

Data Security You Can Trust

At Proctorio, keeping test taker data secure is our top priority. This is why our security has gone through years of testing and is tailored to protect test takers and their exam data.



Three Layers are Better Than One

All test taker data is secured and processed through three layers of encryption:

01

The zero-knowledge layer is secured using AES-GCM, using encryption keys never shared with Proctorio.

02

Transmission into the datacenter is only over TLS 1.2 or 1.3 and, if the client supports it, we use Perfect Forward Secrecy (PFS).

03

Data at rest within the data center is encrypted using AES-256 and is FIPS 140-2 compliant. All data centers are ISO 27001 certified, SOC 2 attested.



Zero-knowledge Encryption

Proctorio utilizes Zero-Knowledge Encryption, which means Proctorio does not have access to the encryption keys to decrypt your exam-session recording data. This unique design ensures that nothing leaves the test taker's computer until it has been encrypted, and data is only decrypted when unlocked by an institution-approved individual. **It's not just end-to-end encryption, it's a zero-knowledge system.**

Please see our third party security audit that verifies our use of these technologies at <https://proctorio.docsend.com/view/mj83bzs62vqrtuky>



Daily Vulnerability Tests

Our platform goes through daily vulnerability and penetration tests to assess the strength of our systems against a potential attack. Partnered institutions can see these daily vulnerability scans under an NDA. These strategies create a security system you can trust.