HECVAT - Lite | Vendor Response

Version 3.04

Vendor Response

DATE-01	**Date**	*9/9/2025*

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	Vendor Name	*Cursive Technology, Inc.*
GNRL-02	Product Name	*NA*
GNRL-03	Product Description	*Authorship verification and writing analytics utilizing key event data*
GNRL-04	Web Link to Product Privacy Notice	https://cursivetechnology.com/privacy-policy/
GNRL-05	Web Link to Accessibility Statement or VPAT	
GNRL-06	Vendor Contact Name	*Joseph Thibault*
GNRL-07	Vendor Contact Title	*Founder*
GNRL-08	Vendor Contact Email	joe@cursivetechnology.com
GNRL-09	Vendor Contact Phone Number	*802-735-2066*
GNRL-10	Vendor Accessibility Contact Name	*Vendor Accessibility Contact Name*
GNRL-11	Vendor Accessibility Contact Title	*Vendor Accessibility Contact Title*
GNRL-12	Vendor Accessibility Contact Email	*Vendor Accessibility Contact Email*
GNRL-13	Vendor Accessibility Contact Phone Number	*410-231-3323*
GNRL-14	Vendor Hosting Regions	*US - East (VA)*
GNRL-15	Vendor Work Locations	*Baltimore, MD, USA; Atlanta, GA, USA; Dubai, UAE; Bangladesh*

Vendor 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 requesting institution.

Company Overview		Vendor Answers	Additional Information	Guidance
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	We are founder and employee owned S-Corporation, incorporated in Maryland, USA.		N/A
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	No		N/A
COMP-03	Do you have a dedicated Information Security staff or office?	Yes	Our named security officer is named	Describe your Information Security Office, including size, talents, resources, etc.

COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Yes	As a small team our organization engages some 3rd party resources for development but otherwise manages all aspects of our support, implementation, and product development life-cycle internally.	Describe the structure and size of your Software and System Development teams. (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?	No		
COMP-06	Will data regulated by PCI DSS reside in the vended product?	No		
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	From day one we've build security and privacy into our system due to the nature of the biometric typing data that we collect, analyze, and store. We use and pursue the highest standard of encryption for transferring and storing data and leverage our information system hosting partner (AWS) for their tools to keep data secure.		N/A
Documentation		**Vendor Answers**	**Additional Information**	**Guidance**
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?	No	By leveraging AWS as our information technology hosting partner our system is built upon known quality standards for secure hosting and position our team to pursue SOC2 compliance in the future. Amazon Web Services is responsible for the hosting of our systems and data and they are certified by 3rd party organizations.	Describe any plans to undergo a SSAE 18 audit.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?	No		Describe any plans to complete the CSA CAIQ.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No		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, CIS Controls, ISO 27001, etc.)	No		Describe any plans to conform to an industry standard security framework.
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	Yes	We have not yet pursued 3rd party compliance attestation, but by using AWS infrastructure our systems can be compliant.	Indicate level, Supplier Performance Risk System ('SPRS') Score or certification information.
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?	Yes	https://cursive-shared.s3.us-east-2.amazonaws.com/Cursive+Information+System+%26+Baseline+Configuration.pdf	Provide your diagrams (or a valid link to it) upon submission.
DOCU-07	Does your organization have a data privacy policy?	Yes	https://cursivetechnology.com/privacy-policy/	Provide your data privacy document (or a valid link to it) upon submission.
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes	Cursive Technology Policies and Procedures	Provide a reference to your employee onboarding and offboarding policy and supporting documentation or submit it along with this fully-populated HECVAT.
DOCU-09	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	Yes	Cursive Technology Policies and Procedures	Provide a reference to your BCP and supporting documentation or submit it along with this fully-populated HECVAT.

DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	Yes	Cursive Technology Policies and Procedures	Provide a reference to your DRP and supporting documentation or submit it along with this fully-populated HECVAT.
DOCU-11	Do you have a documented change management process?	Yes	Cursive Technology Policies and Procedures	Summarize your current 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?	Yes	Cursive Technology Policies and Procedures	State the date the VPAT was completed. Include this VPAT in your submission and/or link to its web location.
DOCU-13	Do you have documentation to support the accessibility features of your product?	Yes	Cursive Technology Policies and Procedures	Provide examples with links where possible.
IT Accessibility		**Vendor Answers**	**Additional Information**	**Guidance**
ITAC-01	Has a third party expert conducted an accessibility audit of the most recent version of your product?	Yes	We engaged a 3rd party individual, Jordan Connor of Baltimore, MD. The result of the audit led to the creation of our VPAT located at Cursivetechnology.com/accessibility	State when the audit was conducted and by whom? Include the results in your submission and/or link to its web location.
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	No	Our process engages a qualified 3rd party expert in accessibility and convert their reports to our Plan of Action and Milestones for remediation.	Summarize how you ensure accessible products. Provide plans to develop documented processes to validate accessibility.
ITAC-03	Have you adopted a technical or legal accessibility standard of conformance for the product in question?	Yes	WCAG 2.0 A	Indicate which primary standards and comment upon any additional standards the product meets.
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	No	As we execute action items related to Accessibility on our Plan of Action and Milestones issues are remediated.	Please provide any plans to develop and share an accessibility product roadmap in the future.
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	No	Our team has general awareness of accessibility and is informed of deficiencies by qualified 3rd parties performing periodic review of our system and products.	Describe any plans to ensure appropriate and ongoing staff knowledge about accessibility.
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Yes	Any logged or reported issues become part of our Plan of Action and Milestones process.	Describe the process and any recent examples of fixes as a result of the process.
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes	Any logged or reported issues become part of our Plan of Action and Milestones process.	Provide further details or multiple means in Additional Information.
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	Yes	Verified on Windows 11 via web interface to the browser extension and Moodle LMS (plugin) as recently a 4/10/24	State when and on which platform this was verified.
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a 'lite version' or accessing an alternate interface for accessibility purposes?	No		

Application/Service Security		Vendor Answers	Additional Information	Guidance
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)?	Yes	Client usage is limited to the LMS where the software is installed as a plugin. There is no client access to our information system. Administration of our system is performed by qualified and dedicated internal staff with role-based access controls.	Describe available roles.
HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Yes	In addition to RBAC we also employ AWS IAM security groups to control system access.	
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)	Yes	Operational access is to general productivity tools (e.g. Google Suite). As a remote first organization, access to our information system is limited and by secure key, MFA, or role-based access. Endpoint protection is provided by commercially available services such as Windows Defender, Windows Security, and Activelock	Provide supporting documentation of your strategy.
HLAP-04	Does the system provide data input validation and error messages?	Yes	Logging and task management error reporting is available within the learning management system.	Describe how your system(s) provide data input validation and error messages.
HLAP-05	Are you using a web application firewall (WAF)?	No	We utilize security groups and restrict access to ports to protect the information system. Stateful packet inspection (SPI) firewall via AWS Network Firewall	Describe compensating controls that protect your web application, if applicable.
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Yes	We utilize Github Organization and a combination of private and public repositories for code management in addition to ongoing management of our Plan for Action and Milestones.	Provide supporting documentation of your processes.
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**
HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	Yes	User authentication is via the client learning management system only. Auth for other aspects is supported by Google. There is no direct login to Cursive user data or services.	Describe how strong authentication is enforced (e.g., complex passwords, multifactor tokens, certificates, biometrics, aging requirements, re-use policy).
HLAA-02	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	No	We will consider eduGAIN if and as required.	Describe plans to participate in InCommon or another eduGAIN affiliated trust federation.
HLAA-03	Does your application support integration with other authentication and authorization systems?	No	We support LTI integration, otherwise the application is natively integrated to the learning management system inhereting all authentcation methods utilized by the client.	Describe any plans to 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]	Yes	Learning Tools Interoperability (LTI) standard.	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.
HLAA-05	Do you support differentiation between email address and user identifier?	Yes	In a native implementation, only a unique user identifier is collected.	

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]	No	Not applicable.	Describe plans to allow customers to specify attribute mappings.
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?	Yes	These are available via the client LMS.	
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.)	Yes	2FA is utilized for our application	List all supported multi-factor authentication methods, technologies, and/or products and provide a brief summary of each.
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?	Yes	This defaults to the client LMS settings.	Describe the default behavior of this capability.
Systems Management		**Vendor Answers**	**Additional Information**	**Guidance**
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)?	Yes	We have created a baseline configuration model and network architecture outlining data flows and integration. This includes and end to end depiction of client to system, and system to system connectivity to our infrastructure.	Summarize your systems management and configuration strategy.
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Yes	In the event that our internal Security Impact Analysis identifies a change that will impact an institution's security posture the institution will be alerted.	State how and when the institution will be notified of major changes to your environment.
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?	Yes	As part of configuration management, testing, QA, and deployment.	Provide a brief description.
HLSY-04	Have your systems and applications had a third party security assessment completed in the last year?	Yes	A 3rd party review was completed Dec '23/Jan '24 using Tenable Nessus.	Provide the results with this document (link or attached), if possible. State the date of the last completed third party security assessment.
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	In the event a security improvement, flaw, or vulnerability is identified, required updates for remediation will be documented in a Plan of Action and Milestones and carried out through existing change and configuration management processes.	Summarize the policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.
Data		**Vendor Answers**	**Additional Information**	**Guidance**
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).	Yes	As necessary, we can create and manage dedicated single-tenant systems for customers. However, as rule and per our data security and privacy policies, customer data is identified and categorized by source, user, resource ID and a secure token to ensure customer data is not available to any other customer. End user access is limited by role on the local learning management system.	Describe or provide a reference to how institution data is separated from that of other customers.
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	Yes	TLS 1.2	Summarize your transport encryption strategy
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	Yes	CNSA approved encryption for data at rest.	Summarize your data encryption strategy and state what encryption options are available.

HLDA-04	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Yes	We utiilize automation within AWS for backup management.	If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.
HLDA-05	Can the Institution extract a full or partial backup of data?	Yes	All data available via the client's LMS to pull manually.	Provide a general summary of how full and partial backups of data can be extracted.
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?	Yes	We do not collect media.	Provide documented details of this process (link or attached).
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?	Yes	Only authorized team members have access to internal systems following Principle of least privilege.	Summarize what access staff (or third parties) have to institutional data.
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**
HLDC-01	Does your company manage the physical data center where the institution's data will reside?	No	AWS	Provide a detailed description of where the institution's data will reside.
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?	Yes	As required by law or contract.	
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf	Obtain the report if possible and add it to your submission.
HLDC-04	Does your organization have physical security controls and policies in place?	Yes	Fully inhereted from AWS.	Describe your physical security strategy.
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?	Yes	Fully inhereted from AWS.	Describe how you prevent and detect unauthorized access to your data center.
Networking		**Vendor Answers**	**Additional Information**	**Guidance**
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?	Yes	We utilize AWS organization management to close our network and only provide access through secure token-based authentication for external connections.	Provide a brief summary of how trusted and untrusted networks are segmented.
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	Via AWS Network Firewall	Describe the currently implemented SPI firewall.
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?	No	At this time with AWS Network Firewall implemented we have postponed commercial IDS monitoring.	Describe your plan to implement an IDS/IPS in your environment.
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?	No	Our we will evaluate and adopt commercially available solution such as AWS GuardDuty as needed.	Describe your intent to implement 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?	Yes	Periodically (and temporarily) we may need temporary access for support, troubleshooting, or training.	Describe the tools and technical controls implemented to secure remote access.
Incident Handling		**Vendor Answers**	**Additional Information**	**Guidance**

HLIH-01	Do you have a formal incident response plan?	Yes	Cursive Technology Policies and Procedures	Summarize or provide a link to your 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?	Yes	At the time an incident becomes known, we triage, act, and remediate based on the designated severity level.	Summarize your incident response and reporting processes.
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes	Cyber risk insurance is provided through The Hanover Insurance Group of Towson, MD.	Summarize your cyber insurance strategy.
HLIH-04	Do you have either an internal incident response team or retain an external team?	Yes	Our small team manages all incident response processes.	Summarize your internal approach or reference your third party contractor.
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?	Yes	As a small team we have created an incident response plan to resolve issues as quickly as possible.	Describe the implemented procedure for 24/7/365 coverage.
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	Cursive Technology Policies and Procedures	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	We aim for SOC2 type 2 Compliance at a later date, in effort to meet this information security principles are designed into the product lifecycle.	Summarize the information security principles designed into the product lifecycle.
HLPP-03	Do you have a documented information security policy?	Yes	Cursive Technology Policies and Procedures	Provide a reference to your information security policy or submit documentation with this fully-populated HECVAT-Lite.
Third Party Assessment			**Additional Information**	**Guidance**
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)	Yes	Hosting providers and cloud services such as AWS.	State each third party which institutional data will be shared with and/or hosted by and their level of responsibility.
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.).	Yes	In evaluation of our third party companies we look 3rd party attestations, clear policies, and available documentation to support enterprise level security policies and practices.	Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.
HLTP-03	Do you have an implemented third party management strategy?	Yes	We work with AWS directly when evaluating infrastructure, tools, and services which can improve and support our information systems and architecture.	Provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)		Not applicable.	Make sure you address any national or regional regulations