HECVAT - Lite | Vendor Response

Vendor Response

DATE-01	**Date**

General Information

In order to protect the institution and its systems, vendors whose products and/or servi
tool, anywhere where the term data is used, this is an all-encompassing term including
in preventing breaches of protected information and comply with institution policy, state
vendor.

GNRL-01	Vendor Name
GNRL-02	Product Name
GNRL-03	Product Description
GNRL-04	Web Link to Product Privacy Notice
GNRL-05	Web Link to Accessibility Statement or VPAT
GNRL-06	Vendor Contact Name
GNRL-07	Vendor Contact Title
GNRL-08	Vendor Contact Email
GNRL-09	Vendor Contact Phone Number
GNRL-10	Vendor Accessibility Contact Name

GNRL-11	Vendor Accessibility Contact Title
GNRL-12	Vendor Accessibility Contact Email
GNRL-13	Vendor Accessibility Contact Phone Number
GNRL-14	Vendor Hosting Regions
GNRL-15	Vendor Work Locations

Vendor Instructions

Step 1: Complete each section answering each set of questions in order from top to bot
Toolkit - Lite to the requesting institution.

Company Overview

COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?

COMP-03	Do you have a dedicated Information Security staff or office?
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)
COMP-05	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?
COMP-06	Will data regulated by PCI DSS reside in the vended product?
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.
Documentation	
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?

DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?
DOCU-03	Have you received the Cloud Security Alliance STAR certification?
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?
DOCU-07	Does your organization have a data privacy policy?

DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?
DOCU-09	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?
DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?
DOCU-11	Do you have a documented change management process?
DOCU-12	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?
DOCU-13	Do you have documentation to support the accessibility features of your product?

IT Accessibility	
ITAC-01	Has a third party expert conducted an accessibility audit of the most recent version of your product?
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?
ITAC-03	Have you adopted a technical or legal accessibility standard of conformance for the product in question?
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?

ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?
ITAC-08	Can all functions of the application or service be performed using only the keyboard?
ITAC-09	Does your product rely on activating a special ‘accessibility mode,’ a ‘lite version’ or accessing an alternate interface for accessibility purposes?
Application/Service Security	
HLAP-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?

HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?
HLAP-03	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)
HLAP-04	Does the system provide data input validation and error messages?
HLAP-05	Are you using a web application firewall (WAF)?
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)

Authentication, Authorization, and Accounting

HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?
HLAA-02	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?
HLAA-03	Does your application support integration with other authentication and authorization systems?
HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]
HLAA-05	Do you support differentiation between email address and user identifier?
HLAA-06	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]

HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following; login, logout, actions performed, timestamp, and source IP address?
HLAA-08	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?
Systems Management	
HLSY-01	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?

HLSY-04	Have your systems and applications had a third party security assessment completed in the last year?
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?
Data	
HLDA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)
HLDA-04	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?

HLDA-05	Can the Institution extract a full or partial backup of data?
HLDA-06	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?
HLDA-07	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) within the application/system?
Datacenter	
HLDC-01	Does your company manage the physical data center where the institution's data will reside?
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?
HLDC-04	Does your organization have physical security controls and policies in place?

HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?
Networking	
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?
HLNT-05	Do you require connectivity to the Institution's network for support/administration or access into any existing systems for integration purposes?
Incident Handling	
HLIH-01	Do you have a formal incident response plan?

HLIH-02	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
HLIH-04	Do you have either an internal incident response team or retain an external team?
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?
Policies, Procedures, and Processes	
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?
HLPP-02	Are information security principles designed into the product lifecycle?
HLPP-03	Do you have a documented information security policy?

Third Party Assessment	
HLTP-01	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)
HLTP-02	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).
HLTP-03	Do you have an implemented third party management strategy?
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)

11/13/23

ces will access and/or host institutional data must complete the Higher Education Community Vend
at least data and metadata. Answers will be reviewed by institution security analysts upon submitt
, and federal law. This is intended for use by vendors participating in a Third Party Security Assess

LearningClues
CourseGPT™
A unique combination of search capabilities and generative AI that allows for the creation of a course-speci *student questions are based only those materials presented or shared in a course with citations linking eac*
https://learningclues.com/privacy-policy/
https://learningclues.com/accessibility/
Perry Samson
Co-Founder
samson@learningclues.com
734-276-0815
Perry Samson

co-Founder
samson@learningclues.com
734-276-0815
United States
United States

tom; the built-in formatting logic relies on this order. **Step 2**: Submit the completed Higher Educa

Vendor Answers	Additional Information
LearningClues is an LLC registered in the States of Michigan and Washington. Its current capitalization is through the NSF SBIR Phase I grant and supplemented by the Michigan Emerging Technology Fund. The LearningClues technology was licensed exclusively to LearningClues via the UM Technology Transfer Office on September 29, 2023.	
No	

Yes	As a startup, the entire staff is responsible.
Yes	Staff of three full-time employees in development and two part-time. As a startup, the entire staff is responsible for customer support.
No	
No	

AWS Cloud services for backend services and Azure OpenAI (or equivalent) as a Large Langauge Model. Video and associated captions are obtained from vendors via their APIs.

Vendor Answers	Additional Information
No	Not considered in Pilot stage. Will address in the future.

No	Not considered in Pilot stage. Will address in the future.
No	Not considered in Pilot stage. Will address in the future.
No	Not considered in Pilot stage. Will address CIS controls in the future.
No	Not considered in Pilot stage. Will address in the future.
No	Work in progress
Yes	https://learningclues.com/privacy-policy/

Yes	We review account access periodically and when new employees are on-boarded. Access is revoked upon termination.
No	As a startup the company's business continuity plan (BCP) is in early stages.
No	As a startup the company's disaster recovery plan (DRP) is in early stages.
No	Under development
No	Under development during pilot study period.
No	Under development

Vendor Answers	Additional Information
No	Initially, audit will be conducted internally . External audit will be completed when technology is in final state.
No	Under development
No	WCAG 2.2 AA, is the level we will be targeting. Work in progress.
No	Once application is in deployable state we will proceed with definition of roadmap.
Yes	Once application is in deployable state we will proceed with design of accessibility trainings. We expect our staff to have accessibility best practices in mind.

Yes	In our task tracker we have a tag for accessibility issues.
No	Under development
No	Under development
No	
Vendor Answers	**Additional Information**
Yes	Separate roles for student, instructors, course admins and institution admins.

Yes	
Yes	All data and systems are protected by a Virtual Private Network, bound by limited office IP addresses, require use of username and valid SSH certificate. Any access to network console is additionally bound by rotating Google Authenticator provider tool in best practice with AWS.
Yes	All API requests are validated against specific and accepts schema types. Additionally, all of our errors are documented.
No	We utilize AWS which provides some built-in protection.
Yes	We utilize standard tools (pip, rpm, dependabot) to keep our software stack up to date and manage dependencies
Vendor Answers	**Additional Information**

Yes	We use Google authentication and LTI1.3 authentication.
No	Planned for the future
Yes	We use Google authentication and LTI1.3 authentication.
Yes	OIDC for LTI 1.3
Yes	
Yes	

Yes	
Yes	We log out users with unattended sessions after three hours.

Vendor Answers	Additional Information
No	Unclear what this means
Yes	Email to system administrator from the institution.
Yes	We use dependabot for dependency vulerabilities. AWS handles protection of the cloud.

No	Will plan
No	We will develop
Vendor Answers	**Additional Information**
Yes	Separate AWS accounts and infrastructures per tenet.
Yes	We use https for comminication between client and applications.
Yes	We use S3 and RDS encryption.
Yes	We use S3 and RDS backups.

Yes	Contact LearningClues support for full or partial backup.
No	We do not make any hard copies of the data.
No	

Vendor Answers	Additional Information
No	AWS RDS and AWS S3
Yes	
Yes	Available from https://aws.amazon.com/artifact/getting-started/
No	We have no physical location

Yes	AWS manages the data center
Vendor Answers	**Additional Information**
Yes	We utilize AWS VPC to separate out network access based on internal versus external communication.
No	Once application is in deployable state we plan to implement SPI firewall.
No	Once application is in deployable state we plan to implementIDS/IPS system.
No	Once application is in deployable state we plan to implement NGPT system.
No	
Vendor Answers	**Additional Information**
No	Early stages. Detection procedures under development. AWS logging allows us to respond to security incidents.

No	Early stages. Detection procedures under development. AWS logging allows us to respond to security incidents.
Yes	$1,000,000 aggregate limit; $1,000,000 Notification Costs; $1,000,000 Business Interuption; $1,000,000 Data Recovery; $1,000,000 Network Security
Yes	Early stage, all employees responsible.
No	We have plans to set up monitoring and paging but not available initially.
Vendor Answers	**Additional Information**
Yes	Under development
Yes	In the process of designing code review processes. Currently implementing Dependabot on GitHub repos. We an individual responsible for reviewing pull requests from GitHub.
No	Documents are under review.

	Additional Information
No	

Version 3.04
dor Assessment Toolkit. Throughout this al. This process will assist the institution sment and should be completed by a
ific virtual teaching assistant. Responses to *h part of the response to the course*

ıtion Community Vendor Assessment	
Guidance	**Analyst Notes**
N/A	
N/A	

Describe your Information Security Office, including size, talents, resources, etc.	
Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)	
N/A	
Guidance	**Analyst Notes**
Describe any plans to undergo a SSAE 18 audit.	

Describe any plans to complete the CSA CAIQ.	
Describe any plans to obtain CSA STAR certification.	
Describe any plans to conform to an industry standard security framework.	
Describe any plans to provide NIST SP 800-171 or CMMC Level 3 services.	
Provide a detailed summary of overall system and/or application architecture.	
Provide your data privacy document (or a valid link to it) upon submission.	

Provide a reference to your employee onboarding and offboarding policy and supporting documentation or submit it along with this fully-populated HECVAT.	
Briefly summarize your response.	
Briefly summarize your response.	
Briefly summarize your response.	
Please state your plans (when and by whom) to complete a VPAT.	
Provide plans for any documentation that would make accessible content, features and functions easily knowable by end users.	

Guidance	Analyst Notes
Please provide plans (when and by whom) any audit is planned, if any or rationale if not.	
Summarize how you ensure accessible products. Provide plans to develop documented processes to validate accessibility.	
Summarize your decision to not adopt a technical or legal standard of conformance for the product in question.	
Please provide any plans to develop and share an accessibility product roadmap in the future.	
Provide any further relevant information about how expertise is maintained; include any accessibility certifications staff may hold (e.g., IAAP WAS <https://www.accessibilityassociation.org/certifications> or DHS Trusted Tester <https://section508.gov/test/trusted-tester>.	

Describe the process and any recent examples of fixes as a result of the process.	
Describe any plans to update processes and procedures to better incorporate accessibility.	
Indicate a plan to test the product, develop a roadmap for keyboard accessibility or any further context.	
Guidance	**Analyst Notes**
Describe available roles.	

Provide supporting documentation of your strategy.	
Describe how your system(s) provide data input validation and error messages.	
Describe compensating controls that protect your web application, if applicable.	
Provide supporting documentation of your processes.	
Guidance	**Analyst Notes**

Describe how strong authentication is enforced (e.g., complex passwords, multifactor tokens, certificates, biometrics, aging requirements, re-use policy).	
Describe plans to participate in InCommon or another eduGAIN affiliated trust federation.	
List which systems and versions supported (such as Active Directory, Kerberos, or other LDAP compatible directory) in Additional Info.	
State the Web SSO standards supported by your solution and provide additional details about your support, including framework(s) in use, how information is exchanged securely, etc.	

Describe the default behavior of this capability.	
Guidance	**Analyst Notes**
Describe your intent to implement a systems management and configuration strategy.	
State how and when the institution will be notified of major changes to your environment.	
Provide a brief description.	

State plans to have your systems and applications assessed by a third party.	
State your plans to implement policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.	
Guidance	**Analyst Notes**
Describe or provide a reference to how institution data is separated from that of other customers.	
Summarize your transport encryption strategy	
Summarize your data encryption strategy and state what encryption options are available.	
If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.	

Provide a general summary of how full and partial backups of data can be extracted.	
Provide a detailed summary of media handling processes that do exist.	
Guidance	**Analyst Notes**
Provide a detailed description of where the institution's data will reside.	
Obtain the report if possible and add it to your submission.	
State plans to develop and implement a physical security policy	

Describe how you prevent and detect unauthorized access to your data center.	
Guidance	**Analyst Notes**
Provide a brief summary of how trusted and untrusted networks are segmented.	
Describe any plans to implement a SPI firewall or your currently implemented compensating controls.	
Describe your plan to implement an IDS/IPS in your environment.	
Describe your intent to implement NGPT monitoring.	
Guidance	**Analyst Notes**
State plans to formalize an incident response plan.	

Describe your timeline for implementing such a process for response and reporting.	
Summarize your cyber insurance strategy.	
Summarize your internal approach or reference your third party contractor.	
State plans to implement this capability in the future	
Guidance	**Analyst Notes**
Provide a links to these documents in Additional Information or attach them with your submission.	
Summarize the information security principles designed into the product lifecycle.	
State plans to implement information security policy at your company.	

Guidance	Analyst Notes
No need to answer HLTP-02 through 04	
Ensure that all elements of HLTP-01 are clearly stated in your response.	
Robust answers from the vendor improve the quality and efficiency of the security assessment process.	
Make sure you address any national or regional regulations	

00000048

Have you received the Cloud Security Alliance STAR certification?

Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3

Do you have a well documented Business Continuity Plan (BCP) that is tested annually?

Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?

Do you have a documented change management process?

Has a VPAT or ACR been created or updated for the product and version under consideration within the pa

Do you have documentation to support the accessibility features of your product?