Higher Education Community Vendor Assessment Tool (HECVAT) - Lite			Version 2.11
HEISC Shared Assessments Working Group			
DATE-01	**Date**	*13/02/2020*	
General Information			
In order to protect the institution and its systems, vendors whose products and/or services will access and/or host institutional data must complete the Higher Education Community Vendor Assessment Toolkit. Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least data and metadata. Answers will be reviewed by institution security analysts upon submittal. This process will assist the institution in preventing breaches of protected information and comply with institution policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security Assessment and should be completed by a vendor.			
GNRL-01 through GNRL-15; populated by Vendor			
GNRL-01	Vendor Name	*Proctorio, Inc.*	
GNRL-02	Product Name	*Proctorio*	
GNRL-03	Product Description	*Proctorio is a learning integrity platform focused on validating student IDs, activity, and originality in any clasroom environmnt.*	
GNRL-04	Web Link to Product Privacy Notice	*https://proctorio.com/*	
GNRL-05	Vendor Contact Name	*Connor Koper*	
GNRL-06	Vendor Contact Title	*Head of Sales - North America*	
GNRL-07	Vendor Contact Email	*connor@proctorio.com*	
GNRL-08	Vendor Contact Phone Number	*480-428-2879*	
GNRL-09	Vendor Data Zone	*United States*	
GNRL-10	Institution Data Zone	*United States*	
GNRL-11 and GNRL-12; populated by Institution's Security Office			
GNRL-11	Campus Security Analyst/Engineer	*Institution's Security Analyst/Engineer Name*	
GNRL-12	Assessment Contact	*ticket#@yourdomain.edu*	
Instructions			
Step 1: Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. Step 2: Submit the completed Higher Education Community Vendor Assessment Toolkit - Lite to the institution according to institutional procedures.			

Documentation		Vendor Answers	Additional Information	Guidance
DOCU-01	Have you undergone a SSAE 18 audit?	Yes	Proctorio maintains SOC reports, they are not accessible via a url but upon request.	Provide the date of assessment and include a SOC 2 Type 2 (preferred) or SOC 3 report. If you have a SOC3 report, include a URL for the published report. Indicate if your hosting provider was the subject of the audit.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	Yes	Proctorio has completed the CSA Self Assessment.	Please include a copy with your response and include a URL for the published assessment.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	Proctorio has not received the Cloud Security Alliance STAR certification, but will be seeking it in the future.	Describe any plans to obtain CSA STAR certification.
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)	Yes	Proctorio conforms with industry-standard security frameworks along with internal proprietary measures to protect data security.	Provide documentation on how your organization conforms to each framework and indicate current certification levels, where appropriate.

DOCU-05	Are you compliant with FISMA standards?	Yes	Proctorio is FISMA compliant at Level 115 (low impact).	Indicate level, agency issuing ATO, and necessary details on ATO. If using FEDRamp, please indicate the supporting details.
DOCU-06	Does your organization have a data privacy policy?	Yes	Proctorio Data Privacy Policies can be viewed here: https://proctorio.com/privacy	Provide your data privacy document (or a valid link to it) upon submission.
Company Overview		**Vendor Answers**	**Additional Information**	**Guidance**
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	Proctorio is based in Scottsdale, Arizona, and provides proctoring, identity verification, content security, and learning integrity products through cloud services that integrate with a learning management system. Proctorio is a privately held Delaware corporation with offices in the United States and Europe.		Include circumstances that may involve off-shoring or multi-national agreements.
COMP-02	Describe how long your organization has conducted business in this product area.	Proctorio was created in 2013 to provide a convenient, scalable, and objective service to secure exams. Since then, Proctorio grown rapidly in size to become an industry leader with a full learning integrity platform to guard education for the 21st century.		Include the number of years and in what capacity.
COMP-03	Do you have existing higher education customers?	Yes	Proctorio has worked with hundreds of education, commercial, and government customers in the USA and internationally. A complete reference list is available upon request. In Texas, Proctorio currently works with University of Texas at Austin, University of Texas at San Antonio, University of Texas at Houston, Texas Tech University, Baylor University, Lamar University, and theTarrant County Community College District.	Provide a list of Higher Ed references, with contact information.
COMP-04	Have you had a significant breach in the last 5 years?	No	Proctorio has not ever had a significant breach.	
COMP-05	Do you have a dedicated Information Security staff or office?	Yes	Proctorio has a dedicated software, environment, and deployment security team that ensures that the company's current and forthcoming products and features meet or exceed industry security standards.	Decribe your Information Security Office, including size, talents, resources, etc.
COMP-06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Yes	Proctorio employs individualized teams of developers consisting of engineers that work on front-facing UI, server maintenance, production support for specific LMS instances, and new feature development.	Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	Extensive site controls are used to limit access that include, badge scanning, biometrics, CCTV cameras, and an on-premise bank vault that remains locked and is only accessible to authorized personnel. Proctorio's development environment consists of isolated code bases in order to ensure that engineering teams only have access to necessary aspects of Proctorio. Proctorio has received third-party recognition of its data security and student privacy standards from iKeepSafe. Proctorio uses zero-knowledge, double-encryption techniques to ensure that all data is secure in both		Share any details that would help information security analysts assess your product.
Application/Service Security		**Vendor Answers**	**Additional Information**	**Guidance**
HLAP-01	Do you support role-based access control (RBAC) for end-users?	Yes	Proctorio leverages a user's role in the constituent learning management system to determine access level, and provide records when a request is received.	Describe any infrastructure dependencies.
HLAP-02	Do you support role-based access control (RBAC) for system administrators?	Yes	Proctorio functionality respects the LMS roles. Access to Proctorio's administrative dashboard containing master controls and data analytics is restricted to individuals specifically authorized by partner institutions.	Describe the utilized technology.
HLAP-03	Can employees access customer data remotely?	No	Proctorio employees are not able to access customer data due to Proctorio's zero knowledge encryption scheme. Employees are not allowed to work remotely or connect personal devices in order to maintain security standards	Provide details that prevent this capability.

HLAP-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?	Yes	Proctorio can provide high level architecture documents. However, given that Proctorio operates as an integration into the LMS, the user interface with Proctorio architecture is limited to the point of connection. Proctorio's network architecture used geo steering to direct the load to the closest physical region	Provide a reference to the requested documents or provide them when submitting this fully-populated HECVAT.
HLAP-05	Does the system provide data input validation and error messages?	Yes	Coded messages are internal only. Text error messages are displayed to users if the user is experiencing a hardware or connection error. Users are then connected to Proctorio customer support and/or the Proctorio Help Center to troubleshoot the issue.	Provide a reference to documentation of your data input validation and error messaging capabilities.
HLAP-06	Do you employ a single-tenant environment?	Yes	Proctorio offers a multi-tenant environment by default but single tenant systems can be created at additional cost. Single tenant environments are dedicated application servers, databases and private virtual networks.	Describe your single-tenant strategy.
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**
HLAA-01	Can you enforce password/passphrase aging requirements?	Yes	Proctorio does not collect or store user passwords. Proctorio operates through single sign on into a partner institution's learning management system (LMS). Our partners are free to impose any password security requirements they deem necessary within the LMS.	Describe how aging requirements are implemented in the product.
HLAA-02	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)	Yes	Proctorio supports single sign on via a partner institution's learning management system.	Describe or provide a reference to the supported types of authentication.
HLAA-03	Does your *application* support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?	Yes	Proctorio supports single sign on via a partner institution's learning management system.	Provide a brief description of supported authentication and authorization systems.
HLAA-04	Does the *system* (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	Yes	These integrations are not required as Proctorio supports single sign on via partner institutions learning management system.	Describe all authentication services supported by the system.
HLAA-05	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes	Exam and security settings create and update actions are available in audit logs.	Ensure that all elements of HLAA-05 are evaluated for your response. Provide a description of logging capabilities.
Business Continuity Plan		**Vendor Answers**	**Additional Information**	**Guidance**
HLBC-01	Do you have a documented Business Continuity Plan (BCP)?	Yes	Proctorio has a business continuity plan that can be shared upon request.	Provide a copy of your BCP along with this document (link or attached).
HLBC-02	Is there a documented communication plan in your BCP for impacted clients?	Yes	Proctorio's business continuity plan consists of multiple server and database redundancies in strategically placed locations via Microsoft Azure. Should one region fail or become inoperable, all data and product service remains available for clients. Proctorio also has operations in both North America and Europe for redundancy and around the clock support.	Summarize your documented communication plan contained in your BCP.
HLBC-03	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes	All components of the BCP are tested to ensure consistency with Proctorio's security design principles.	Describe your BCP component review strategy.
HLBC-04	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Yes	Proctorio performs monthly vulnerability scans in accordance with company security requirements using both internal and external resources. Proctorio employs daily penetration testing to ensure complete security. Results available upon request.	State the date of your last alternate site relocation test.
Change Management		**Vendor Answers**	**Additional Information**	**Guidance**
HLCH-01	Do you have a documented and currently followed change management process (CMP)?	Yes	Proctorio has a change management plan and it is available upon request. Proctorio also has several control checkpoints used regularly including code reviews, code silos, development testing and approvals, and post implementation verification, among others.	Summarize your current change management process.

HLCH-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Yes	The institution will be notified of major changes to our environment proactively, as well as, within our public change log at changes.proctorio.com	State how and when the institution will be notified of major changes to your environment.
HLCH-03	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	Proctorio has an extensive detection, communication, and remedy processes implemented to guide how security risks are mitigated until patches can be applied.	Summarize the policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.
HLCH-04	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	Yes	Should an emergency change be required in production to optimize functionality, that change may be implemented outside of the standard review and approval process. Afterward, change reason and approvals are retroactively documented. Available upon request.	Summarize implemented procedures ensuring that emergency changes are documented and authorized.
Data		**Vendor Answers**	**Additional Information**	**Guidance**
HLDA-01	Do you physically and logically separate institution's data from that of other customers?	Yes	Institutional data is logically separated using unique customer identifiers.	Describe or provide a reference to how institution data is physically and logically separated from that of other customers.
HLDA-02	Is sensitive data encrypted in transport? (e.g. system-to-client)	Yes	Proctorio employs zero-knowledge, double-encryption technology in transport	Summarize your transport encryption strategy.
HLDA-03	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	Yes	Proctorio employs zero-knowledge, double-encryption technology in transport and storage at-rest.	Summarize your data encryption strategy.
HLDA-04	Do backups containing institution data ever leave the institution's Data Zone, either physically or via network routing?	No	Proctorio will never back up an institution's data to a cloud database hosted outside of the host country's region or nation. Proctorio understands how critical data security, governance, and legal compliance are for partner institutions, and will continue to offer	
HLDA-05	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?	Yes	Proctorio sanitizes all data by destroying decommissioned or failed data records in the production environment. Proctorio delivers or destroys all data at the end of contract at the institution's request (when available).	Provide details of these procedures (link or attached).
HLDA-06	Is any institution data visible in system administration modules/tools?	Yes	Institutional data is not visible to any member of Proctorio. This data is only visible to authorized users within the institution.	Summarize why the institution's data is visible in system adminitration modules/tools.
Database		**Vendor Answers**	**Additional Information**	**Guidance**
HLDB-01	Does the database support encryption of specified data elements in storage?	Yes	All data elements recorded during an exam session are first encrypted, then encrypted a second time in transfer, and finally a third time in storage (at-rest).	Describe the type of encryption that is supported.
HLDB-02	Do you currently use encryption in your database(s)?	Yes	All data stored in Proctorio's database is encrypted both in transfer and then again in storage as a custom binary element for additional security.	Describe how encryption is leveraged in your database(s).
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**
HLDC-01	Will any institution data leave the institution's Data Zone?	No	Proctorio's client data centers are owned and maintained by Microsoft with full redundancies in California, Texas, Illinois, and Virginia.	
HLDC-02	Does your company own the physical data center where the institution's data will reside?	No	No	Provide a detailed description of where the institution's data will reside.
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	The SOC 2 Type 2 report may be provided upon request.	Obtain the report if possible and add it to your submission.
HLDC-04	Does the physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	Yes	Because Proctorio customer data resides exclusively at data centers controlled by Microsoft Azure, Proctorio customers enjoy the security measures provided by Microsoft including, but no limited to, security cameras, badge-limited access, and physical intrusion detection	Describe your physical barrier strategy.
Disaster Recovery Plan		**Vendor Answers**	**Additional Information**	**Guidance**

HLDR-01	Do you have a Disaster Recovery Plan (DRP)?	Yes	Proctorio was built with planned Business Continuity and Disaster Recovery Plans that include procedures and contact information in the event of a widespread incident or disaster.	Describe or provide a reference to your Disaster Recovery Plan (DRP).
HLDR-02	Are any disaster recovery locations outside the institution's Data Zone?	No	For data and governance compliance purposes, no disaster recovery locations are outside the Institution's Data Zone. Note: foreign disaster recovery locations do exist as redundancies but only for the country or region in which the foreign data center is hosted.	
HLDR-03	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes	Disaster Recovery Plans has been tested and reviewed semi-annually and updated as needed	Summarize your DRP review and update processes and/or procedures.
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**	**Guidance**
HLFI-01	Are you utilizing a web application firewall (WAF) and/or a stateful packet inspection (SPI) firewall?	Yes	Proctorio uses a web application firewall in blocking mode	Describe the currently implemented WAF.
HLFI-02	Do you have a documented policy for firewall change requests?	Yes	Proctorio leverages traditional Access Control Lists for firewall change requests.	Describe your documented firewall change request policy.
HLFI-03	Are you employing any next-generation persistent threat (NGPT) monitoring?	Yes	Proctorio monitors for intrusions constantly, employing NGPT monitoring.	Describe your NGPT monitoring strategy.
HLFI-04	Do you monitor for intrusions on a 24x7x365 basis?	Yes	Proctorio monitors for intrusions constantly, while logs and created and preserved for investigation and review of intrusion attempts.	Provide a brief summary of this activity.
Physical Security		**Vendor Answers**	**Additional Information**	**Guidance**
HLPH-01	Does your organization have physical security controls and policies in place?	Yes	Proctorio's physical premises include a layered badging system, alarms, CCTV cameras, biometrics, and an on-premise bank vault. As a security precaution, no customer data is stored at on-premise servers - all critical customer data is maintained in cloud servers exclusively with Microsoft Azure.	Provide a copy of your physical security controls and policies along with this document (link or attached).
HLPH-02	Are employees allowed to take home customer data in any form?	No	Proctorio's zero knowledge encryption scheme. Employees are not allowed to work remotely or connect personal devices in order to maintain security standards.	
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**	**Guidance**
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Yes	Proctorio's org chart is an internal document that can be shared upon request, and our mission statement can be found on Proctorio's website. Proctorio is the industry leader in data security and privacy protection. Our software is designed for maximum data privacy and security; no personally	Provide a links to these documents in Additional Information or attach them with your submission.
HLPP-02	Are information security principles designed into the product lifecycle?	Yes	Proctorio has built in controls to ensure external application and infrastructure security as well as internal controls during the development process including, but not limited to, code reviews, automated and manual QA testing, and post implementation	Summarize the information security principles designed into the product lifecycle.
HLPP-03	Do you have a formal incident response plan?	Yes	Proctorio has a formal incident response plan in which institutes can communicate formal incidents.	Summarize your formal incident response plan.
HLPP-04	Do you have a documented information security policy?	Yes	Proctorio's information security policies are regularly reviewed and updated as needed, and are available for viewing on the company's website.	Provide a reference to your information security policy or submit documentation with this fully-populated HECVAT-Lite.
Systems Management & Configuration		**Vendor Answers**	**Additional Information**	**Guidance**
HLSY-01	Are systems that support this service managed via a separate management network?	No	Systems that support this service are not managed via a separate management network.	Describe your strategy to maintain system integrity (e.g. compensating controls).
HLSY-02	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?	Yes	Proctorio has developed the Change Development and Management Policy that addresses purpose, scope, and the change management policy in regards to the following areas: Securing System Files, Making changes to the Production Environment, Monitoring and Implementing Patches, Unauthorized Changes, Approval of Changes, Separation of Environments, System of	Summarize your systems management and configuration strategy.

Vulnerability Scanning		Vendor Answers	Additional Information	Guidance
HLVU-01	Have your systems and applications had a third party security assessment completed in the last year?	Yes	Proctorio performs monthly vulnerability scans in accordance with company security requirements using both internal and external resources. Proctorio employs daily penetration testing to ensure complete security. Results available upon request.	Provide the results with this document (link or attached), if possible. State the date of the last completed third party security assessment.
HLVU-02	Are your systems and applications scanned for vulnerabilities [that are remediated] prior to new releases?	Yes	Proctorio leverages human and technical resources to test for vulnerabilities as a part of every release. Additionally, Proctorio ensures that all release aspects, whether patches or new features, are architected in a manner consistent with our company's security	Provide a brief description.