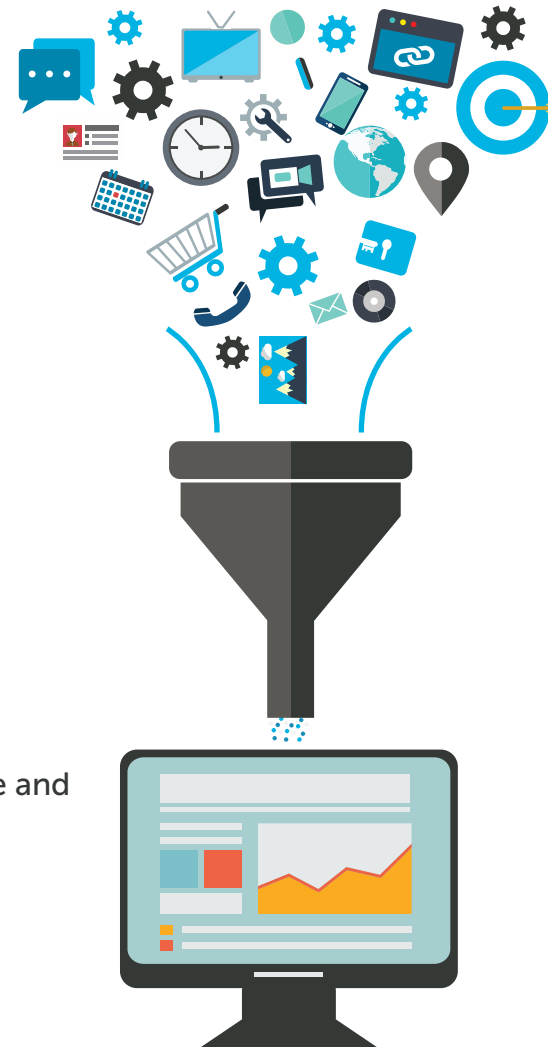
- ▶ Authorize.Net — Payment processing
- ▶ TypingDNA — Keystroke biometric profiling
- ▶ Veratad — Knowledge-Based Authentication (KBA) challenge generation
- ▶ Amazon Key Management — Encryption key management
- ▶ Cloudflare — CDN, DNS, DDoS protection
- ▶ LogMeIn Central Premiere — Internal IT asset management & monitoring
- ▶ LogMeIn Rescue — Remote screen-sharing used in proctoring
- ▶ Zendesk — Customer support resolution management
- ▶ G Suite — Internal communication, email, and file collaboration
- ▶ Ring Central — Internal/external communication & support
- ▶ Intact — Partner invoicing
- ▶ Dropbox — Marketing assets
- ▶ Dropcam — All proctoring facilities under 24/7 monitoring

We are fiercely committed to protecting the data of our users and partners. ProctorU does not claim ownership of your data or that of test-takers. We intentionally limit the amount of Personally Identifiable information (PII) data collected while still offering a valid means to protect exam integrity and ensure users are exactly who they say they are.

## We collect:

- ▶ E-mail address
- ▶ First and last name
- ▶ Username
- ▶ Password
- ▶ Time zone
- ▶ Mobile / home / work phone numbers
- ▶ Address
- ▶ Picture
- ▶ IP address
- ▶ Keystroke pattern
- ▶ Copy of government-issued ID
- ▶ Screen recordings
- ▶ Webcam/voice recordings
- ▶ IDology challenge questions

Our Privacy Policy & Terms of Service are easily accessible and agreement is required before users may use the service.



## Network Protection

Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a ProctorU router or firewall.

**ProctorU utilizes the following solutions to ensure network security:**



Amazon WAF



Cloudflare WAF



Sonicwall IDS/IPS NSA  
devices



OSSEC

## Encryption

Our encryption methods follow industry best practices and all data is collected over TLS 1.2 connections. Proctored sessions are secured with end-to-end AES 256-bit encryption and all data is stored with this same military-grade protection. Passwords are also salted/hashed before being stored with AES 256.

## Other data:

- ▶ Government ID capture — 7 day storage before secure deletion
- ▶ Exam session video recordings — 2 year or mutually agreed upon storage duration before secure deletion
- ▶ Keystroke biometrics — Data is anonymized and sent securely via API to TypingDNA servers. ProctorU only stores the results of the keystroke pattern analysis and TypingDNA can never use data to personally identify users.
- ▶ User payment — We do not allow users to store payment details in our system. All payments are processed by Authorize.Net, a VISA subsidiary, via API.

## Backup Procedures

ProctorU has redundancy for all major technology tools, including local and offsite backups of the ProctorU code base. With respect to data, we make daily back-ups and multi-region read replicas that can be promoted at a moment's notice and backups are encrypted using AES 256 via Amazon Relational Database Service (RDS).

## Access Controls

| Institution Administrator  | Institution Instructor  | Institution Observer   | Student  |
|--|---|--|--|
| These accounts manage institution settings, departments, terms, instructors, iterations, students and other users. | These accounts have the view of institution, students, and can manage and view associated institution exams, and run reports related to an institution. | These accounts have the ability to manage student accounts, view appointments, exams, and reports related to an institution. | These accounts can create accounts and schedule exams. |

### Internal access controls:

- ▶ Internal access controls include passwords, encryption, access control lists, constrained user interfaces, etc.
- ▶ Building access (HID locks w/ logging & quarterly review)
- ▶ Revoking terminated or departing employee
- ▶ All user interactions with system are date/time stamped
- ▶ User accounts audited at least twice yearly



## Learning Tools Interoperability (LTI)

ProctorU seamlessly integrates with the LTI standard and is supported by all major Learning Management Systems (LMS) including Blackboard, Canvas, Moodle, D2L and more.

**We use LTI to pull information about users to populate the ProctorU system including:**



Username/ID



First & last name



Email



User role

Installation takes less than 10 minutes and is completed by an LMS administrator or IT department. After providing you with a secret authorization token that is unique to your institution or organization, users can access all of ProctorU's system and features directly in the LMS.

## Application Programming Interface (API)

We make an API available to any group looking to integrate the ProctorU service in to their test delivery platform or LMS that isn't supported by LTI. The API is RESTful-based and all documentation can be found at <https://postman.proctoru.com/>. Webhooks are also supported and documentation can be found at <https://webhooks.proctoru.com/>.

## Can you provide your Disaster Recovery Plan?

ProctorU has a detailed disaster recovery and business continuity plan. While we cannot contemplate each and every possible force majeure event, this plan allows for redundancy and minimal down time in the event of any catastrophic failure of any of our server environments or physical locations. This plan is tested and updated on an annual basis.

## Do you conduct security awareness training?

All ProctorU employees undergo extensive security training and data privacy protocols at time of hire and before they proctor exams or conduct business functions. This training is ongoing and conducted on a quarterly basis.

## Do you conduct background checks on employees?

All employees undergo employment reference checks, investigative consumer reports and background investigations prior to making a final offer of employment. We used a third-party to verify:

- ▶ SSN validation
- ▶ Address history
- ▶ National Sex Offender Registry check
- ▶ National criminal record search
- ▶ Local court records
- ▶ Driving record/license Validity (if employee is expected to travel)

## What happens in the event of a data breach?

In the event of a data breach, the first step is to verify the accuracy and validity of the situation. In the event that systems were indeed breached, ProctorU will patch the vulnerability as soon as possible. During this process, verifying the extent of the breach and its implications is crucial. If necessary, local or federal law enforcement will be contacted.

Once an assessment of the extent has been completed, institutions and test-takers will be notified of the breach and the appropriate remediation strategies.

## What team members are responsible for overall company security?

- ▶ Matt Jaeh, CTO
- ▶ Mano Vangeepuram, Software Security Engineer

## Was your application developed using secure coding techniques?

All our engineers code with OWASP Top 10 in mind. All code is internally peer-reviewed and extensively tested in a sandboxed environment using non-production data.

**Describe how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)**

Administrator access is requested by an individual and goes through an approval process. The administration privileges are assessed and scoped to the role. In the event a user no longer needs access, it is removed. As a failsafe, all users are evaluated on a quarterly basis to establish the need for their level of access.

**Do you employ a single-tenant or multi-tenant environment?**

Our system is capable of multi-tenant environment, but most users are single-tenant.

**Is redundant power available for all data centers where Institution data will reside?**

Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

**Describe or provide a reference to the availability of cooling and fire suppression systems in all data centers where institution data will reside.**

The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

## **Should the primary environment fail, what is the anticipated downtime before the backup environment is live? What is the anticipated data loss?**

We operate multiple Amazon servers and, in the event that all servers are forced offline, we can seamlessly transition to backup servers provided by the Google Cloud Platform. All data written to the backup will be replicated to the main Amazon servers immediately following server restoration and there is no anticipated data loss.

Since 2008, ProctorU has never experienced a major data loss or disruption.

## **Is there a scheduled maintenance window?**

Maintenance is performed as needed and does not impact user experience.

## **How and when are partners notified of major changes to the environment that could impact security or user experience?**

Any updates or fixes that affect client experience are communicated at least 30 days in advance. API and LTI changes are communicated at least 90 days in advance.

## **Do you enforce password requirements?**

All passwords must be a minimum of 8 characters.

## **Are controls in place to restrict visitor (non-employee or guest) access to the building & network, whether via direct LAN access, wireless or remote access?**

All visitors are escorted by a ProctorU employee. No access to ProctorU's networks is permitted unless in an official capacity by an approved contractor to perform services (i.e., Comcast onsite to fix an issue).

## **Do you have cyber liability insurance & general liability insurance (GL)?**

Yes, policy information is outlined below.

### **Public Liability Insurance**

- ▶ \$1M Occurrence/\$2M Aggregate + \$10M Umbrella limits

### **Employer's Liability Insurance**

- ▶ Statutory requirement of \$1M

### **Product Insurance**

- ▶ Statutory requirement of \$1M

### **Professional Indemnity Insurance**

- ▶ \$3M

### **Cyber and Data Risks Insurance**

- ▶ \$2M cyber policy aggregate, which includes \$2M for network security & privacy liability (sublimits for regulatory claims)
- ▶ \$500K for privacy breach
- ▶ \$500K for data assets breach
- ▶ \$1M for cyber extortion threat