Higher Education Community Vendor Assessment Tool (HECVAT) - Lite

Version 2.11

HEISC Shared Assessments Working Group

DATE-01	**Date**	*4/16/25*

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	*EquipCheck, LLC*
GNRL-02	Product Name	*EquipCheck*
GNRL-03	Product Description	*Athletic Equipment Inventry Tracking Software, cloud based and mobile apps included*
GNRL-04	Web Link to Product Privacy Notice	https://getequipcheck.com/privacy.html
GNRL-05	Vendor Contact Name	*Brad*
GNRL-06	Vendor Contact Title	*Lead Developer*
GNRL-07	Vendor Contact Email	support@equipchecksoftware.com
GNRL-08	Vendor Contact Phone Number	*1-877-77-EQUIP*
GNRL-09	Vendor Data Zone	*USA*
GNRL-10	Institution Data Zone	*USA*
GNRL-11 and GNRL-12; populated by Institution's Security Office		
GNRL-11	Campus Security Analyst/Engineer	
GNRL-12	Assessment Contact	

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?	No		Describe any plans to undergo a SSAE 16 audit.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	No		Describe any plans to complete the CSA self assessment or 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, ISO 27001, etc.)	No		Describe any plans to conform to an industry standard security framework.
DOCU-05	Are you compliant with FISMA standards?	No		Describe any plans to become FISMA compliant.
DOCU-06	Does your organization have a data privacy policy?	Yes	https://getequipcheck.com/privacy.html	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.	EquipCheck is owned by individuals residing in the US who are all US citizens.		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.	7 Years		Include the number of years and in what capacity.
COMP-03	Do you have existing higher education customers?	Yes	University of South Alabama, Florida International University, Georgia Southern University, South Florida University, University of New Mexico, University of Nevada Las Vegas, many more	Provide a list of Higher Ed references, with contact information.
COMP-04	Have you had a significant breach in the last 5 years?	No		
COMP-05	Do you have a dedicated Information Security staff or office?	Yes		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		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.	Our cloud solution is hosted on then Google App Engine platform. This provides secuirty and scalablity for the web app, and mobile apps.		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	We provide a custom solution to allow fine grain controler over what users have permissions to.	Describe any infrastructure dependencies.
HLAP-02	Do you support role-based access control (RBAC) for system administrators?	Yes		Describe the utilized technology.
HLAP-03	Can employees access customer data remotely?	Yes	Using the secure console provided by Google App Engine we may have remote access to customer data to facilitate support calls.	If available, submit documentation and/or web resources.
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?	No		State any plans to provide system and/or application architecture diagrams.
HLAP-05	Does the system provide data input validation and error messages?	Yes		Provide a reference to documentation of your data input validation and error messaging capabilities.
HLAP-06	Do you employ a single-tenant environment?	No		
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**
HLAA-01	Can you enforce password/passphrase aging requirements?	No		Describe plans to support password/passphrase aging requirements.
HLAA-02	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)	Yes	We implement our own custom authentication that ensure users can only access account data they have permissions to.	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?	No	None	Describe any plans to support integration with other 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?	No	None	Describe any plans to support external authentication services in place of local authentication.
HLAA-05	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes	Every page opened by the user and every bit of data they change is logged.	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)?	No	None	Describe your intention to complete a Business Continuity Plan.
HLBC-02	Is there a documented communication plan in your BCP for impacted clients?	No	None	Describe any plans to document a communication plan in your BCP.
HLBC-03	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	No	None	Describe any plans to annually review and update (as needed) your BCP.
HLBC-04	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	No	None	Describe your strategy to implement annual alternate site relocation testing.
Change Management		**Vendor Answers**	**Additional Information**	**Guidance**
HLCH-01	Do you have a documented and currently followed change management process (CMP)?	No		Describe current plans to implement a 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	Any large change would be documented and rolled out to clients via email mailing list. This would include any changes that effect how or where their data is stored.	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	All security risks are logged in realtime. Any issues will be reported and prioritized to be corrected. If any data is effect the respective clients will be notified.	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)?	No	There are no emergency proceducres. All code changes will go through the same process.	Describe plans to implement procedure 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	Each account has it's own database that is completely separate from other accounts. The credentials are different to ensure it's not possible to access anothers account.	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		Summarize your transport encryption strategy.
HLDA-03	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	Yes		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		
HLDA-05	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?	No	No physical media	Provide a detailed summary for this response.

HLDA-06	Is any institution data visible in system administration modules/tools?	Yes	In order to facilitate customer support calls. As well as we provide services where we do work for the custom. Such as importing their orders from vendors into their account.	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 is encrypted at rest.	Describe the type of encryption that is supported.
HLDB-02	Do you currently use encryption in your database(s)?	Yes		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		
HLDC-02	Does your company own the physical data center where the institution's data will reside?	No	Google App Engine has distrupted systems nation way to allow for fastest data processing based on the users location.	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		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?	No	No physical media	State plans to implement a physical barrier to prevent physical contact with any of your devices.
Disaster Recovery Plan		**Vendor Answers**	**Additional Information**	**Guidance**
HLDR-01	Do you have a Disaster Recovery Plan (DRP)?	No		State any plans to create a Disaster Recovery Plan.
HLDR-02	Are any disaster recovery locations outside the institution's Data Zone?	No		
HLDR-03	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	No		State plans to implement annual (at a minimum) testing of your DRP.
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	Built into Google App Engine platform	Describe the currently implemented WAF.
HLFI-02	Do you have a documented policy for firewall change requests?	No		Describe your plans to implement a documented policy for firewall change requests.
HLFI-03	Are you employing any next-generation persistent threat (NGPT) monitoring?	No		Describe your intent to implement NGPT monitoring.

HLFI-04	Do you monitor for intrusions on a 24x7x365 basis?	Yes		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?	No		Describe your intent to implement physical security controls and policies.
HLPH-02	Are employees allowed to take home customer data in any form?	No		
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?	No		Provide a brief summary for this response.
HLPP-02	Are information security principles designed into the product lifecycle?	Yes		Summarize the information security principles designed into the product lifecycle.
HLPP-03	Do you have a formal incident response plan?	No		State plans to formalize an incident response plan.
HLPP-04	Do you have a documented information security policy?	No		State plans to implement information security policy at your company.
Systems Management & Configuration		**Vendor Answers**	**Additional Information**	**Guidance**
HLSY-01	Are systems that support this service managed via a separate management network?	Yes		Provide a brief description of how this is implemented.
HLSY-02	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?	No		Describe your intent to implement a 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?	No		State plans to have your systems and applications assessed by a third party.
HLVU-02	Are your systems and applications scanned for vulnerabilities [that are remediated] prior to new releases?	Yes		Provide a brief description.