Higher Education Community Vendor Assessment Tool (HECVAT) - Full

HEISC Shared Assessments Working Group

DATE-01	**Date**	*1/25/2023*

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 (HECVAT). 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 through GNRL-08; populated by the Vendor

GNRL-01	Vendor Name	*Twenty Six Design LLC*
GNRL-02	Product Name	*WCONLINE*
GNRL-03	Product Description	*Scheduling, recordkeeping, and reporting program*
GNRL-04	Web Link to Product Privacy Notice	*https://www.26llc.com/doc_tos.php*
GNRL-05	Web Link to Accessibility Statement or VPAT	*26llc.com/doc_vpat.pdf*
GNRL-06	Vendor Contact Name	*Carla Hay*
GNRL-07	Vendor Contact Title	*Co-Owner*
GNRL-08	Vendor Contact Email	*carla@26llc.com* or *support@26llc.com*
GNRL-09	Vendor Contact Phone Number	*866-556-1743*
GNRL-10	Vendor Accessibility Contact Name	*Carla Hay*
GNRL-11	Vendor Accessibility Contact Title	*Co-Owner*
GNRL-12	Vendor Accessibility Contact Email	*carla@26llc.com*, *support@26llc.com*
GNRL-13	Vendor Accessibility Contact Phone Number	*866-556-1743*
GNRL-14	Vendor Hosting Regions	*USA and all other countries except Canada: USA; Canada: USA & Canada - We do not limit our services to regions within the United States, and our support team, including for Canadian clients, is located in the United States. For more information, see DATA-16, DCTR-02, or DRPL-04.*
GNRL-15	Vendor Work Locations	*USA*

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 Community Vendor Assessment Toolkit (HECVAT) to the Institution according to institutional procedures.

Qualifiers	Vendor Answers	Additional Information
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	The data that is collected within WCONLINE is defined by the administrator for a given WCONLINE account. This means that the site administrator has the ability to ask the questions that are needed while assuring compliance with local restrictions and recommendations. By default, WCONLINE does not request HIPAA or PHI data, and WCONLINE is used at academic support centers. Note that our infrastructure security is at the level needed for HIPAA and PHI data, but WCONLINE is intended to be used in academic centers that are not distributing information to students about health privacy or, typically, following specific HIPAA guidelines with staff.
QUAL-02	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	Per our Terms of Service, our support team uses your site and data only to provide support, such as by answering questions about your settings. We work with other companies, such as to audit our security and maintain the datacenter that we use. Access is given only at the level needed, and to appropriate employees or partners.
QUAL-03	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	Yes	We have business continuity plans, including executed agreements, but we do not share those with our clients.
QUAL-04	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	Yes	We have disaster recovery plans, including executed agreements, but do not share those with our clients.
QUAL-05	Is the vended product designed to process or store Credit Card information?	No	WCONLINE is used at academic support centers to collect data about students' appointments. It cannot process payments. Administrators may enter any questions they would like on their own forms, but we recommend not collecting credit card numbers, and we have never seen a center try to collect them using WCONLINE.
QUAL-06	Does your company provide professional services pertaining to this product?	No	We develop and support WCONLINE (and therefore provide professional product support), but we do not provide center management or tutoring services.
QUAL-07	Select your hosting option	7) Other	
Company Overview		**Vendor Answers**	**Additional Information**
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	WCONLINE was first developed about 25 years ago, and it has been developed with updates, mostly based on our clients' requests, over that time. It is used by thousands of writing, academic support, advising, disability, and testing centers across colleges, universities, and high schools in the United States, in Canada, and overseas. WCONLINE is a product of TWENTY SIX DESIGN LLC, which has more information at https://26llc.com. We have two owners and a support team all in the United States, and, because of the level of knowledge and collaboration that we insist upon for our staff, there is not a hierarchy of support levels and supervisors. Each of our support representatives can provide the same amount and level of support. We do not outsource support.	
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	No	
COMP-03	Do you have a dedicated Information Security staff or office?	Yes	Our information security personnel carry certifications from educational institutions and have product-specific training and certifications. We also partner with the firms that monitor and audit us for security. These are established, professional firms with staff members who have also undergone extensive training and testing, and that are proven leaders in security and network design, development and monitoring.

COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Yes	We maintain development teams that constantly work on and test new features or versions, and that respond to new recommendations (such as FERPA, security, or accessibility updates) and our clients' requests.
COMP-05	Use this area to share information about your environment that will assist those who are assessing your company data security program.	We perform testing, monitoring and in-house and contracted auditing, and we work proactively to determine whether updates need to be done. We respond quickly to any advisories or recommendations. We also back up data and sites continually and house WCONLINE only in Tier 4 datacenters, with our primary datacenter being the CH1 Digital Realty facility. A description of our infrastructure is included as the last page of this HECVAT.	
Documentation		**Vendor Answers**	**Additional Information**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?	No	Our network and applications are constantly monitored—both manually and via automatic protocols and processes—and are audited on a daily and weekly basis by two outside firms that perform multiple types of audits. While we do not fulfill requests for specific types of audits or provide the results of our audits, any security advisories—even recommendations—are responded to immediately. We also maintain logs and analyze and audit these logs.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	Yes	Similar to the answers here, in the list of questions, every answer is a "Yes" except for two that do not describe the way WCONLINE works. The only "no" is whether we force password changes on first login. Users are not given a password for their first login. And we can access WCONLINE on mobile devices, because it is a web-based program. Our VPN can be accessed only through specific computers.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	We do not always join groups or request certifications, especially when those would repeat work done by the firms that already audit our security.
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	Yes	We conform with multiple industry standard security frameworks.
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	No	Our security levels meet and exceed those listed in both (and, especially, in the extensive, detailed document provided under the NIST's information for NIST SP 800-171). However, we are not audited specifically for one of these two standards. Our audits are similarly thorough, but there is not a result stating that we are compliant with one of these specific standards. Additionally, in relation to CMMC Level 3 standards, we do not share some of the specific details of our security outside of our company.
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	While we do not provide full diagrams that would show our entire infrastructure to individuals or organizations outside of our company, a description of our infrastructure is included as the last page of this HECVAT, and its security mentioned in our Terms of Service. We can also help with support-related questions (such as about how backups work).
DOCU-07	Does your organization have a data privacy policy?	Yes	Our privacy policy is part of our Terms of Service, at https://www.26llc.com/doc_tos.php.
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes	Our policies include signing confidentiality and NDA agreements, addition or instant removal of access, automatic and personal monitoring, extensive training, alerts for multiple types of access, and more.
DOCU-09	Do you have a documented change management process?	Yes	Similar to the above, any change would include instant changes to access and continued confidentiality requirements. We have not had an actual change to management in many, many years.

DOCU-10	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	Yes	We maintain and update a VPAT that was last updated on October 5, 2022. Note that the VPAT does not discuss security, other than when confirming that individuals need to log in to access FERPA-protected data.
DOCU-11	Do you have documentation to support the accessibility features of your product?	Yes	Our VPAT is detailed and addresses specific accessibility requirements and recommendations. We also check for any needed changes and update WCONLINE as needed, even without a requirement to update the VPAT. We are also happy to respond to support emails asking questions about accessibility. Note that our VPAT and conversations about accessibility typically do not address security.
IT Accessibility		**Vendor Answers**	**Additional Information**
ITAC-01	Has a third party expert conducted an audit of the most recent version of your product?	Yes	We regularly audit internally, and we are also audited by outside firms. As with security, we do not provide results outside of our company, but we update immediately for any new requirements or issues.
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	Yes	In addition to testing and auditing, we track any new federal requirements and recommendations, and also take our clients' questions, requests, and suggestions, and work on them immediately.
ITAC-03	Have you adopted a technical or legal standard of conformance for the product in question?	Yes	We constantly ensure that we meet web requirements and guidelines (such as WCAG).
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	No	We do not use a roadmap; we update immediately when needed or begin working on updates if there is a non-urgent request that we can fulfill.
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	Yes	We review and discuss accessibility needs, work with the relevant areas of WCONLINE, review our own VPAT, and research the most up-to-date standards.
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Yes	As mentioned above in relation to a roadmap, we update immediately when needed, or begin working on updates if there is a non-urgent request that we can fulfill.
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes	Similar to the above, we work on accessibility updates right away.
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	Yes	
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a 'lite version' or accessing an alternate interface for accessibility purposes?	No	
Assessment of Third Parties		**Vendor Answers**	**Additional Information**

THRD-01	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	
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	We work with partner companies to handle our infrastructure, but there is no sharing of institutional data.	
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?	We have contracts regarding our equipment, service and support, privacy and security, NDA, etc.	
THRD-04	Do you have an implemented third party management strategy?	Yes	
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)	Yes	This is under multiple contracts, and both equipment and procedures are reviewed more than annually.
Consulting - Optional based on QUALIFIER response		**Vendor Answers**	**Additional Information**
CONS-01	Will the consulting take place on-premises?	No	We do not provide or use consulting services.
CONS-02	Will the consultant require access to Institution's network resources?	No	
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	No	
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	No	
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	No	
CONS-06	Will any data be transferred to the consultant's possession?	No	
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	No	
CONS-08	Will the consultant need remote access to the Institution's network or systems?	No	

CONS-09	Can we restrict that access based on source IP address?	No	
Application/Service Security		**Vendor Answers**	**Additional Information**
APPL-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	WCONLINE always includes access for full administrators, basic administrators, and non-administrators, so that each role at a center can access appropriate data and options.
APPL-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Yes	Within our company, employees access WCONLINE accounts only from company-owned and secured devices. All access is logged, monitored and audited and only takes place via Company-owned equipment. Database or server access is further secured via VPN access limited to specific devices and bio-based authentication. Each individual has access to only the data and areas they need to work with.
APPL-03	Does the system provide data input validation and error messages?	Yes	All data within WCONLINE is validated. (WCONLINE is not connected to university servers, so, other than pulling in one or two specific pieces of information that may be set by administrators, there is not validation in the sense of checking entered data against the university database.) WCONLINE, without exception, employs prepared statements for all database calls that are also validated independently. And the system is audited for injection vulnerabilities as part of the standard and continual security audits.
APPL-04	Are you using a web application firewall (WAF)?	Yes	Our infrastructure always includes a firewall. A description of our infrastructure is included as the last page of this HECVAT.
APPL-05	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Yes	We have a comprehensive and long-term list of every part of our infrastructure, and we revisit possible updates and replacements more than each year. All our systems are redundant and we have supplies above what we need.
APPL-06	Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?	Yes	All our systems are up-to-date; we would not use anything past its end of life.
APPL-07	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?	No	WCONLINE includes a mobile site that is part of the same program and that was developed only internally, just like the rest of WCONLINE. We do not offer an app.
APPL-08	Does your application require access to location or GPS data?	No	
APPL-09	Does your application provide separation of duties between security administration, system administration, and standard user functions?	Yes	Only our company can work on security, code, our infrastructure, etc. Standard user functions are accessed through WCONLINE by individuals who can log into their WCONLINE sites. There is no access for users (clients, center staff, administrators, etc.) to any of our infrastructure or programming.
APPL-10	Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?	Yes	Employees, including company owners, access our systems and programs using specific devices that can be locked, and every action related to WCONLINE (and our other products) is logged. Employees access WCONLINE accounts only from company-owned and secured devices with specific, tracked passwords. All access is logged, monitored and audited and only takes place via Company-owned equipment. (Database or server access is further secured via VPN access limited to specific devices and bio-based authentication.)
APPL-11	Have your developers been trained in secure coding techniques?	Yes	Since security is our highest priority, all development is done by individuals using secure coding techniques.
APPL-12	Was your application developed using secure coding techniques?	Yes	Since security is our highest priority, WCONLINE was developed, and continues to be updated, using secure coding techniques.

APPL-13	Do you subject your code to static code analysis and/or static application security testing prior to release?	Yes	As part of our security audits, existing and new code is tested for security.
APPL-14	Do you have software testing processes (dynamic or static) that are established and followed?	Yes	We test internally and are audited by outside firms, specifically for security.
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**
AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	3) Both modes available	WCONLINE includes built-in, optional SSO. For security, it allows authenticated clients, non-administrators, to log in, but administrators are required to log in on the WCONLINE login page.
AAAI-02	Does your solution support local authentication protocols for user and administrator authentication?	1) Yes	WCONLINE offers options to set up either SSO or LDAP/S. With LDAP/S, everyone logs in using their institutional username and password. With SSO, non-administrators log in on a page at the institution and are passed to WCONLINE logged-in.
AAAI-03	Can you enforce password/passphrase aging requirements?	Yes	For our support team and within our infrastructure, we use time-sensitive passwords and have passwords that expire and/or require additional authentication. In WCONLINE, administrators can choose to force profile updates.
AAAI-04	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Yes	Passwords must by default be at least ten characters. Administrators in WCONLINE may use built-in options to require that new registrations and profile updates use passwords that are ten characters including a symbol or ten characters including a symbol and a capital letter. With sites using LDAP or SSO, users log in using their university or college passwords, which are not stored in WCONLINE.
AAAI-05	Does the system have password complexity or length limitations and/or restrictions?	Yes	Passwords must be at least ten characters. Administrators can add requirements as described above. Our "Yes" response to the left means that WCONLINE does have an option to enforce password requirements; there is not a "limitation" on the actual security of passwords.
AAAI-06	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	Yes	Without LDAP/S or SSO, someone who has forgotten their password clicks to reset their password on the login page. They receive an email with a link that confirms that individual does want to change their password. Clicking the link allows them to create a new password. Our support team does not change or send passwords; instead, we instruct individuals to use the password reset. If an account-holder has extensive difficulty understanding the steps or is not able to receive emails, we may begin the password reset process for them. With LDAP or SSO, students and/or administrators would use the process in place at their institution.
AAAI-07	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	No	We are not members of specific organizations or programs that require payments that would result in a need to increase our subscription price. However, note that this question is usually asked in relation to setting up SSO, and SSO can be used at an institution using, for example, InCommon. While the bulk of our clients use WCONLINE by having students register directly on the site, WCONLINE supports LDAP and SSO, so that students can use their university usernames/email addresses and passwords. With LDAP, everyone logs in on the WCONLINE login page using their university username and password. With SSO, students (who are non-administrators) log in on a page such as a portal and are taken to WCONLINE already authenticated. SSO authentication to the university's servers so, it can be used with any existing authentication method.
AAAI-08	Does your application support integration with other authentication and authorization systems?	Yes	As described above, WCONLINE allows optional setup of SSO and LDAP/S. Since SSO offloads authentication to the institution, it can be used with any authentication method.

AAAI-09	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	Yes	As described above, WCONLINE allows optional setup of SSO. Since SSO offloads authentication to the institution, it can be used with any authentication method. There are no specific, special, different, or more detailed instructions or data needed to set up SSO with SAML or other methods.
AAAI-10	Do you support differentiation between email address and user identifier?	Yes	Within WCONLINE, individuals are identified by email address. If an institution chooses to use LDAP/S, individuals log in using their username instead of email address.
AAAI-11	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]	Yes	LDAP/S settings include eight OUs (with only one required), username, and email. SSO settings include an option to pull one piece of other data (such as a student's list of courses) onto the appointment form.
AAAI-12	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	While WCONLINE does support SSO, administrators always have the option to enable text messaging, add their cell phone number, and enable multi-factor authentication on their own logins.
AAAI-13	Does your application automatically lock the session or log-out an account after a period of inactivity?	Yes	Since WCONLINE is web-based and accessed through a website, individuals are timed out in a period depending on the browser and device.
AAAI-14	Are there any passwords/passphrases hard coded into your systems or products?	No	
AAAI-15	Are you storing any passwords in plaintext?	No	Passwords are encrypted with a salted hash, and AES-256 is included as one of the standards. Our support team uses time-sensitive passwords.
AAAI-16	Does your application support directory integration for user accounts?	No	With SSO or LDAP/S, the authentication method simply allows individuals to log in using their institutional credentials. SSO settings include an option to pull one piece of other data (such as a student's list of courses) onto the appointment form. (When this question is asked in relation to combining data from WCONLINE with institutional data, we recommend using one of the built-in exports and using email address as a key field.) When a center's or institution's need is to verify data, there are several ways to accomplish that. For example, without even using SSO or LDAP/S a WCONLINE full administrator can easily require valid institutional email addresses. And, WCONLINE does not have a reason to require all directory information, but administrators can choose which information they need from students.
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes	Within WCONLINE, administrators can see registrations, last logins, profile updates, which login made changes to specific areas (including the site's schedules, staff, administrators, clients, forms, and other options), emails that were sent, and clock-in and clock-out data, all with IP addresses, dates, times, and email addresses. Specific members of our support team can access more extensive logs. (We typically do not share all logs with our clients, because thousands of lines of logs are of normal actions, such as logging in, making an appointment, and logging out, and access to the data that an administrator needs is built in.)
AAAI-18	Describe or provide a reference to the a) system capability to log security/ authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.	We do not provide all the details of our logs, but the same information as above describes the logs that are available to administrators and mentions that we log all actions: Within WCONLINE, administrators can see registrations, last logins, profile updates, which login made changes to specific areas (including the site's schedules, staff, administrators, clients, forms, and other options), emails that were sent, and clock-in and clock-out data, all with IP addresses, dates, times, and email addresses. Specific members of our support team can access more extensive logs. (We typically do not share all logs with our clients, because thousands of lines of logs are of normal actions, such as logging in, making an appointment, and logging out, and access to the data that an administrator needs is built in.)	

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).	Most logs are available for as long as the customer is using WCONLINE until they cancel. We may retain logs for longer or not make all logs available outside of our company. Logs that are available to the customer are listed in Global System Settings and in the System Data Export, and these include most administrative changes that affect settings and data, such as changes to schedules, client deletions, and much more. Customers can also find other information within WCONLINE, such as information about when clients last logged in, who made appointments, when appointments were made and modified, when blackouts were created and who created them, who canceled appointments and when, etc.	
BCP - Respond to as many questions below as possible.		**Vendor Answers**	**Additional Information**
BCPL-01	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	Yes	More than only an individual company owner is responsible for our BCP.
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Yes	In the event that our business continuity plan is enacted, clients would be provided details regarding access to data and company communications.
BCPL-03	Is there a documented communication plan in your BCP for impacted clients?	Yes	We would share this if we ever had to enact it.
BCPL-04	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes	As with other areas of our work, we review this at least annually (usually before the fall semester) plus several other times during the year.
BCPL-05	Are specific crisis management roles and responsibilities defined and documented?	Yes	Similar to the above, we have specific roles for crisis management, but we do not share those outside of our company.
BCPL-06	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	Yes	Employees have specific, defined roles within the Company during periods of standard and emergency support.
BCPL-07	Does your organization have an alternative business site or a contracted Business Recovery provider?	Yes	This is part of our disaster recovery plan. And, we use primarily Digital Realty Tier 4 datacenters and would continue such use should a move to an alternative facility be necessary.
BCPL-08	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Yes	As with the above answer, we also test our BCP at least annually. We avoid reporting the date because these answers are not updated on the same schedule.
BCPL-09	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	Yes	In the event of an outage or catastrophic event, the Company would work to simultaneously restore access to all Company products and services equally without prioritizing a specific client above the others. Additionally, while we always recognize the need for our WCONLINE clients to have constant and fast access to their sites, our infrastructure uses several different technologies, and there would be a possibility of having another client up first only because no work was required to restore their access.
BCPL-10	Are all services that support your product fully redundant?	Yes	This is one of the features of our infrastructure.
Change Management		**Vendor Answers**	**Additional Information**
CHNG-01	Does your Change Management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?	Yes	Before even working on any update, we research and work through possible questions, and, before adding updates to WCONLINE sites, we test and check further. There is never a time that someone not authorized would have any ability to make or even work on a change or update.

CHNG-02	Does your Change Management process also verify that all required third party libraries and dependencies are still supported with each major change?	Yes	Everything within WCONLINE works in a single package. We do check, for example, that exports to Microsoft Excel work with current versions of Excel if we update the export function.
CHNG-03	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Yes	We update WCONLINE with new features approximately monthly. These updates may or may not include security updates. Security updates are done whenever needed, including more frequently than monthly if there are any advisories, recommendations, etc. Changes to the WCONLINE codebase or to the hosting infrastructure are applied by company staff via several custom solutions. Updates are researched and tested before being released. The top ten OWASP vulnerabilities are checked for both existing and new features, and we also test specifics related to features in WCONLINE. Note that we update quickly with no downtime and therefore do not always notify and do not have to obtain permission in advance. Our clients cannot reject or deny an update (but would be allowed to cancel if they found something objectionable). New options are added in their disabled or off position so that customers can choose to use them. We send an email once updates are complete to explain new features and make sure administrators know how to find them.
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	No	While some updates are minor tweaks, some are important for data security and to keep our technology up-to-date. Our policy is to not schedule or allow clients to deny updates. New features and options are added in their off or inactive positions, so clients are not requried to use new features or adjust for them, unless or until they are interested in using them.
CHNG-05	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?	Yes	As soon as we begin an update, all clients’ sites are updated within a short time, such as only one day. Our support team and infrastructure are fully capable of supporting both versions at once, but there is no need to regularly use concurrent versions.
CHNG-06	Does the system support client customizations from one release to another?	Yes	The options that are built into WCONLINE provide opportunities to completely customize nearly every aspect of the application--including the questions asked and the data collected within the program, and the features needed for a specific client. In the rare case where those control panels do not speak to a specific institutional need, WCONLINE staff will work with a client to offer advice or possibly provide additional customizations to the system. This is not entirely related to releases of new versions, because customizations either remain in place permanently or are turned into updates that are rolled out to everyone. A client would not lose their customizations or ability to implement their customizations.
CHNG-07	Do you have a release schedule for product updates?	No	We do not maintain a public schedule for updates but rather continually update the system--both for security and new features--as updates become desirable or necessary. This allows us to update more frequently, and for clients' convenience, than would be possible with a public release schedule.
CHNG-08	Do you have a technology roadmap, for at least the next 2 years, for enhancements and bug fixes for the product/service being assessed?	No	We do not maintain a roadmap. We work with our clients through a lot of discussion, and we have found that a roadmap frustrates and stresses a lot of people. When we are working on an update, we communicate about it with anyone who asks (or has recently asked) related questions, and we also communicate our willingness to incorporate suggestions and requests into upcoming updates. Bug fixes are done before a version or feature is released, and we have not had a bug on a production site. We may apply tweaks, such as when we find clients are using or understanding a feature differently, and such a small update could be considered a “fix” that is simply done within about 24 hours on all sites.

CHNG-09	Is Institution involvement (i.e. technically or organizationally) required during product updates?	No	As with installation and support, we handle all this support on our end.
CHNG-10	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	Yes	This would be similar to all other updates. We would apply the update and test it on an internal site, roll it out and test it on another internal site, and then roll it out to everyone and re-test and monitor it. This would be done more quickly—within only about a day or less—for a critical update, because we would stop other work to complete it and it would not take the same subjective testing that feature updates do.
CHNG-11	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	WCONLINE runs behind several F5 appliances that help mitigate security issues in real time. Security patches are applied in seconds after becoming available.
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Yes	WCONLINE updates and patches are applied in real time and without any noticeable effect on use. (For example, individual feature updates are completed nearly instantly with zero interruption to service, and a full version upgrade is completed in less than 20 seconds, with well under 20 seconds of interruption. Data and settings always remain in place.) If ever applicable, an example of an off-peak time would be 3 am Eastern time on the first Sunday after December 25.
CHNG-13	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	Yes	Changes cannot be applied without being documented, authorized, and logged.
CHNG-14	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	This is the same as CHNG-11. WCONLINE runs behind several F5 appliances that help mitigate security issues in real time. Security patches are applied in seconds after becoming available.
CHNG-15	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	Yes	All changes to the company's infrastructure or to the WCONLINE codebase and systems are peer reviewed before implementation, tested in a sandbox environment, and tested in a limited, live production environment before being rolled out to all clients. We continue to monitor all features in WCONLINE even after testing, both to be aware of any potential errors and to understand how our clients are using them. Internally, we maintain multiple test and update sites that would allow us to review old and new versions at once. Note that updates are only rolled out without bugs, so there would never be a time that we would offer to roll back a specific client's site.
CHNG-16	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	Yes	
Data		**Vendor Answers**	**Additional Information**
DATA-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	Data for each client is maintained in separate and separately-encrypted databases. No data is co-mingled between clients.
DATA-02	Will Institution's 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-03	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	Yes	Data is encrypted in transport/transit and at rest. SSL is provided and required on all WCONLINE sites.
DATA-04	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	Yes	Data is encrypted in transport/transit and at rest. Data is encrypted on a per instance bases with site-specific keys.
DATA-05	Do all cryptographic modules in use in your product conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	No	
DATA-06	At the completion of this contract, will data be returned to the institution and deleted from all your systems and archives?	No	This question is not applicable. Since WCONLINE is a web-based program (and we are providing SaaS), we never own our clients' data, and clients can always access, work with, and download all their data. When a client cancels and we close their site, their data is no longer accessible, because it is no longer online, and, on our end, we permanently and securely delete it. We describe cancelations in our information and in emails, as well as specifically to a client if they communicate with us before canceling, and we typically recommend running reports and saving them as pdfs, as well as using the built-in export to save data offline.
DATA-07	Will the institution's data be available within the system for a period of time at the completion of this contract?	No	If a client cancels a WCONLINE subscription, the site will be immediately inaccessible. Depending on communication from the client regarding cancelation, we typically (but are not requried to) recommend using the built in System Data Export to save data offline. And we may, but are not required to, retain data in backups for up to a year.
DATA-08	Can the Institution extract a full or partial backup of data?	Yes	As mentioned above, clients can use a built-in export to download all registration, appointment, client report, survey, time clock, and waiting list data into Excel files. We maintain backups that are full-image backups that can be applied to a site if needed (such as if an administrator deletes their data and wants it back). Our backups are not available to our clients, because they would not have a function outside of a WCONLINE site; however, if an institution would like to save data offline and would consider that a "backup," they may use the export anytime with no limitations on our end.
DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	Yes	Per our Terms of Service, your data belongs to you. Any research that you do with your data, center records within or outside of WCONLINE, etc. are yours.
DATA-10	Are these rights retained even through a provider acquisition or bankruptcy event?	Yes	There is never a situation in which we own your data.
DATA-11	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?	Yes	As legally and procedurally able, notice would be given of closures or other instances affecting WCONLINE access.
DATA-12	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Yes	WCONLINE data is backed up constantly in case there were some kind of natural disaster, fire, or entire datacenter loss. Data is also backed up daily and may be saved for up to a year. Backups are encrypted using site-specific keys and are saved securely as all data is.
DATA-13	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	Yes	Each client's files are backed up and saved together, so there are not separate files of data stored individually or mixed with other data.
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)	Yes	Backups are saved so that we could restore an individual's site from backup or coule use them to restore all sites to a point in time.
DATA-15	Are physical backups taken off site? (i.e. physically moved off site)	No	Our backups are off-site, but we do not move physical equipment, files, disks, etc. around, as there is no need to do so.

DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	Yes	We work with institutions throughout the United States and outside of the US. We do not keep data within specific regions of the US; for example, Southwest and Northeast states' data alike can be handled in the Midwest and in Florida. For Canadian institutions, we have long-term database storage in Canada. (Our support representatives are in the US and, our products all run from US datacenters.)
DATA-17	Are data backups encrypted?	Yes	All backups are encrypted using site-specific keys, and access to those backups is secured and logged.
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)	Yes	While we do not provide information on the specific encryption strategies employed within WCONLINE, backups are encrypted and stored securily both on-site and off-site.
DATA-19	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	When data is deleted, it is securely deleted using industry standard methods for FERPA-protected and other private data.
DATA-20	Does the process described in DATA-19 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	No	
DATA-21	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	Yes	Our entire infrastructure is highly secure, including all types of data that we save and use.
DATA-22	Will you handle data in a FERPA compliant manner?	Yes	WCONLINE is intended for use at academic support centers, so it has always been FERPA-compliant.
DATA-23	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) through any means?	Yes	Per our privacy policy, our support team members may access the data on your WCONLINE site for the purpose of providing support. A lot of centers collect PHI, such as students' majors, courses, other demographic information, and subjective notes on their appointments. We cannot access data outside of WCONLINE at the institution.
DATA-24	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	Within our company, employees access WCONLINE accounts only from company-owned and secured devices. All access is logged, monitored and audited and only takes place via Company-owned equipment. Database or server access is further secured via VPN access limited to specific devices and bio-based authentication. Each individual has access to only the data and areas they need to work with. We equip employees to work from home and, if ever needed, while traveling, securely using exactly the same systems.
Datacenter		**Vendor Answers**	**Additional Information**
DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?	No	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1. We do not provide any specific reports outside of our company.
DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?	No	We work with institutions throughout the United States and outside of the US. We do not keep data within specific regions of the US; for example, Southwest and Northeast states' data alike can be handled in the Midwest and in Florida. For Canadian institutions, we also use a datacenter in Canada. (Our support representatives are in the US and therefore may work with Canadian questions, answers, sites. and data in the US, too.)
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	Yes	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-04	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	Yes	Our servers are in locked cabinets that can be accessed only after multiple IDs (photo and fingerprint) are approved and multiple locks are unlocked.

DCTR-05	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	Yes	
DCTR-06	Are your primary and secondary data centers geographically diverse?	Yes	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-07	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	Other	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime Institute)?	Yes	The possible answers are only "yes" and "no." Our response is: Tier IV
DCTR-09	Is the service hosted in a high availability environment?	Yes	WCOLINE runs off of an infrasture that is designed as a high availability and highly redundant environment.
DCTR-10	Is redundant power available for all datacenters where institution data will reside?	Yes	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-11	Are redundant power strategies tested?	Yes	All datacenter-redundant systems are tested per Digital Realty testing requirements and schedules.
DCTR-12	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	Yes	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?	Tier IV	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-14	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	Tier IV	For information on our primary datacenter, visit https://www.dft.com/data-center/ch1
DCTR-15	Are you requiring multi-factor authentication for administrators of your cloud environment?	Tier IV	Yes
DCTR-16	Are you using your cloud providers available hardening tools or pre-hardened images?	Tier IV	
DCTR-17	Does your cloud vendor have access to your encryption keys?	No	We do not use a cloud vendor. And, there is no access given to our encryption keys outside of our company.
DRP - Respond to as many questions below as possible.		**Vendor Answers**	**Additional Information**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	We have disaster recovery and other plans, including executed agreements, but do not share these publicly. Even with a loss of an entire Tier 4 datacenter (something that would be near impossible), WCONLINE would continue to run with very little interruption. If our Terms of Service would be helpful, please see https://26llc.com/doc_tos.php.	
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Yes	More than only an individual company owner is responsible for our DRP.

DRPL-03	Can the Institution review your DRP and supporting documentation?	No	We do not share these specifics with our clients.
DRPL-04	Are any disaster recovery locations outside the Institution's geographic region?	Yes	We work with institutions throughout the United States and outside of the US. We do not keep data within specific regions of the US; for example, Southwest and Northeast states' data alike can be handled in the Midwest and in Florida. For Canadian institutions, we also use a datacenter in Canada. (Our support representatives are in the US and therefore may work with Canadian questions, answers, sites. and data in the US, too.)
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	Yes	We use primarily Digital Realty Tier 4 datacenters and would continue such use should a move to an alternative facility be necessary.
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	Yes	While the Company maintains a disaster recovery plan that includes the infrastructure and procedures necessary for a datacenter or corporate move, the actual move of data and infrastructure to an alternate datacenter is virtually tested, but not physically performed.
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	Yes	In the event that our disaster recovery plan is enacted, clients would be provided details regarding access to data (such as a timeline if we had to be down) and company communications.
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	Yes	While we do not share the details of our disaster recovery plan with our clients, we can easily communicate with all clients at once, as well as email and/or call individuals if needed, even without access to WCONLINE.
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	The Company's disaster recovery plan is periodically reviewed and tested, and employees are given specific, defined roles during such an emergency event.	
DRPL-10	Has the Disaster Recovery Plan been tested in the last year?	Yes	
DRPL-11	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes	Similar to DRPL-11 above, the plan is reviewed and tested frequently and if there are any updates to staff, technology, our infrastructure, equipment, etc.
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	As mentioned above: Our infrastructure employs several software and hardware security appliances, including F5 Big IP devices. A description of our infrastructure is included as the last page of this HECVAT.
FIDP-02	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info	Yes	Changes to any part of our infrastructure have to go through an approval and review process, and changes are documented both before and after taking place. For privacy, we do not provide names.
FIDP-03	Do you have a documented policy for firewall change requests?	Yes	Typically, both company owners discuss any changes with specific datacenter staff, and we work together on any updates.
FIDP-04	Have you implemented an Intrusion Detection System (network-based)?	Yes	Typically, both company owners discuss any changes with specific datacenter staff, and we work together on any updates.
FIDP-05	Have you implemented an Intrusion Prevention System (network-based)?	Yes	In addition to our F5s, we have multiple layers of security, including physical wires, that would detect attempts and prevent intrusion.

FIDP-06	Do you employ host-based intrusion detection?	Yes	In addition to our F5s, we have multiple layers of security, including physical wires, that would detect attempts and prevent intrusion.
FIDP-07	Do you employ host-based intrusion prevention?	Yes	In addition to our F5s, we have multiple layers of security, including physical wires, that would detect attempts and prevent intrusion.
FIDP-08	Are you employing any next-generation persistent threat (NGPT) monitoring?	Yes	In addition to our F5s, we have multiple layers of security, including physical wires, that would detect attempts and prevent intrusion.
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?	Yes	In addition to our F5s, we have multiple layers of security, including physical wires, that would detect attempts and prevent intrusion.
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?	Yes	Network and infrastructure are monitored both automatically and manually 24/7/365 by internal staff, a contracted auditing/security firm, and automatic logs and notifications.
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	Extensive logs are available to us internally. We do not share audit logs with our clients, but, if there are any recommendations or findings, we update immediately. We have never had an intrusion or breach.	
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Yes	Our network and applications are constantly monitored—both manually and via automatic protocols and processes—and are audited on a daily and weekly basis by two outside firms. While we do not provide the results of those audits, any security advisories—even recommendations—are responded to immediately. We also maintain logs and analyze and audit these logs. We perform testing, monitoring and in-house and contracted auditing, and we work proactively to determine whether updates need to be done. We respond quickly to any advisories or recommendations. We do not allow vulnerability or other security testing by our customers or IT or security departments on behalf of our customers.
PPPR-02	Do you have a documented patch management process?	Yes	As with security and other updates described elsewhere in this document, patches are peer reviewed, tested in a sandbox environment, and tested in a limited production environment before being rolled out to all clients.
PPPR-03	Can you accommodate encryption requirements using open standards?	Yes	
PPPR-04	Are information security principles designed into the product lifecycle?	Yes	WCONLINE does not have a product lifecycle in the sense of having the current version expire. Rather, the application is constantly updated for both feature and security needs.
PPPR-05	Do you have a documented systems development life cycle (SDLC)?	Yes	WCONLINE does not have a product lifecycle in the sense of having the current version expire. Rather, the application is constantly updated for both feature and security needs. Our infrastructure and programming behind the scenes are updated before any equipment or systems would reach their end of life, since this is necessary for security and speed. We have a schedule to routinely check our equipment and infrastructure for any needed updates.
PPPR-06	Do you have a formal incident response plan?	Yes	While we do not provide details outside of our company, we do have plans in place to handle security updates or other issues.
PPPR-07	Will you comply with applicable breach notification laws?	Yes	Our responsibilities related to a security breach are in described our Terms of Service at http://26llc.com/doc_tos.php.

PPPR-08	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	Yes	Our security policies are not university-specific. However, we can help centers with needs, such as adding information to the login page or registration form.
PPPR-09	Is your company subject to Institution's geographic region's laws and regulations?	No	We work with institutions throughout the United States and outside of the US. Since laws and regulations typically have to do with privacy and security, most, but not all, laws and regulations apply across all the areas we work with. However, we always comply with US federal laws and regulations and do not guarantee that we track or comply with others.
PPPR-10	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	Yes	Background checks are performed on our staff, but we do not provide results outside of our company. (To allow us to provide support efficiently, we request that customers not demand one specific support team member. For this and other reasons, we do not provide a lot of personal information about our staff.)
PPPR-11	Do you require new employees to fill out agreements and review policies?	Yes	We have multiple agreements to sign, as well as extensive training that includes knowledge and discussion of our policies. Employees review and execute specific security, non-disclosure, privacy, and other policy documents, and an employee handbook.
PPPR-12	Do you have a documented information security policy?	Yes	Please see our Terms of Service (http://26llc.com/doc_tos.php).
PPPR-13	Do you have an information security awareness program?	Yes	We do not have a labeled program, but we work constantly on knowledge of security policies, programming, etc., depending on staff members' positions.
PPPR-14	Is security awareness training mandatory for all employees?	Yes	We train and then frequently discuss FERPA, data privacy, and account privacy, and we discuss appropriate levels of how security works in our infrastructure and datacenters.
PPPR-15	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?	Yes	With all our employees working on company-owned hardware with unique and changing logins, we can instantly shut down any indivudal's access to support (such as the ability to log into any WCONLINE site) and computer. Any individual who should have temporary access has that access removed instantly, too. There is never a time we are not aware of who is accessing what.
PPPR-16	Do you have documented, and currently implemented, internal audit processes and procedures?	Yes	Our code and infrastructure are audited by professional outside firms. Internally, we research and test constantly, and we audit all informaiton, from accounts to infrastructure-level information.
PPPR-17	Does your organization have physical security controls and policies in place?	Yes	
Incident Handling		**Vendor Answers**	**Additional Information**
IH-01	Do you have a formal incident response plan?	Yes	While we do not provide details outside of our company, we do have plans in place to handle security updates or other issues.
IH-02	Do you have either an internal incident response team or retain an external team?	Yes	
IH-03	Do you have the capability to respond to incidents on a 24x7x365 basis?	Yes	
IH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes	Note that our coverage is for everything except an unforeseen outage. Our uptime is 99.999%, and, for most of our history, our outages have been for times such as two minutes. We would not reimburse institutions for outages, with or without insurance.

Quality Assurance		Vendor Answers	Additional Information
QLAS-01	Do you have a documented and currently implemented Quality Assurance program?	Yes	WCONLINE is continually tested and monitored, and changes (including updates) to the program are handled through a specific QA procedure. Similar to answers to earlier questions, all changes to the company's infrastructure or to the WCONLINE codebase and systems are peer reviewed before implementation, tested in a sandbox environment, and tested in a limited, live production environment before being rolled out to all clients. We continue to monitor all features in WCONLINE even after testing, both to be aware of any potential errors and to understand how our clients are using them.
QLAS-02	Do you comply with ISO 9001?	Yes	WCONLINE updates and changes are handled via a process that incorporates the recommendations made in ISO 9001.
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	While we do confirm that all the areas and features of WCONLINE are working properly, continue to report a 99.999% uptime, and confirm availability if someone has a question (even about their own internet connectivity), we do not provide reports or metrics to our clients.
QLAS-04	Do you incorporate customer feedback into security feature requests?	No	Most of our feature updates are based on requests; however, updates that are done for security are done without being influenced by customers, because doing so could mean backing off of security that we believe or learn should be implemented. We have never, and would never, release a version that had not already been tested for security; therefore, our customers do not find security issues.
QLAS-05	Can you provide an evaluation site to the institution for testing?	No	The institution is welcome to use the existing WCONLINE site or use our demo that is available to everyone. We do not set up extra sites only for testing of security or any other feature. Note that all quality/security testing is done on our end. An institution would not have to test for actual functionality of the product but would more likely want to "test" to make sure the features that they were interested in would work well for their students and staff.
Vulnerability Scanning		**Vendor Answers**	**Additional Information**
VULN-01	Are your systems and applications regularly scanned externally for vulnerabilities?	Yes	We work with specific outside firms to audit and test our security.
VULN-02	Have your systems and applications had a third party security assessment completed in the last year?	Yes	Our network and applications are constantly monitored—both manually and via automatic protocols and processes—and are audited on a daily and weekly basis by two outside firms. While we do not provide the results of those audits, any security advisories—even recommendations—are responded to immediately. We also maintain logs and analyze and audit these logs.
VULN-03	Are your systems and applications scanned with an authenticated user account for vulnerabilities [that are remediated] prior to new releases?	Yes	All updates are comprehensively tested for both functionality and security before being applied in production, and updates are never released with any issues in any area.
VULN-04	Will you provide results of application and system vulnerability scans to the Institution?	No	Any recommendations or advisories are acted upon immediately, but we do not report results—even the many extensive results of our systems, applications, and network being secure—outside of our company.
VULN-05	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.).	Yes	While we monitor agains common web application security vulnerabilities such as those mentioned and more, we do not report details outside of our company. As a summary, as mentioned above, our network and applications are constantly monitored—both manually and via automatic protocols and processes—and are audited on a daily and weekly basis by two outside firms. While we do not provide the results of those audits, any security advisories—even recommendations—are responded to immediately. We also maintain logs and analyze and audit these logs.

VULN-06	Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	No	Per our Terms of Service at http://26llc.com/doc_tos.php, we do not allow this type of testing. In brief, "testing" of our application or environment in order to evaluate our security or capacity would be considered "hacking" attempts and would result in termination of services and possible prosecution.
HIPAA - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	No	For HIPA-1 to 29, the entire HIPAA section does not apply to WCONLINE.
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	
HIPA-05	Have you conducted a risk analysis as required under the Security Rule?	No	
HIPA-06	Have you identified areas of risks?	No	
HIPA-07	Have you taken actions to mitigate the identified risks?	No	
HIPA-08	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	No	
HIPA-09	Does your application require a user to set their own password after an administrator reset or on first use of the account?	No	
HIPA-10	Does your application lock-out an account after a number of failed login attempts?	Yes	
HIPA-11	Does your application automatically lock or log-out an account after a period of inactivity?	Yes	
HIPA-12	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	No	
HIPA-13	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	No	
HIPA-14	Does your application provide the ability to define user access levels?	Yes	
HIPA-15	Does your application support varying levels of access to administrative tasks defined individually per user?	No	

HIPA-16	Does your application support varying levels of access to records based on user ID?	No	
HIPA-17	Is there a limit to the number of groups a user can be assigned?	No	
HIPA-18	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	No	(Where applicable, note that our support access is more heavily monitored than normal user access.)
HIPA-19	Does the application log record access including specific user, date/time of access, and originating IP or device?	Yes	
HIPA-20	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-21	How long does the application keep access/change logs?	Yes	
HIPA-22	Can the application logs be archived?	No	
HIPA-23	Can the application logs be saved externally?	Yes.	
HIPA-24	Does your data backup and retention policies and practices meet HIPAA requirements?	No	
HIPA-25	Do you have a disaster recovery plan and emergency mode operation plan?	Yes	
HIPA-26	Have the policies/plans mentioned above been tested?	Yes	
HIPA-27	Can you provide a HIPAA compliance attestation document?	No	
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?	No	
HIPA-29	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	No	
PCI DSS		**Vendor Answers**	**Additional Information**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/ credit/debt card) data?	No	For PCID-01 to 12, the entire PCI section does not apply to WCONLINE. (Our company does use a merchant processor, but that is totally unconnected to WCONLINE.)
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	No	
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	No	

PCID-04	Are you classified as a service provider?	No	
PCID-05	Are you on the list of VISA approved service providers?	No	
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	No	
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	N/A	
PCID-08	What payment processors/gateways does the system support?	N/A	
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	No	
PCID-10	Is the application listed as an approved PA-DSS application?	No	
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	No	
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.	N/A	

HECVAT - Full - Analyst Report

HEISC Shared Assessments Working Group

Instructions

Step 1: Select the security framework used at your institution in cell B10. **Step 2:** Convert qualitative vendor responses into quantitative values, starting at cell G37. **Step 3:** Review converted values, ensuring full population of report. **Step 4:** Move to the Summary Report tab.

Vendor Name	*Twenty Six Design LLC*	**Product Name**	WCONLINE
Vendor Contact Name	26llc.com/doc_vpat.pdf	**Product Description**	Scheduling, recordkeeping, and reporting program
Vendor Contact Title	Carla Hay	**HECVAT Version**	Full
Vendor Email Address	Co-Owner	**Date Prepared**	1/25/2023
Institution's Security Framework	**NIST SP 800-171r1**		

Report Sections	Max_Score	Score	Score %
Company	80	50	63%
Documentation	120	60	50%
Accessibility	180	140	78%
Third Parties	100	75	75%
Consulting	150	150	100%
Application Security	315	280	89%
Authentication, Authorization, and Accounting	445	255	57%
Business Contituity Plan	210	210	100%
Change Management	295	240	81%
Data	440	325	74%
Datacenter	100	60	60%
Disaster Recovery Plan	230	190	83%
Firewalls, IDS, IPS, and Networking	240	215	90%
Policies, Procedures, and Processes	315	290	92%
Incident Handling	45	45	100%
Quality Assurance	90	90	100%

		Vulnerability Scanning	130	80	62%		
		HIPAA	595	555	93%		
		PCI-DSS	220	170	77%		
		Overall Score	**4300**	**3480**	**81%**		

Override/Correct Vendor Responses and Set Weights Per Institution's Use Case				**Override/Correct Vendor Responses and Set Weights Per Institution's Use Case**			
ID	**Question**	**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
Company Overview		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
COMP-01	Describe your organization's business background and ownership structure, including all	WCONLINE was first developed about 25 years ago, and it has been developed with updates, mostly based on our clients'	Did not require additional information.	Yes		15	
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	No	Did not require additional information.	Yes	Yes	10	
COMP-03	Do you have a dedicated Information Security staff or office?	Yes	Our information security personnel carry certifications	Yes		15	
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support	Yes	We maintain development teams that constantly work	Yes		25	
COMP-05	Use this area to share information about your environment that will assist those who are	We perform testing, monitoring and in-house and contracted auditing, and we	Did not require additional information.	Yes		15	
Documentation		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?	No	Our network and applications are constantly monitored—both manually and via automatic	Yes		20	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	Yes	Similar to the answers here, in the list of questions, every answer is a	Yes		20	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	We do not always join groups or request certifications, especially when those would repeat	Yes		20	

DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001,	Yes	We conform with multiple industry standard security frameworks.	Yes		20		
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3	No	Our security levels meet and exceed those listed in both (and, especially, in the extensive,	Yes		20		
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	While we do not provide full diagrams that would show our entire infrastructure to individuals or organizations outside of our company, a	Yes		20		
DOCU-07	Does your organization have a data privacy policy?	Yes	Our privacy policy is part of our Terms of Service, at https://www.26llc.com/	Yes		20		
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes	Our policies include signing confidentiality and NDA agreements, addition or instant removal of	Yes		20		
DOCU-09	Do you have a documented change management process?	Yes	Similar to the above, any change would include instant changes to access	Yes		20		
DOCU-10	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	Yes	We maintain and update a VPAT that was last updated on October 5, 2022. Note that the VPAT	Yes		20		
DOCU-11	Do you have documentation to support the accessibility features of your	Yes	Our VPAT is detailed and addresses specific accessibility requirements and	Yes		0		
IT Accessibility		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**	

ITAC-01	Has a third party expert conducted an audit of the most recent version of your product?	Yes	We regularly audit internally, and we are also audited by outside firms. As with security, we do not provide results	Yes		20	
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	Yes	In addition to testing and auditing, we track any new federal requirements and recommendations, and also take our	Yes		20	
ITAC-03	Have you adopted a technical or legal standard of conformance for the product in question?	Yes	We constantly ensure that we meet web requirements and guidelines (such as WCAG).	Yes		20	
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	No	We do not use a roadmap; we update immediately when needed or begin working on updates if	Yes		20	
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	Yes	We review and discuss accessibility needs, work with the relevant areas of	Yes		20	
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Yes	As mentioned above in relation to a roadmap, we update immediately when needed, or begin working on updates if	Yes		20	
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes	Similar to the above, we work on accessibility updates right away.	No		20	
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	Yes	Did not require additional information.	Yes		20	
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a 'lite version' or accessing an alternate interface for accessibility purposes?	No	0	No		20	

Assessment of Third Parties		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override
THRD-01	Do you perform security assessments of third party companies with which you share data? (i.e. hosting	Yes	N/A	Yes		25	
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	We work with partner companies to handle our infrastructure, but there is	N/A	Yes	Yes	25	
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address	We have contracts regarding our equipment, service and support, privacy and security, NDA, etc.		Qualitative Question	Qualitative Question	25	
THRD-04	Do you have an implemented third party management strategy?	Yes	N/A	Yes		25	
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain?	Yes	N/A	No	No	25	
Consulting - Optional based on QUALIFIER response		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override
CONS-01	Will the consulting take place on-premises?	No	N/A	No	No	25	
CONS-02	Will the consultant require access to Institution's network resources?	No	N/A	No	No	20	
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	No	N/A	Yes	Yes	25	
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	No	N/A	No	No	20	
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	No	N/A	Yes	Yes	20	
CONS-06	Will any data be transferred to the consultant's possession?	No	N/A	No	No	25	
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	No	N/A	Yes	Yes	20	
CONS-08	Will the consultant need remote access to the Institution's network or systems?	No	N/A	Yes	Yes	25	
CONS-09	Can we restrict that access based on source IP address?	No	N/A	Yes	Yes	20	

Application/Service Security		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override
APPL-01	Are access controls for institutional accounts based on structured rules, such as role-based access	Yes	WCONLINE always includes access for full administrators,	Yes		25	
APPL-02	Are access controls for staff within your organization based on structured rules, such as	Yes	Within our company, employees access WCONLINE accounts	Yes		20	
APPL-03	Does the system provide data input validation and error messages?	Yes	All data within WCONLINE is validated.	Yes		20	
APPL-04	Are you using a web application firewall (WAF)?	Yes	Our infrastructure always includes a firewall. A description	Yes		25	
APPL-05	Do you have a process and implemented procedures for managing your software supply chain (e.g.	Yes	We have a comprehensive and long-term list of	Yes		20	
APPL-06	Are only currently supported operating system(s), software, and libraries leveraged by the	Yes	All our systems are up-to-date; we would not use anything past	No		25	
APPL-07	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?	No	WCONLINE includes a mobile site that is part of the same	Yes	Yes	15	
APPL-08	Does your application require access to location or GPS data?	No	Did not require additional information.	No		25	
APPL-09	Does your application provide separation of duties between security administration, system	Yes	Only our company can work on security, code, our	Yes		40	
APPL-10	Do you have a fully implemented policy or procedure that details how your employees obtain	Yes	Employees, including company owners, access our systems	No		10	
APPL-11	Have your developers been trained in secure coding techniques?	Yes	Since security is our highest priority, all development is done	Yes		20	
APPL-12	Was your application developed using secure coding techniques?	Yes	Since security is our highest priority, WCONLINE was	Yes		20	
APPL-13	Do you subject your code to static code analysis and/or static application security testing prior to	Yes	As part of our security audits, existing and new	Yes		25	
APPL-14	Do you have software testing processes (dynamic or static) that are established and	Yes	We test internally and are audited by outside firms,	Yes		25	
Authentication, Authorizati		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override

AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator	3) Both modes available	WCONLINE includes built-in, optional SSO. For security, it	Yes	Yes	25		
AAAI-02	Does your solution support local authentication protocols for user and administrator	1) Yes	WCONLINE offers options to set up either SSO or LDAP/	Yes	Yes	25		
AAAI-03	Can you enforce password/passphrase aging requirements?	Yes	For our support team and within our infrastructure, we	Yes		20		1
AAAI-04	Can you enforce password/passphrase complexity requirements [provided by the	Yes	Passwords must by default be at least ten characters.	No		40		
AAAI-05	Does the system have password complexity or length limitations and/or restrictions?	Yes	Passwords must be at least ten characters.	No	No	40		
AAAI-06	Do you have documented password/passphrase reset procedures that are currently implemented in	Yes	Without LDAP/S or SSO, someone who has forgotten their	Yes		25		
AAAI-07	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	No	We are not members of specific organizations or	Yes		40		
AAAI-08	Does your application support integration with other authentication and authorization systems?	Yes	As described above, WCONLINE allows optional setup of SSO	Yes		20		
AAAI-09	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect	Yes	As described above, WCONLINE allows optional setup of	No		15		
AAAI-10	Do you support differentiation between email address and user identifier?	Yes	Within WCONLINE, individuals are identified by email	Yes		15		
AAAI-11	Do you allow the customer to specify attribute mappings for any needed information beyond a user	Yes	LDAP/S settings include eight OUs (with only one	No		20		
AAAI-12	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor	Yes	While WCONLINE does support SSO, administrators always	No	Yes	15		
AAAI-13	Does your application automatically lock the session or log-out an account after a period of	Yes	Since WCONLINE is web-based and accessed through a	Yes		15		
AAAI-14	Are there any passwords/passphrases hard coded into your systems or products?	No	Did not require additional information.	No		25		
AAAI-15	Are you storing any passwords in plaintext?	No	Passwords are encrypted with a salted hash, and	Yes		25		
AAAI-16	Does your application support directory integration for user accounts?	No	With SSO or LDAP/S, the authentication method simply allows	Yes	Yes	20		

AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed	Yes	Within WCONLINE, administrators can see registrations, last	Yes		25	
AAAI-18	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes		**Qualitative Question**	**Qualitative Question**	25	
AAAI-19	Describe or provide a reference to the a) system capability to log security/ authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.	We do not provide all the details of our logs, but the same information as above describes the logs that are available to administrators and mentions that we log all actions: Within WCONLINE, administrators can see registrations, last logins, profile updates, which login made changes to specific areas (including the site's schedules, staff, administrators, clients, forms, and other options), emails that were sent, and clock-in and clock-out data, all with IP addresses, dates, times, and email addresses. Specific members of our support team can access more extensive logs. (We typically do not share all logs with our clients, because thousands of lines of logs are of normal actions, such as logging in, making an appointment, and logging out, and access to the data that an administrator needs is built in.)		**Qualitative Question**	**Qualitative Question**	25	
BCP - Respond to as		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
BCPL-01	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity	Yes	More than only an individual company owner is responsible	Yes		20	
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Yes	In the event that our business continuity plan is enacted,	Yes		20	
BCPL-03	Is there a documented communication plan in your BCP for impacted clients?	Yes	We would share this if we ever had to enact it.	Yes		25	
BCPL-04	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes	As with other areas of our work, we review this at least	Yes		25	
BCPL-05	Are specific crisis management roles and responsibilities defined and documented?	Yes	Similar to the above, we have specific roles for crisis	Yes		20	

BCPL-06	Does your organization conduct training and awareness activities to validate its employees	Yes	Employees have specific, defined roles within the Company	Yes		20	
BCPL-07	Does your organization have an alternative business site or a contracted Business	Yes	This is part of our disaster recovery plan. And, we use	Yes		20	
BCPL-08	Does your organization conduct an annual test of relocating to an alternate site for business recovery	Yes	As with the above answer, we also test our BCP at least	Yes		20	
BCPL-09	Is this product a core service of your organization, and as such, the top priority during	Yes	In the event of an outage or catastrophic event,	Yes		15	
BCPL-10	Are all services that support your product fully redundant?	Yes	This is one of the features of our infrastructure.	Yes		25	
Change Management		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
CHNG-01	Does your Change Management process minimally include authorization, impact	Yes	Before even working on any update, we research and work	Yes		20	
CHNG-02	Does your Change Management process also verify that all required third party libraries and	Yes		**Qualitative Question**		20	
CHNG-03	Will the institution be notified of major changes to your environment that could impact the	Yes	We update WCONLINE with new features	Yes		25	
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	No	While some updates are minor tweaks, some are important	Yes		10	
CHNG-05	Do you have a fully implemented solution support strategy that defines how many	Yes		**Qualitative Question**		15	
CHNG-06	Does the system support client customizations from one release to another?	Yes		**Qualitative Question**		25	
CHNG-07	Do you have a release schedule for product updates?	No		**Qualitative Question**		15	
CHNG-08	Do you have a technology roadmap, for at least the next 2 years, for enhancements and bug	No	We do not maintain a roadmap. We work with our clients	Yes		15	
CHNG-09	Is Institution involvement (i.e. technically or organizationally) required during product updates?	No	As with installation and support, we handle all this	Yes		15	
CHNG-10	Do you have policy and procedure, currently implemented, managing how critical patches are	Yes	This would be similar to all other updates. We would apply the	Yes		20	

CHNG-11	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated	Yes	WCONLINE runs behind several F5 appliances that help	Yes		20		
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a manner that does not	Yes	WCONLINE updates and patches are applied in real time	Yes		15		
CHNG-13	Do procedures exist to provide that emergency changes are documented and authorized (including	Yes	Changes cannot be applied without being documented,	Yes		15		
CHNG-14	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated	Yes	This is the same as CHNG-11. WCONLINE runs behind several	Yes		25		
CHNG-15	Do you have an implemented system configuration management process? (e.g. secure	Yes	All changes to the company's infrastructure or to	Yes				
CHNG-16	Do you have a systems management and configuration strategy that encompasses servers	Yes	Did not require additional information.	Yes				
Data		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**	
DATA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your	Yes	Data for each client is maintained in separate and	No	No	15		
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...)	No	Did not require additional information.	No		25		
DATA-03	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-	Yes	Data is encrypted in transport/transit and at rest. SSL is	Yes		40		
DATA-04	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk	Yes	Data is encrypted in transport/transit and at rest. Data is	Yes		25		
DATA-05	Do all cryptographic modules in use in your product conform to the Federal Information	No	Did not require additional information.	Yes		25		
DATA-06	At the completion of this contract, will data be returned to the institution and deleted from all your	No	This question is not applicable. Since WCONLINE is a web-	Yes	No	20		
DATA-07	Will the institution's data be available within the system for a period of time at the completion of this	No	If a client cancels a WCONLINE subscription, the site	Qualitative Question	Qualitative Question	25		
DATA-08	Can the Institution extract a full or partial backup of data?	Yes	As mentioned above, clients can use a built-in export to	Yes		20		
DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	Yes	Per our Terms of Service, your data belongs to you. Any	Yes		15		

DATA-10	Are these rights retained even through a provider acquisition or bankruptcy event?	Yes	There is never a situation in which we own your data.	Yes		25	
DATA-11	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide	Yes	As legally and procedurally able, notice would be given	Yes		0	
DATA-12	Are involatile backup copies made according to pre-defined schedules and securely stored and	Yes	WCONLINE data is backed up constantly in case there were	Yes		15	
DATA-13	Do current backups include all operating system software, utilities, security software	Yes	Each client's files are backed up and saved together, so there are	Yes		20	
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)	Yes		**Qualitative Question**	**Qualitative Question**	20	
DATA-15	Are physical backups taken off site? (i.e. physically moved off site)	No	Did not require additional information.	Yes	Yes	20	
DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or	Yes		**Qualitative Question**	**Qualitative Question**	25	
DATA-17	Are data backups encrypted?	Yes	All backups are encrypted using site-specific keys, and	Yes		15	
DATA-18	Do you have a cryptographic key management process (generation, exchange	Yes	While we do not provide information on the specific	Yes		10	
DATA-19	Do you have a media handling process, that is documented and currently implemented that meets	Yes	When data is deleted, it is securely deleted using industry	Yes		20	
DATA-20	Does the process described in DATA-19 adhere to DoD 5220.22-M and/or NIST SP 800-88	No	Did not require additional information.	No		20	
DATA-21	Is media used for long-term retention of business data and archival purposes stored in a secure,	Yes	Our entire infrastructure is highly secure,	Yes		25	
DATA-22	Will you handle data in a FERPA compliant manner?	Yes	WCONLINE is intended for use at academic support	Yes		15	
DATA-23	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other	Yes	Per our privacy policy, our support team members may	Yes		20	
DATA-24	Do you have a documented and currently implemented strategy for securing employee	Yes	Within our company, employees access WCONLINE accounts	Yes		20	
Datacenter		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**

DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?	No	For information on our primary datacenter, visit	Yes		20	
DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?	No	We work with institutions throughout the	Yes	Yes	20	
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	Yes	For information on our primary datacenter, visit	No	No	20	
DCTR-04	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	Yes	Our servers are in locked cabinets that can be accessed only	Yes		20	
DCTR-05	Does a physical barrier fully enclose the physical space preventing unauthorized physical	Yes	Did not require additional information.	Yes		25	
DCTR-06	Are your primary and secondary data centers geographically diverse?	Yes	For information on our primary datacenter, visit	Yes		20	
DCTR-07	If outsourced or co-located, is there a contract in place to prevent data from leaving the	Other		Qualitative Question	Qualitative Question	20	
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime Institute)?	Yes	The possible answers are only "yes" and "no." Our response	Yes	Yes	20	
DCTR-09	Is the service hosted in a high availability environment?	Yes	WCOLINE runs off of an infrasture that is designed as a high	Yes		20	
DCTR-10	Is redundant power available for all datacenters where institution data will reside?	Yes		Qualitative Question	Qualitative Question	20	
DCTR-11	Are redundant power strategies tested?	Yes	All datacenter-redundant systems are tested per Digital	Yes		25	
DCTR-12	Describe or provide a reference to the availability of cooling and fire suppression systems in	Yes	For information on our primary datacenter, visit	Yes		20	
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?	Tier IV	For information on our primary datacenter, visit	Yes	Yes	20	
DCTR-14	Does every datacenter where the Institution's data will reside have multiple telephone	Tier IV	For information on our primary datacenter, visit	Yes	Yes	20	
DCTR-15	Are you requiring multi-factor authentication for administrators of your cloud environment?	Tier IV	Yes	Yes	Yes	20	
DCTR-16	Are you using your cloud providers available hardening tools or pre-hardened images?	Tier IV	Did not require additional information.	Yes	Yes	20	

DCTR-17	Does your cloud vendor have access to your encryption keys?	No	We do not use a cloud vendor. And, there is no access	No		20		
DRP - Respond to as many questions below as possible.		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**	
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	We have disaster recovery and other plans, including executed agreements, but	We have disaster recovery and other plans, including	Yes		20		
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Yes	More than only an individual company owner is responsible	Yes		15		
DRPL-03	Can the Institution review your DRP and supporting documentation?	No	We do not share these specifics with our clients.	No		25		
DRPL-04	Are any disaster recovery locations outside the Institution's geographic region?	Yes	We work with institutions throughout the	Yes		20		
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery	Yes	We use primarily Digital Realty Tier 4 datacenters and	Yes		20		
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery	Yes	While the Company maintains a disaster recovery plan that	Yes		20		
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	Yes	In the event that our disaster recovery plan is enacted,	Yes		20		
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	Yes	While we do not share the details of our disaster recovery	Yes		20		
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR	The Company's disaster recovery plan is periodically reviewed and tested, and	Did not require additional information.	Yes		20		
DRPL-10	Has the Disaster Recovery Plan been tested in the last year?	Yes	Did not require additional information.	Yes		25		
DRPL-11	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes	Similar to DRPL-11 above, the plan is reviewed and tested	Yes		25		
Firewalls, IDS, IPS, and		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**	
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	As mentioned above: Our infrastructure employs several	Yes		25		
FIDP-02	Is authority for firewall change approval documented? Please list approver names or titles in	Yes	Changes to any part of our infrastructure have to go through	Yes		20		

FIDP-03	Do you have a documented policy for firewall change requests?	Yes		Qualitative Question		25	
FIDP-04	Have you implemented an Intrusion Detection System (network-based)?	Yes	Typically, both company owners discuss any changes	Yes		25	
FIDP-05	Have you implemented an Intrusion Prevention System (network-based)?	Yes	In addition to our F5s, we have multiple layers of	Yes		20	
FIDP-06	Do you employ host-based intrusion detection?	Yes	In addition to our F5s, we have multiple layers of	Yes		25	
FIDP-07	Do you employ host-based intrusion prevention?	Yes	In addition to our F5s, we have multiple layers of	Yes		20	
FIDP-08	Are you employing any next-generation persistent threat (NGPT) monitoring?	Yes	In addition to our F5s, we have multiple layers of	Yes		20	
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?	Yes	In addition to our F5s, we have multiple layers of	Yes		15	
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?	Yes	Network and infrastructure are monitored both	Yes		20	
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	Extensive logs are available to us internally. We do not share audit logs with our	Did not require additional information.	Yes		25	
Policies, Procedures, and Processes		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security	Yes	Our network and applications are constantly monitored	Yes		20	
PPPR-02	Do you have a documented patch management process?	Yes	As with security and other updates described elsewhere	Yes		25	
PPPR-03	Can you accommodate encryption requirements using open standards?	Yes	Did not require additional information.	Yes		20	
PPPR-04	Are information security principles designed into the product lifecycle?	Yes	WCONLINE does not have a product lifecycle in the sense	Yes		15	
PPPR-05	Do you have a documented systems development life cycle (SDLC)?	Yes	WCONLINE does not have a product lifecycle in the sense	Yes		20	
PPPR-06	Do you have a formal incident response plan?	Yes	While we do not provide details outside of our	Yes		15	

PPPR-07	Will you comply with applicable breach notification laws?	Yes	Our responsibilities related to a security breach are in	Yes		15	
PPPR-08	Will you comply with the Institution's IT policies with regards to user privacy and data	Yes	Our security policies are not university-specific. However, we	Yes		25	
PPPR-09	Is your company subject to Institution's geographic region's laws and regulations?	No	We work with institutions throughout the	Yes		25	
PPPR-10	Do you perform background screenings or multi-state background checks on all employees	Yes	Background checks are performed on our staff, but we do not	Yes		20	
PPPR-11	Do you require new employees to fill out agreements and review policies?	Yes	We have multiple agreements to sign, as well as extensive	Yes		20	
PPPR-12	Do you have a documented information security policy?	Yes	Please see our Terms of Service (http://26llc.com/	Yes		20	
PPPR-13	Do you have an information security awareness program?	Yes	We do not have a labeled program, but we work constantly	Yes		15	
PPPR-14	Is security awareness training mandatory for all employees?	Yes	We train and then frequently discuss FERPA, data privacy,	Yes		15	
PPPR-15	Do you have process and procedure(s) documented, and currently followed, that require a review and	Yes	With all our employees working on company-owned	Yes		15	
PPPR-16	Do you have documented, and currently implemented, internal audit processes and	Yes	Our code and infrastructure are audited by	Yes		15	
PPPR-17	Does your organization have physical security controls and policies in place?	Yes	Did not require additional information.	Yes		15	
Incident Handling		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
IH-01	Do you have a formal incident response plan?	Yes	While we do not provide details outside of our	Yes		15	
IH-02	Do you have either an internal incident response team or retain an external team?	Yes	Did not require additional information.	Yes		15	
IH-03	Do you have the capability to respond to incidents on a 24x7x365 basis?	Yes	Did not require additional information.	Yes		15	
IH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost	Yes	Note that our coverage is for everything except an	Yes		0	

Quality Assurance		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override
QLAS-01	Do you have a documented and currently implemented Quality Assurance program?	Yes		Qualitative Question		10	
QLAS-02	Do you comply with ISO 9001?	Yes	WCONLINE updates and changes are handled via a process	Yes		15	
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and	No	While we do confirm that all the areas and features of	Yes	Yes	20	
QLAS-04	Do you incorporate customer feedback into security feature requests?	No	Most of our feature updates are based on requests; however,	Yes	Yes	25	
QLAS-05	Can you provide an evaluation site to the institution for testing?	No	The institution is welcome to use the existing WCONLINE	Yes	Yes	20	
Vulnerability Scanning		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override
VULN-01	Are your systems and applications regularly scanned externally for vulnerabilities?	Yes	We work with specific outside firms to audit and test our security.	Yes		15	
VULN-02	Have your systems and applications had a third party security assessment completed in the last year?	Yes	Our network and applications are constantly monitored	Yes		20	
VULN-03	Are your systems and applications scanned with an authenticated user account for vulnerabilities	Yes	All updates are comprehensively tested for both	Yes		25	
VULN-04	Will you provide results of application and system vulnerability scans to the Institution?	No	Any recommendations or advisories are acted	Yes		25	
VULN-05	Describe or provide a reference to how you monitor for and protect against common web	Yes	While we monitor agains common web application security	Yes		20	
VULN-06	Will you allow the institution to perform its own vulnerability testing and/or scanning of your	No	Per our Terms of Service at http://26llc.com/	Yes		25	
HIPAA - Optional based on		Vendor Answer	Additional Information	Preferred Response	Compliant Override	Default Weight	Weight Override
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and	No	For HIPA-1 to 29, the entire HIPAA section does not apply to	Yes	Yes	25	
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	No	N/A	Yes	Yes	20	

HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	No	N/A	Yes	Yes	20		
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical	No	N/A	Yes	Yes	20		
HIPA-05	Have you conducted a risk analysis as required under the Security Rule?	No	N/A	Yes	Yes	20		
HIPA-06	Have you identified areas of risks?	No	N/A	Yes	Yes	25		
HIPA-07	Have you taken actions to mitigate the identified risks?	No	N/A	Yes	Yes	20		
HIPA-08	Does your application require user and system administrator password changes at a frequency no	No	N/A	Yes	Yes	20		
HIPA-09	Does your application require a user to set their own password after an administrator reset or on	No	N/A	Yes	Yes	20		
HIPA-10	Does your application lock-out an account after a number of failed login attempts?	Yes	Did not require additional information.	Yes	Yes	20		
HIPA-11	Does your application automatically lock or log-out an account after a period of inactivity?	Yes	Did not require additional information.	No	Yes	20		
HIPA-12	Are passwords visible in plain text, whether when stored or entered, including service level	No	N/A	Yes	Yes	20		
HIPA-13	If the application is institution-hosted, can all service level and administrative account	No	N/A	Yes	Yes	20		
HIPA-14	Does your application provide the ability to define user access levels?	Yes	Did not require additional information.	Yes	Yes	20		
HIPA-15	Does your application support varying levels of access to administrative tasks defined individually	No	N/A	Yes	Yes	20		
HIPA-16	Does your application support varying levels of access to records based on user ID?	No	N/A	No	Yes	20		
HIPA-17	Is there a limit to the number of groups a user can be assigned?	No	N/A	Yes	Yes	20		
HIPA-18	Do accounts used for vendor supplied remote support abide by the same authentication policies and	No	(Where applicable, note that our support access is more	Yes	Yes	20		

HIPA-19	Does the application log record access including specific user, date/time of access, and originating IP	Yes	Did not require additional information.	Yes	Yes	20		
HIPA-20	Does the application log administrative activity, such user account access changes and password	Yes	Did not require additional information.	Yes	Yes	20		
HIPA-21	How long does the application keep access/ change logs?	Yes	Did not require additional information.	Yes	Yes	20		
HIPA-22	Can the application logs be archived?	No	N/A	Yes	Yes	20		
HIPA-23	Can the application logs be saved externally?	Yes.	Did not require additional information.	Yes	Yes	20		
HIPA-24	Does your data backup and retention policies and practices meet HIPAA requirements?	No	N/A	Yes	Yes	15		
HIPA-25	Do you have a disaster recovery plan and emergency mode operation plan?	Yes	Did not require additional information.	Yes	Yes	20		
HIPA-26	Have the policies/plans mentioned above been tested?	Yes	N/A	Yes	Yes	25		
HIPA-27	Can you provide a HIPAA compliance attestation document?	No	N/A	Yes	Yes	20		
HIPA-28	Are you willing to enter into a Business Associate Agreement (BAA)?	No	N/A	Yes	Yes	20		
HIPA-29	Have you entered into a BAA with all subcontractors who may have access to protected	No	N/A	Yes	Yes	25		
PCI DSS		**Vendor Answer**	**Additional Information**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**	
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt	No	For PCID-01 to 12, the entire PCI section does not apply to	Yes	Yes	20		
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	No	N/A	Yes	Yes	20		

PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	No	N/A	Yes	Yes	25		
PCID-04	Are you classified as a service provider?	No	N/A	Yes	Yes	20		
PCID-05	Are you on the list of VISA approved service providers?	No	N/A	Yes	Yes	20		
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	No		Qualitative Question	Yes	20		
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	N/A		Qualitative Question	Yes	10		
PCID-08	What payment processors/ gateways does the system support?	N/A		Qualitative Question	Yes	10		
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	No	N/A	Yes	Yes	10		
PCID-10	Is the application listed as an approved PA-DSS application?	No	N/A	No	Yes	25		
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	No	N/A	No	Yes	25		
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	N/A		Qualitative Question	Yes	15		