Higher Education Cloud Vendor Assessment Tool - Lite

HEISC Shared Assessments Working Group

DATE-01	**Date**	

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 Cloud Vendor Assessment Tool. 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-06; populated by Institution		
GNRL-01	Institution Department	*Institution Department Name*
GNRL-02	Institution Department Primary Campus	*Primary Campus*
GNRL-03	Institution Department Code	*Institution Department Code*
GNRL-04	Institution Department Contact Name	*Institution Department Contact Name*
GNRL-05	Institution Department Contact Email	*Institution Department Contact Email*
GNRL-06	Institution Department Contact Phone Number	*555-555-5555*
GNRL-07 through GNRL-14; populated by Vendor		
GNRL-07	Vendor Name	*Degree Analytics*
GNRL-08	Product Name	*Engauge*
GNRL-09	Product Description	*Engauge uses institution data, such as LMS, SIS, and WiFi logs, to derive and calculate student behaviors such as library usage. The platform then performs machine learning to understand what behaviors lead to success and failure.*
GNRL-10	Web Link to Product Privacy Notice	*https://drive.google.com/open?id=184Mi-OXISPnkTAcet3Q0pG8GINakKRTg*
GNRL-11	Vendor Contact Name	*Aaron Benz*
GNRL-12	Vendor Contact Title	*CEO*
GNRL-13	Vendor Contact Email	*aaron@degreeanalytics.com*
GNRL-14	Vendor Contact Phone Number	*931-532-0452*
GNRL-15 and GNRL-16; populated by Institution Security Office		
GNRL-15	Campus Security Analyst/Engineer	*Campus Security Analyst/Engineer Name*
GNRL-16	Assessment Contact	*ticket#@yourdomain.edu*

Higher Education Shared Assessments Confirmation

By completing the Higher Education Cloud Vendor Assessment Tool, cloud service providers understand that the completed assessment may be shared among higher education institutions. Answers to the following statements will determine how this assessment may be shared within the Higher Education community. Shared assessment sharing details can be found on the "Sharing Read Me" tab.

		Vendor Answers	Additional Information
HESA-01	I understand the goal of Higher Education Shared Assessments and that the completed Higher Education Cloud Vendor Assessment Tool may be shared with other higher education institutions, based on the following selections.	Yes	Scope: Higher Education Institutions Only
HESA-02	Add this completed assessment to a list of Higher Education assessed service providers, with contact information for service providers. No answers are shared; it is a list stating vendor, product, version, and service provider contact information.	Yes	Scope: Higher Education Institutions Only
HESA-03	This completed Vendor Assessment Tool (with vendor answers intact) can be shared within Higher Education institutions through the Cloud Broker Index, https://www.ren-isac.net/hecvat/cbi.html.	Yes	Scope: Higher Education Institutions Only
HESA-04	The security report created by this Higher Education institution, after evaluating this assessment, can be shared within Higher Education institutions.	Yes	Scope: Higher Education Institutions Only

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 Cloud Vendor Assessment Tool - Lite to the Institution according to institutional procedures.

Documentation		Vendor Answers	Additional Information
DOCU-01	Have you undergone a SSAE 16 audit?	Yes	Degree Analytics' cloud provider AWS routinely performs SOC 1 and SOC 2 and SOC 3 audits from a third party auditor
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?		
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Special Publication 800-53, ISO 27001, etc.)	Yes	Yes. All systems are run in environments or tools where Amazon Web Services has run audits or achieved certifications for SOC 1, SOC 2, SOC 3, ISO 9001, ISO 27001, ISO 27017, ISO 27018, as is best practice for FERPA compliance on AWS
DOCU-05	Are you compliant with FISMA standards (indicate at what level)?	Yes	Degree Analytics' cloud provider AWS has achieved FISMA Moderate Authorization and Accreditation from the US General Services Administration
DOCU-06	Does your organization have a data privacy policy?	Yes; Upon request can be provided	Degree Analytics has a Data Security Document that outlines how data is used, processed, and stored within the system

Company Overview		Vendor Answers	Additional Information
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	MF Genius, Corp d.b.a Degree Analytics is based in Austin, TX, and has been in existence since 2014. We serve higher education institutions in identify at-risk students as well as provide insights into student behavior and engagement.	
COMP-02	Describe how long your organization has conducted business in this product area.	3 Years	
COMP-03	How many higher education, commercial customers and government customers do you serve in North America? Please provide a higher education customer reference if available.		

COMP-04	Please explain in detail any involvement in business-related litigation in the last five years by your organization, its management, or the staff that will be providing the administrative services.	There is not any active or past business-related litigation	
COMP-05	Describe the structure and size of your Security Office and overall information security staff. (e.g. Admin, Engineering, QA/Compliance, etc.)	2 Administrators, 1 Engineer	
COMP-06	Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)	Degree Analytics has dedicated full time development engineers, project managers, QA testers	
COMP-07	Use this area to share information about your environment that will assist those who are evaluating you company data security safeguards.	Degree Analytics uses hash separation that is built into the foundation of all storage and access of data. This prevents different users and institutions from seeing information that does not belong to them. Additionally, it prevents Degree Analytics's employees from accessing information that is forbidden to them. Our data rests on AWS's S3 environment, as well as in a Cassandra database that assures data redundancy. All outside connections are made using strictly TLS encryption, and all internal access has a series of restricted IP ranges and ssh certifications. Production access is heavily restricted to team members whose responsibilities require such access.	
Application/Service Security		**Vendor Answers**	**Additional Information**
HLAP-01	Can user access be customized to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions?	Yes	Yes, users can be restricted to read-only access, update access, individual student access, cohort access (groups of students)
HLAP-02	Describe or provide a reference to how user security administration is performed?	Each institution is given one administrator as designated by the institution that serves as the campus administrator. That administrator then has the ability to add users to the institution and assign different levels of access.	
HLAP-03	Describe or provide a reference to the controls that are in place to secure their remote environment and connection to institution's data.	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.	
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; Upon request can be provided	We have a Data Security Document that express how each system is used, protections around each system, as well a diagram that shows how each component works within the system
HLAP-05	Does the system provide data input validation and error messages?	Yes	Yes, all API requests are validated against specific and accepts schema types. Additionally, all of our errors are well documented whether its invalid input, access, etc…
HLAP-06	Do you employ a single-tenant or multi-tenant environment?	Yes	Multi-tenant environment
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**
HLAA-01	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Yes	Can configure minimum character requirements, requirements of numbers, special characters, and uppercase characters
HLAA-02	Describe or provide a reference to the types of authentication, including standards-based single-sign-on (SSO, InCommon), that are supported by the web-based interface?	Google SSO, Other	
HLAA-03	Describe or provide a reference to the authentication and authorization systems such as Active Directory, Kerberos (what version) or a institution centralized authorization service that work with your application.	Google SSO	
HLAA-04	Does the system (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	Yes	Currently in road map to support SAML 2.0 protocol
HLAA-05	Does your system have the capability to log security/authorization changes as well as user and administrator security (physical or electronic) events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system. Include information about SIEM/log collector usage.	Yes	All user actions through web application/api are recorded. If necessary, they are available upon request
Business Continuity Plan		**Vendor Answers**	**Additional Information**
HLBC-01	Do you have a documented Business Continuity Plan (BCP)? If so, can it be shared?	Yes; Upon request can be provided	Degree Analytics has BCP and DRP that include processes and the contacts information of desired parties in case of such an event
HLBC-02	Is there a documented communication plan in your BCP for impacted clients?	Yes	Degree Analytics has BCP and DRP that include processes and the contacts information of desired parties in case of such an event
HLBC-03	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes	Degree Analytics has BCP and DRP that include processes and the contacts information of desired parties in case of such an event. In addition, Degree Analytics leverage's Amazon Web Services to create a distributed architecture to protect against disasters.
HLBC-04	Does your organization conduct an annual test of relocating to this alternate site for business recovery purposes?	Yes	Employees are encouraged and inevitably visit and work out of the alternate location several times a year
Change Management		**Vendor Answers**	**Additional Information**
HLCH-01	Do you have a Change Management Plan? If so, can it be shared?	Yes	All new code is ran against a lengthy unit tests process. Updates will not proceed if a single unit test is not run successfully. Any changes to existing unit tests must be approved by employee manager in code reviews. Once code passes test, and a code review is completed, code is merged and executed in a development environment. Once development environment is shown to be viable and secure, approved by appropriate IT managers, update is scheduled to deploy.

HLCH-02	How and when will the Institution be notified of major changes to your environment that could impact our security posture?	Yes; Any changes they may require security changes are notified as early as possible, and we will work closely with Institution to make sure they understand ramifications of change. At minimum, 7 days in advance of any planned change that would qualify as "major". Notification may be provided in the form of phone, text, and email.	
HLCH-03	Do you have documented procedures on how security risks are mitigated until patches can be applied? If so, can it be shared?	Yes	If a critical patch is required immediately, it must first pass all unit tests and pass development environment tests. If successful, it is deployed in a rolling update so insure no or minimal customer downtime
HLCH-04	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)? If so, can it be shared?	Yes	After going through emergency patch updates, all changes must be documented and approved
Data		**Vendor Answers**	**Additional Information**
HLDA-01	Is institution data physically and logically separated from that of other customers.	Yes	Degree Analytics uses a logical hash separation that is built into the foundation of all storage and access of data. This prevents different users and institutions from seeing information that does not belong to them. In short, each user has a unique id that is tied to an institution unique id so that data may only be accessed when a particular user id is given access to a particular institution id. Additionally, it prevents Degree Analytics's employees from accessing information that is forbidden to them.
HLDA-02	Is sensitive data encrypted in transport and storage (e.g. disk encryption and at-rest)?	Yes	All transmission of data is used over TLS - all HTTPS certificates are managed by AWS Certificate Manager. Data is additionally encrypted at rest through the AES-256 algorithm through AWS IAM Encrypted Keys.
HLDA-03	Do backups containing institution data ever leave the United States of America either physically or via network routing?	Yes	All data from the USA remains in the USA
HLDA-04	Describe or provide a reference to your media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures.	Degree Analytics has a data security document that may be provided upon request which describes the time to live of all data entering the system, as well as de-identification procedures	
HLDA-05	Is any institution data visible in system administration modules/tools?	Yes	No institutional data is visible through system administration tools or modules.
Database		**Vendor Answers**	**Additional Information**
HLDB-01	Does the database support encryption of specified data elements in storage?	Yes	All data in the database is encrypted at rest with AWS IAM Encrypted Keys.
HLDB-02	Do you currently use encryption in your database?	Yes	All data in the database is encrypted at rest with AWS IAM Encrypted Keys.
Datacenter		**Vendor Answers**	**Additional Information**
HLDC-01	List all datacenters and their cities, states (provinces), and countries where institution data will be stored (including within the United States). Does your company own these data centers?	Degree Analytics utilizes Amazon Web Services to store its data in two availability zones: Northern Virginia (US East) and Oregon (US West)	
HLDC-02	Does your company own the physical data center where institution data will reside? If so, do these servers reside in a co-located data center?	Yes	No, Degree Analytics does not own the physical data centers.
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	Yes
HLDC-04	Does the physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	Yes	Degree Analytics uses Amazon Web Services, who has employed several mechanism to prohibit unauthorized access. See AWS's controls here: https://aws.amazon.com/compliance/data-center/controls/
Disaster Recovery Plan		**Vendor Answers**	**Additional Information**
HLDR-01	Do you have a Disaster Recovery Plan (DRP)? If so, can it be shared?	Yes; Upon request can be provided	Degree Analytics has BCP and DRP that include processes and the contacts information of desired parties in case of such an event
HLDR-02	Are any disaster recovery locations outside the United States? If so, please provide the locations.	Yes	No, Degree Analytics does not have any location outside the United States
HLDR-03	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes	Degree Analytics has BCP and DRP that include processes and the contacts information of desired parties in case of such an event. It includes a minimal annual review
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**
HLFI-01	Are you utilizing a web application firewall (WAF) and / or a stateful packet inspection (SPI) firewall?	Yes	Degree Analytics uses WAF to block potential dangerous traffic
HLFI-02	Do you have a documented policy for firewall change requests? If so, can it be shared?	Yes	Security Groups and ACLs are used to restrict traffic to and inside of the virtual private cloud.
HLFI-03	Describe or provide a reference to any other safeguards used to monitor for attacks?	Degree Analytics actively monitors traffic and adjusts firewall protections in line with best practices and use of network. Degree Analytics uses WAF to block and prevent dangerous traffic	
HLFI-04	Do you monitor for intrusions on a 24x7x365 basis?	Yes	Yes, Degree Analytics has setup monitoring services that work around the clock. Beyond preventative tools already mentioned, Degree Analytics has a comprehensive set of monitors that may trigger alarms as a response to intrusions
Physical Security		**Vendor Answers**	**Additional Information**
HLPH-01	Does your organization have physical security controls and policies in place? If so, can it be shared?	Yes	Degree Analytics has procedures to report incidents, as well as monitors guest visits & usage by guests, and access to facility
HLPH-02	Are employees allowed to take home customer data in any form?	Yes	No, Employees are not allowed to take customer data. Customer data is highly restricted to select employees who must access that data with proper identifying security credentials as well as from select IP ranges.

Policies, Procedures, and Processes		Vendor Answers	Additional Information
HLPP-01	Can you share the org chart, mission statement and policies for your information security unit?	Yes; Upon request can be provided	You may find some of this information online. Degree Analytics polices in place, as well a culture that is concentrated on keeping students safe and providing insights that enable them to succeed.
HLPP-02	Are information security principles designed into the product and / or SDLC lifecycle?	Yes	The design and engineering process is full of several controls which establish when and how certain code can get deployed. This includes processes like code reviews, unit testing, development testing, and approvals. Degree Analytics performs sets of both static and dynamic tests to perform application code reviews.
HLPP-03	Do you have a formal incident response plan? If so, can it be shared?	Yes	Yes, Degree Analytics has a process for such incidents that include: 1) Preparation (proper training before any incident occurs) 2)Identification 3) Containment 4) Eradication 5) Recovery 6) Lessons Learned
HLPP-04	Do you have a documented information security policy? If so, can it be shared?	Yes; Upon request can be provided	Yes, Degree Analytics has Data Security Policy that governs how we work and use institutions data.
Systems Management & Configuration		**Vendor Answers**	**Additional Information**
HLSY-01	Are systems that support this service managed via a separate management network?	No	No, systems supporting Degree Analytic's service are not managed via a separate management network. Degree Analytics uses a Virtual Private Cloud within AWS - all access is governed by security controls set in AWS IAM.
HLSY-02	Can you provide a general summary of your systems management and configuration strategy, including servers, appliances, and mobile devices (company and employee owned).	Yes	Degree Analytics has roles and policies in place that govern the use and change of systems in the network. Changes to the system undergo specific approval and are available only to select roles.
Vulnerability Scanning		**Vendor Answers**	**Additional Information**
HLVU-01	Have your systems and applications had a third party security assessment completed in the last year? If so, can the results be provided?	Yes	Degree Analytics performs both internal and external vulnerability scans on a weekly basis. Test packages include Common Vulnerabilities and Exposures; CIS Operating System Security Configuration Benchmarks; Runtime Behavior Analysis; Security Best Practices
HLVU-02	Are your applications scanned for vulnerabilities prior to new releases? If so, can the results be provided?	Yes	Yes, Degree Analytics has testing suites that are run frequently on production and development environments to ensure that any release has been scanned before being moved into production.