ProctorU is dedicated to securing test-taker data collected during all aspects of our business and to managing test-taker information in compliance with the Family Educational Rights and Privacy Act (FERPA).

### Data Security

#### Personal Information
Test-taker directory information such as name, address, and profile picture is collected over a secure connection and stored for internal use only.

#### Financial Information
Credit card transactions are handled using encryption and online payment industry standards. ProctorU does not see or store credit card information.

#### Exam Records
When examinees set up an account and undertake an examination, ProctorU has created an academic record that is handled with the strictest adherence to FERPA guidelines. All proctors must complete FERPA training.

### Methods

- ProctorU.com is channeled through an HTTPS connection
- SSL encryption is used for all financial transactions
- ProctorU partners with the payment gateway service provider, authorize.net
- Screen-sharing technology used by proctors transmits with full, end-to-end 256-bit SSL encryption, the same encryption method endorsed by MasterCard, Visa and American Express
- ProctorU does not share any test-taker information with outside partners for marketing purposes

### Server Compliance

Our servers meet the following compliance requirements for regulations:

- Payment Card Industry Data Security Standards (PCI/DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Statement for Standards for Attestation Engagements (SSAE) No 16 Type II
- Service Organization Control (SOC) 1

Built upon a hardened, purpose-built operating system for security services, ProctorU’s server firewalls provide the highest level of security and have earned many industry recognitions including ICSA Firewall and IPsec certification and Common Criteria EAL4 evaluation status.

For more information about ProctorU’s security protocols, please direct your questions to Chief Technical Officer, Matt Jaeh at mjaeh@proctoru.com or 855-772-8678, ext. 605
ProctorU does not share any test-taker information with outside partners for marketing purposes.

Service Organization Control (SOC) 1, 2 & 3 Compliant

ProctorU uses Amazon Web Services (AWS) and Rackspace servers for the storage and transmission of test-taker information. Both AWS and Rackspace are dedicated to the highest industry standards and a list of their full certification and compliance reports can be seen on their respective websites.
The screen-sharing technology used by proctors transmits with full, end-to-end 256-bit SSL encryption. This is the same level of protection and encryption method that is used by the financial and healthcare industries. The protocols allow client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering and message forgery.

**Student Privacy Pledge**

ProctorU is a signatory on the Student Privacy Pledge, which is dedicated to protecting a test-taker’s private information. ProctorU remains committed to test-taker privacy by adhering to guidelines as laid out in the Family Educational Rights and Privacy Act (FERPA). FERPA not only protects test-taker data, but also ensures proper training of proctors in the use of data gathered during the proctoring process.

[http://studentprivacypledge.org](http://studentprivacypledge.org)

**TRUSTe Certified for Online Privacy**

ProctorU has been awarded TRUSTe’s Privacy seal signifying that the company’s privacy policy and practices have been reviewed by TRUSTe and are in compliance regarding the collection and use of personal information. Compliance gives ProctorU the ability to effectively manage data as part of the proctoring process, and protect test-takers by preventing the misuse of their information.

[http://www.truste.com](http://www.truste.com)

**U.S. - E.U. Safe Harbor**

ProctorU meets the European Union (EU) “adequacy” standard for privacy protection and has been Safe Harbor-certified. The Safe Harbor framework was established in 1998 to bridge differences in privacy laws between the United States and the EU, enhancing privacy protection for citizens.

[http://export.gov/safeharbor](http://export.gov/safeharbor)
ProctorU partners with the payment gateway service provider, Authorize.net, for all payments of service. Authorize.net serves more than 400,000 merchant customers and provides credit card processing, fraud prevention, subscription billing and payment tokenization. Charges applicable to the examinee must be paid with a credit or debit card. Examinees will be required to enter payment information on a secure page connected to a third-party card processor. The page is encrypted and secure, and ProctorU does not see or store the credit card data. Examinees will be required to re-enter payment information each time new charges are incurred. University-pay or hybrid models are arranged with ProctorU’s billing department, based on the unique needs of the institution.

Financial Security

ProctorU uses a variety of techniques to handle financial information.

ProctorU partners with the payment gateway service provider, Authorize.net, for all payments of service. Authorize.net serves more than 400,000 merchant customers and provides credit card processing, fraud prevention, subscription billing and payment tokenization. Charges applicable to the examinee must be paid with a credit or debit card. Examinees will be required to enter payment information on a secure page connected to a third-party card processor. The page is encrypted and secure, and ProctorU does not see or store the credit card data. Examinees will be required to re-enter payment information each time new charges are incurred. University-pay or hybrid models are arranged with ProctorU’s billing department, based on the unique needs of the institution.

ProctorU is in compliance with this federal law that set new and enhanced standards for all U.S. public company boards, management and public accounting firms. Extended documentation can be found at soxlaw.com

ProctorU is fully compliant with Payment Card Industry Data Security Standards (PCI/DSS) to ensure payment card data security. The standards provide a robust framework that establishes a standard payment card security process that includes prevention, detection and appropriate reaction to security incidents.

ProctorU provides consumers with privacy notices and documentation that outlines the company use and information-sharing practices regarding customer information. A copy of ProctorU’s privacy policy is available at www.proctoru.com/privacy.txt

ProctorU is TRUSTe certified, a leading global Data Privacy Management platform to ensure businesses adhere to best practices regarding the collection and use of personal information. This certification seal has also been awarded to Apple, Disney, eBay, Forbes, LinkedIn and Oracle.
Secure Browser
ProctorU’s secure browser requires no installation and enhances the security of testing environments by:
• Disabling virtual machines and secondary computer monitors.
• Removing test-taker ability to copy, paste, print or save exam materials.
• Disabling test-taker ability to navigate away from the exam page and open new browser tabs or windows.

Live Proctors
ProctorU’s philosophy is to prevent cheating rather than just simply catching it. By utilizing live proctors, as opposed to automated recording methods, ProctorU prevents incidents of academic integrity through real time interaction with test-takers and has the ability to stop integrity breaches as they occur.

Incident Prevention
Because ProctorU relies on live proctors monitoring the examination process in real time, academic integrity breaches can be avoided. In the event of an institution-specified irregularities, proctors are there to document and prevent test-taker conduct as it happens, rather than after the fact, as with automated recording methods.

Incident Documentation
Proctors are linked to test-takers in real time, with live audio and video connections, as well as with an established chat box. Live feeds of computer desktop activity are viewed using ProctorU’s screen-sharing technology. ProctorU uses multiple layers of recording and reporting, including full-session video and audio; screen-capturing; spot recording, if needed; and documentation through user chat logs.
ProctorU uses a multi-factored authentication system to verify the identity of test-takers. Using a variety of techniques, the identity of the test-takers that enter the ProctorU system is insured to be accurate.

**Photo ID**
Examining photo identification is the first layer in confirming that the test-taker entering a proctoring session is indeed who they say they are. Proctors check a government-issued photo identification or institution identification card.

**Keystroke**
Keystroke analysis adds another layer of security for identity verification. By examining the unique typing patterns inherent to individuals, identity can be further ensured. Raw timing measurement data is used to create an examinee “typing signature” that is unique to them.

**Challenge Questions**
A third layer of verifying the identity of a test-taker is having them answer a bank of challenge questions based on data from public records related to them. Since this information is proprietary to each test-taker, a high degree of identity verification is ensured.

Questions are generated via a Public records-based quiz using personally-identifiable information against a test bank of over 120 randomly generated questions from Acxiom, a third party provider.
Compliance and Certification

Protection and Privacy of Data in Europe
As part of standards for privacy protection, ProctorU complies with U.S. - Europe and U.S. - Swiss Safe Harbor Frameworks when providing services to all nations. Following these directives allows ProctorU to safely and efficiently exchange data for international test-takers.

http://export.gov/safeharbor

TRUSTe Certified for Online Privacy
ProctorU has been awarded TRUSTe’s privacy seal signifying that the company’s privacy policy and practices have been reviewed by TRUSTe and are in compliance regarding the collection and use of personal information. This gives ProctorU the ability to effectively manage data as a part of the proctoring process, and protect test-takers by preventing misuse of their information.

http://www.truste.com

Student Privacy Pledge
ProctorU is a signatory on the Student Privacy Pledge, which is dedicated to protecting test-taker’s private information.

ProctorU remains committed to test-taker privacy by adhering to guidelines as laid out in the the Family Educational Rights and Privacy Act (FERPA). FERPA not only protects test-taker data, but also ensures proper training of proctors in the use of data gathered during the proctoring process.

http://studentprivacypledge.org

Federal Information Security Management Act FISMA
Built upon a hardened, purpose-built operating system for security services, ProctorU’s server firewalls provide the highest level of security and have earned many industry recognitions including ICSA Firewall and IPsec certification and Common Criteria EAL4 evaluation status.

http://csrc.nist.gov/groups/SMA/fisma/
ProctorU invites your team to tour one of our facilities in Gilbert, Ariz., Folsom, Calif., Livermore, Calif., or Hoover, Ala.

Contact Us
To learn more about ProctorU, please visit our website at

www.ProctorU.com
or call 888-355-8043.

Don’t forget to “like” us on Facebook and follow us on Twitter!

www.facebook.com/ProctorU
http://twitter.com/ProctorU