Higher Education Cloud Vendor Assessment Tool

Version 1.05

HEISC Shared Assessments Working Group

DATE-01	**Date**	*3/4/2018*

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. Review the *Instructions* tab for further guidance.

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	Vendor Name	*CasinoVision Inc*
GNRL-08	Product Name	*Valt - (Video Audio Learning Tool) manufactured by Intelligent Video Solutions*
GNRL-09	Product Description	*Audio/Video recording system for student training and performance assessment*
GNRL-10	Web Link to Product Privacy Notice	*NA*
GNRL-11	Vendor Contact Name	*Richard Bungey*
GNRL-12	Vendor Contact Title	*President*
GNRL-13	Vendor Contact Email	richard@cvisecurity.com
GNRL-14	Vendor Contact Phone Number	*262-569-1986*
GNRL-15	Institution Security Analyst/Engineer	*Institution Security Analyst/Engineer Name*
GNRL-16	Assessment Contact	*ticket#@yourdomain.edu*

Higher Education Shared Assessments Confirmation		Vendor Answers	Additional Information	Guidance
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.				
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		
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; OK to List		
HESA-03	This completed assessment (with vendor answers intact) can be shared within Higher Education institutions.	Yes; OK to Share		
HESA-04	The security report created by this Higher Education institution, after evaluating this assessment, can be shared within Higher Education institutions.	Yes; OK to Share		

Instructions

Step 1: Complete the *Qualifiers* section first. **Step 2:** Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. **Step 3:** Submit the completed Higher Education Cloud Vendor Assessment Tool (HECVAT) to the Institution according to institutional procedures.

Qualifiers		Vendor Answers	Additional Information	Guidance
The Institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented and allows for various parties to utilize this common documentation instrument. **Responses to the following questions will determine the need to answer additional questions below**.				
QUAL-01	**Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?**	No	**Unknown**	Responses to the questions in the HIPAA section are optional.
QUAL-02	**Does the vended product host/support a mobile application?** (i.e. app)	No		Responses to the questions in the Mobile Application section are optional.
QUAL-03	**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)	No		Responses to the questions in the Third Parties section are optional.
QUAL-04	**Do you have a Business Continuity Plan (BCP)?**	No		Responses to the questions in the Business Continuity section are optional.
QUAL-05	**Do you have a Disaster Recovery Plan (DRP)?**	No		Responses to the questions in the Disaster Recovery section are optional.
QUAL-06	**Will data regulated by PCI DSS reside in the vended product?**	No		Responses to the questions in the PCI DSS section are optional.
QUAL-07	**Is your company a consulting firm providing only consultation to the Institution?**	No		Responses to the questions in the Consulting section are optional.

Documentation		Vendor Answers	Additional Information	Guidance
DOCU-01	Have you undergone a SSAE 16 audit?	No	**Not Applicable**	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 Special Publication 800-53, ISO 27001, etc.)	No		Describe any plans to conform to an industry standard security framework.

DOCU-05	Are you compliant with FISMA standards (indicate at what level)?	No		Describe any plans to become FISMA compliant.
DOCU-06	Does your organization have a data privacy policy?	No		Describe any plans to provide a data privacy document.
Company Overview		**Vendor Answers**	**Additional Information**	**Guidance**
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	Privately held Corporation. No subsidiary or parent relationships. No offshoring agreements		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.	2011-2017		
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.	Client list enclosed in CVI Profile. Aproximately 50. Customer references enclosed. Intelligent Video Solutions has over 250 customer installs. The majority of the installs on in data sensitive areas such as speech therapy, psychology, and counseling clinics.		
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.	None		
COMP-05	Describe the structure and size of your Security Office and overall information security staff.	Not applicable as we do not store any HIPAA data		
COMP-06	Describe the structure and size of your Software and System Development teams.	In house and 3rd party developmement Approximately 10 people		
COMP-07	Use this area to share information about your environment that will assist those who are evaluating you company data security safeguards.	With the Valt application it is running on your infrastructure. Please reference our technical document which is attached for a summary of how Valt is implemented in your environment.		
Third Parties - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). 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.	Not Applicable. No data shared.		
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	Not Applicable		
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	Not Applicable		
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	Not Applicable		
Consulting - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
CONS-01	Will the consulting take place on-premises or remotely?		**Section Not applicable**	
CONS-02	Will the consultant require access to institution network resources?			
CONS-03	Will the consultant require access to hardware in the university data centers?			
CONS-04	Will the consultant require an account within the institution's domain (@*.edu)?			
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?			
CONS-06	Will any data be transferred to the consultant's possession?			
CONS-07	How long will it remain in their possession?			
CONS-08	Is it encrypted (at rest) while in the consultant's possession?			
CONS-09	Will the consultant need remote access to the institution's network or systems?			
CONS-10	What software will be used to facilitate that access?			
CONS-11	Can we restrict that access based on source IP address?			
Application/Service Security		**Vendor Answers**	**Additional Information**	**Guidance**
APPL-01	Does the application/service support being virtualized?	Yes	None	Describe any infrastructure dependencies.
APPL-02	Are the servers hosting institution data currently deployed in a virtualized environment?	No		Describe any plans to virtualize your environment hosting University data.
APPL-04	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		If available, submit documentation and/or web resources.

APPL-05	Describe or provide a reference to how user security administration is performed?	Extensive user permissions are granted by user group		
APPL-06	Define the access control roles of employees that will have access to the data and in what capacity.	Our emplopyees will have not access to data as it will be operating on your own infrastructure without permission.		
APPL-07	Do you allow employees to remotely access data (aka work from home)?	No		
APPL-09	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to university data?	Ubuntu - The only data that Valt would have access to is LDAP - With Valt no data from LDAP is downloaded or stored in Valt except user names. No passwords are downloaded. Valt authenticates against University login		List all operating systems and the roles that are fulfilled by each.
APPL-10	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?	No		*
APPL-11	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	Please reference attached technical document		Describe the products and how they will be implemented.
APPL-12	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	Please reference attached technical document		
APPL-13	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	Yes	Please reference attached technical document	Provide a brief description.
APPL-14	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	Please reference attached technical document		Include user-end and adminstrative features and functionality.
APPL-16	Describe or provide a reference to any OS and/or web-browser combinations that are not currently supported.	Please reference attached technical document		
APPL-17	Can your system take advantage of mobile and/or GPS enabled mobile devices?	No		
APPL-18	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	Not applicable		
APPL-19	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	Most administration functions are the same as general user access. Technical administration will require SSH Access.		
APPL-20	Does the system provide data input validation and error messages?	Yes		If available, submit documentation and/or web resources.
APPL-21	Do you employ a single-tenant or multi-tenant environment?	Single-tenant	Not Applicable	
APPL-22	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc…).	Not Applicable		

Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**
AAAI-01	Can you enforce password/passphrase aging requirements?	Yes	Through LDAP Integration	
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Yes		
AAAI-03	What are the minimum and maximum password lengths supported, and what types of characters are supported?	Varies depending upon Authentication method of choice		
AAAI-04	Describe the current/default/supported password/passphrase reset procedures?	Varies depending upon Authentication method of choice		
AAAI-05	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?	Please reference attached technical document		Include user-end and adminstrative authentication types.
AAAI-06	Are there any passwords/passphrases "hard coded" into your systems or products?	No		
AAAI-07	Are user account passwords/passphrases visible in administration modules?	No		
AAAI-08	Are user account passwords/passphrases stored encrypted?	Yes		
AAAI-09	Describe or provide a reference to the algorithm/strategy that is used to encrypt stored passwords/passphrases?	SHA-256		
AAAI-10	Does your *application* and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	No		Describe any plans to provide Duo support.

AAAI-11	List all supported multi-factor authentication methods, technologies, and/or products and provide a brief summary of each.	None		
AAAI-12	Does your *application* support integration with other authentication and authorization systems such as Active Directory, Kerberos (what version) or another institution centralized authorization service?	Yes	Not Applicable	Provide a brief description.
AAAI-13	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	No		
AAAI-14	Does the *system* (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	Yes		Describe all authentication services the system supports.
AAAI-15	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?	Yes		Provide a detailed description.
AAAI-16	Will any external authentication or authorization system be utilized by a system with access to institution data?	No	Not Applicable	
AAAI-17	Are audit logs available that include ALL of the following; login, logout, actions performed, and source IP address?	Yes		Provide a description, if necessary.
AAAI-18	Describe or provide a reference to the system 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.	All events within the system are logged including access, starts and stop recording, viewing, data management actions and administration changes.		
AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	Logs are held indefinitely		

BCP - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
BCPL-01	Describe or provide a reference to your Business Continuity Plan.	Section Not Applicable		
BCPL-02	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?			
BCPL-03	If possible, can the institution review your Business Continuity Plan and supporting documentation?			
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?			
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?			
BCPL-06	Are all components of the Business Continuity Plan reviewed at least annually and updated as needed to reflect change?			
BCPL-07	Indicate the last time that the Business Continuity Plan was tested and provide a summary of the results.			
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?			
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?			
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?			
BCPL-11	Does your organization conduct an annual test of relocating to this alternate site for business recovery purposes?			
BCPL-12	Indicates the priority of service restoration for services utilized by the Institution compared to other applications/services the vendor provides.			

Change Management		**Vendor Answers**	**Additional Information**	**Guidance**
CHNG-01	Do you have a documented and currently followed change management process (CMP)?		Not Applicable	
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.	Not applicable		
CHNG-03	How and when will the institution be notified of major changes to your environment that could impact our security posture?	Not applicable		
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	Yes	Institutions have the option to upgrade software as they wish	
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	All versions are supported concurrently		
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	4.1.7- 60%		
CHNG-07	Describe, if applicable, your support for client customizations from one release to another.	None - Although most updates are a result of enhancement requests.		

CHNG-08	How does your organization ensure that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	Extensive testing		
CHNG-09	Describe or provide a reference to your release schedule for product updates.	Release schedule is generally twice per year		
CHNG-10	Describe or provide a reference to your technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed.	HTML5 Support - user Features - Updated UI - Multi Template - Marker Enhancement		
CHNG-11	Describe or provide a reference to your expectation of client involvement with product updates?	We require access to the server if applied by IVS engineers or updates can be self administered via scripts.		
CHNG-12	Provide a brief summary of how critical patches are applied to all systems and applications.	See above		
CHNG-13	Describe or provide a reference to how security risks are mitigated until patches can be applied.	Not applicable -		
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Yes		Provide a detailed description.
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	No	Not Applicable	Provide a detailed description.
Data		**Vendor Answers**	**Additional Information**	**Guidance**
DATA-01	Describe the highest level of data classification that will be managed within your system(s) and/or application(s).	Not applicable		
DATA-02	Describe or provide a reference to how institution data is physically and logically separated from that of other customers.	Not applicable		
DATA-03	Will university data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	No		
DATA-04	Is sensitive data encrypted in transport?	Yes	Optional - Reference Technical document	Provide a detailed description.
DATA-05	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	Yes	Optional	Provide a detailed description.
DATA-06	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	No	Standard TLS Encryption	
DATA-07	Describe or provide a reference to the encryption technology and strategy you employ for transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN).	TLS and RTMPS		Include all types of encryption; remote-access, application/database, end-user-to-system, etc.
DATA-08	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	Not Applicable		
DATA-09	At the completion of this contract, will data be returned to the institution?	No	Not Applicable	Briefly explain why it won't be returned.
DATA-11	How long will the institution's data be available within the system at the completion of this contract?	Not Applicable		
DATA-12	Can the institution extract a full backup of data?	Yes		Describe frequency and procedures for obtaining a full backup of data.
DATA-13	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	Yes		
DATA-14	Are these rights retained even through a provider acquisition or bankruptcy event?	Yes		Provide a brief description.
DATA-15	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	No	Not Applicable	Provide a brief description.
DATA-16	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	Not Applicable		
DATA-17	Are backup copies made according to pre-defined schedules and securely stored and protected?	No	Not Applicable	
DATA-18	How long are data backups stored?	Not Applicable		
DATA-19	Are you encrypting your backups?	No	Not Applicable	Describe why backups are not encrypted.
DATA-21	Describe or provide a reference to your cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) of all system components (e.g. database, system, web, etc.).	Not applicable		
DATA-22	Do current backups include all operating system software, utilities, security software, application software and data files necessary for recovery?	No	Not Applicable	Provide a brief description.
DATA-23	Are you performing offsite backups? (i.e. digitally moved off site)		Not Applicable	
DATA-24	Are backups taken off site? (i.e. physically moved off site)		Not Applicable	

DATA-25	Do backups containing the institution's data ever leave the United States of America either physically or via network routing?		Not Applicable	
DATA-26	Describe or provide a reference to your media handing process, including end-of-life, repurposing, and data sanitization, that is documented and currently implemented.	Not applicable		
DATA-27	Does this process adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?		Not Applicable	
DATA-28	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?		Not Applicable	
DATA-29	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?		Not Applicable	
DATA-30	Will you handle data in a FERPA compliant manner?		Not Applicable	
DATA-31	Is any institution data visible in system administration modules/tools?		Not Applicable	
Database		**Vendor Answers**	**Additional Information**	**Guidance**
DBAS-01	Does the database support encryption of specified data elements in storage?	Yes	SHA-256	Describe the type of encryption that is supported.
DBAS-02	Do you currently use encryption in your database?	Yes	Passwords	Describe how encryption is leveraged.
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**
DCTR-01	Does your company own the physical data center where the institution's data will reside?	No	Section Not Applicable. University holds all data	Provide a detailed description of where university data will reside.
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?			
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (24x7)?			
DCTR-04	Do any of your servers reside in a co-located data center?			
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?			
DCTR-06	Does the physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?			
DCTR-07	Select the option that best describes the network segment that servers are connected to.			
DCTR-08	Does this data center operate outside of the United States?			
DCTR-09	Will any institution data leave the United States?			
DCTR-10	List all datacenters and their cities, states (provinces), and countries where the institution's data will be stored (including within the United States).			
DCTR-11	Are your primary and secondary data centers geographically diverse?			
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the United States?			
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?			
DCTR-14	Is the service hosted in a high availability environment?			
DCTR-15	Is redundant power available for all datacenters where institution data will reside?			
DCTR-16	How often are redundant power strategies tested?			
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.			
DCTR-18	State how many Internet service providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.			
DCTR-19	Does every datacenter where the institution's data will reside have multiple telephone company or network provider entrances to the facility?			
DRP - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan.	Section Not Applicable. Data stored within University environment		
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the Disaster Recovery Plan?			
DRPL-03	If possible, can the institution review your Disaster Recovery Plan(s) and supporting documentation?			
DRPL-04	Are any disaster recovery locations outside the United States?			
DRPL-05	Does your organization have a Disaster Recovery site or a contracted Disaster Recovery provider?			
DRPL-06	What type of availability does your Disaster Recovery site provide?			

DRPL-07	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?			
DRPL-08	Is there a defined problem/issue escalation plan in your DRP for impacted clients?			
DRPL-09	Is there a documented communication plan in your DRP for impacted clients?			
DRPL-10	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)			
DRPL-11	Indicate the last time that the Disaster Recovery Plan was tested and provide a summary of the results (including actual recovery time).			
DRPL-12	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?			
DRPL-13	Are all components of the Disaster Recovery Plan reviewed at least annually and updated as needed to reflect change?			
DRPL-14	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?			
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**	**Guidance**
FIDP-01	Are you utilizing a web application firewall (WAF)?		Section Not Applicable	
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?			
FIDP-03	State and describe who has the authority to change firewall rules?			
FIDP-04	Do you have a documented policy for firewall change requests?			
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?			
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?			
FIDP-07	Do you employ host-based intrusion detection?			
FIDP-08	Do you employ host-based intrusion prevention?			
FIDP-09	Describe or provide a reference to any other safeguards used to monitor for attacks?			
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?			
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?			
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and/or IPS?			
Mobile Applications - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
MAPP-01	On which mobile operating systems is your software or service supported?	Not Applicable		
MAPP-02	Describe or provide a reference to the application's architecture and functionality.			
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?			
MAPP-04	Does the application store, process, or transmit critical data?			
MAPP-05	Is institution data encrypted in transport?			
MAPP-05	Is institution data encrypted in storage? (e.g. disk encryption, at-rest)			
MAPP-06	Does the mobile application support Kerberos, CAS, or Active Directory authentication?			
MAPP-07	Will any of these systems be implemented on systems hosting the institution's data?			
MAPP-08	Does the application adhere to secure coding practices?			
MAPP-09	Has the application been tested for vulnerabilities by a third party?			
MAPP-10	State the party that performed the test and the date it was conducted?			
Physical Security		**Vendor Answers**	**Additional Information**	**Guidance**
PHYS-01	Describe or provide a reference to physical safeguards that are placed on facilities housing the institution's data (e.g., video monitoring, restricted access areas, man traps, card access controls, etc.)?	Section Not Applicable		
PHYS-02	Are employees allowed to take home customer data in any form?			
PHYS-03	Are video monitoring feeds retained?			
PHYS-04	Is the video feed monitored by data center staff?			
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?			

PHYS-06	What are the equipment removal procedures for the clients?			
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**	**Guidance**
PPPR-01	Briefly describe your security organization. Include the responsible party for your information security program and the size of your security staff?	Section is not applicable		
PPPR-02	Do you have a documented patch management process?	No		
PPPR-03	Can you accommodate encryption requirements using open standards?	Yes		
PPPR-04	Have your developers been trained in secure coding techniques?		Not Applicable	
PPPR-05	Was your application developed using secure coding techniques?		Not Applicable	
PPPR-06	Do you subject your code to Static Code Analysis and/or Static Application Security Testing prior to release? If so, what tool(s) do you use?"		Not Applicable	
PPPR-07	Describe testing processes that are established and followed (e.g., development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results)?	Not Applicable		
PPPR-08	Are information security principles designed into the product lifecycle?		Not Applicable	
PPPR-09	Do you have a documented systems development life cycle (SDLC)?		Not Applicable	
PPPR-10	Describe or provide a reference to your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).	Not Applicable		
PPPR-11	Do you have a formal incident response plan?		Not Applicable	
PPPR-12	Will you comply with applicable Breach Notification Laws?		Not Applicable	
PPPR-13	Will you comply with the institution's IT policies with regards to user privacy and data protection?		Not Applicable	
PPPR-14	Is your company subject to US laws and regulations?	Yes		
PPPR-15	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	No		
PPPR-16	Do you require new employees to fill out agreements and review policies?	No	Not Applicable - Our staff does not have access to your data	Provide a detailed summary.
PPPR-18	Do you have a documented information security policy?		Not Applicable - Our staff does not have access to your data	
PPPR-19	Do you have an information security awareness program?		Not Applicable - Our staff does not have access to your data	
PPPR-20	Is the security awareness training mandatory for all employees?		Not Applicable - Our staff does not have access to your data	
PPPR-21	How frequently are employees required to undergo the security awareness training?	Not Applicable - Our staff does not have access to your data		
PPPR-22	Is a process documented, and currently followed, that requires a review and update of the access-list for privileged accounts?		Not Applicable - Our staff does not have access to your data	
PPPR-23	Describe or provide a reference to your Internal Audit processes and procedures.			
Product Evaluation		**Vendor Answers**	**Additional Information**	**Guidance**
PROD-01	Do you incorporate customer feedback into security feature requests?	Yes	Email	Provide the appropriate method for submitting feature requests.
PROD-02	Can you provide an evaluation site to the institution for testing?	Yes		
Quality Assurance		**Vendor Answers**	**Additional Information**	**Guidance**
QLAS-01	Provide a general summary of your Quality Assurance program.	Quality Assurance program based on advising software updates, requesting periodic customer user feedback and acting on feedback		
QLAS-02	Do you comply with ISO 9001?	No		Describe plans and/or efforts towards certification.
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	No		
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?	Yes	Similar system installed in the Indiana University , School of Education, Center for Human Growth, Director: Lynn Gilman, Systems Admin Darrel Cooper. Value: $78,318.85	Provide the University contact, describe the products and/or services offered, and the total value of the services provided.
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	No		Describe plans and/or efforts towards certification.
Systems Management & Configuration		**Vendor Answers**	**Additional Information**	**Guidance**

SYST-01	Are systems that support this service managed via a separate management network?		Not Applicable	
SYST-02	Do you have an implemented system configuration management process? (i.e. secure "gold" images, etc.)	No		Describe how system configuration management is currently handled.
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?		Not applicable	
SYST-04	Provide a general summary of your systems management and configuration strategy, including servers, appliances, and mobile devices (company and employee owned).	Not applicable		
Vulnerability Scanning		**Vendor Answers**	**Additional Information**	**Guidance**
VULN-01	Are your *applications* scanned externally for vulnerabilities?		This entire section is not applicable as all data is stored in your systems.	
VULN-02	What was the date of your applications last external assessment? (mm/dd/yyyy)			
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?			
VULN-04	Are your *systems* scanned externally for vulnerabilities?			
VULN-05	What was the date of your systems last external assessment? (mm/dd/yyyy)			
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.			
VULN-07	Can we review the results of security scans?			
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).			
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?			
HIPAA - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	No		
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	No		
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	No		
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	No	See enclosed HITECH Statement	
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	No		
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?	No		
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?	No		
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	No	Controlled by University system administrators	
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?	No	Most Universities implement LDAP to align University login controls with the software	
HIPA-12	Does your application lock-out an account after a number of failed login attempts?	Yes	When LDAP is in use	Indicate the number of failed login attempts needed to lock-out an account.
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	Yes		Provide the default configuration details.
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	No		
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	Yes		Provide a brief description.
HIPA-16	Does your application provide the ability to define user access levels?	Yes		Provide documentation or a web resource.
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	Yes		Provide documentation or a web resource.
HIPA-18	Does your application support varying levels of access to records based on user ID?	Yes		
HIPA-19	Is there a limit to the number of groups a user can be assigned?	No		

HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	Yes		
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	Yes		
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	Yes		
HIPA-23	How long does the application keep access/change logs?	Indefinitely		
HIPA-24	Can the application logs be archived?	Yes		
HIPA-25	Can the application logs be saved externally?	Yes		
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?	No	Not Applicable	
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?		Not Applicable	
HIPA-28	Have the policies/plans mentioned above been tested?		Not Applicable	
HIPA-29	Can the application logs be saved externally?		Yes	
HIPA-30	Can you provide a HIPAA compliance attestation document?		Not Applicable	
HIPA-31	Are you willing to enter into a Business Associate Agreement (BAA)?	Yes		
HIPA-32	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	No	Not Applicable	
PCI DSS - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
PCID-01	Does your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?		Entire Section is Not Applicable	
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?			
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?			
PCID-04	Are you classified as a service provider?			
PCID-05	Are you on the list of VISA approved service providers?			
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?			
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.			
PCID-08	What payment processors/gateways does the system support?			
PCID-09	Can the application be installed in a PCI DSS compliant manner ?			
PCID-10	Is the application listed as an approved PA-DSS application?			
PCID-11	Does the systems or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?			
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.			