HECVAT - Full | Vendor Response

Vendor Response

DATE-01	**Date**	*4/14/2023*

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	*Six Deg INC*
GNRL-02	Product Name	*Yellowdig Engage*
GNRL-03	Product Description	*Social learning software as a service platform*
GNRL-04	Web Link to Product Privacy Notice	https://yellowdig.co
GNRL-05	Web Link to Accessibility Statement or VPAT	*TODO*
GNRL-06	Vendor Contact Name	*Brian Hurlow*
GNRL-07	Vendor Contact Title	*V.P. Technology*
GNRL-08	Vendor Contact Email	brian@yellowdig.com
GNRL-09	Vendor Contact Phone Number	*(206) 661-8858*
GNRL-10	Vendor Accessibility Contact Name	*Brian Hurlow*
GNRL-11	Vendor Accessibility Contact Title	*V.P. Technology*
GNRL-12	Vendor Accessibility Contact Email	brian@yellowdig.com
GNRL-13	Vendor Accessibility Contact Phone Number	*(206) 661-8858*
GNRL-14	Vendor Hosting Regions	*United States*
GNRL-15	Vendor Work Locations	*United States, India, Nicaragua*

Instructions

Step 1: Complete the *Qualifiers* section first; responses in this section drive dictate question response requirements throughout the HECVAT Full.
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	
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	Institution data is stored in our AWS region (us-west-2)
QUAL-03	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	Yes	https://drive.google.com/file/d/1JceHLtZVCyWMx-uyvvQ5ibSnzefMjn18/view?usp=share_link
QUAL-04	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	Yes	https://drive.google.com/file/d/1JceHLtZVCyWMx-uyvvQ5ibSnzefMjn18/view?usp=share_link
QUAL-05	Is the vended product designed to process or store Credit Card information?	No	
QUAL-06	Does your company provide professional services pertaining to this product?	No	
QUAL-07	Select your hosting option	4) AWS	

Company Overview		Vendor Answers	Additional Information

COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	Yellowdig is a US C-Corp incorporated in Delaware, US, with headquarters in Philadelphia, PA. The company is privately owned by employees and venture capital investors. The company does not have any subsidiaries	
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	Information Security is managed as a sub-team within Yellowdig development team organization. Dedicated developers own security domains alongside backend development work. Multitple multiple development team individuals own security domains
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Yes	Yellowdig primary team pillars are: Development, Academic Partnerships, Customer Success and Business Development
COMP-05	Use this area to share information about your environment that will assist those who are assessing your company data security program.	Yellowdig is implemented as a multi-tenant cloud application which emphasizes learner engagement. From a technical standpoint the design is similar to social media application and includes user profiles, content authoring, social interaction and content discovery. Yellowdig Engage was made specifically for education use cases	
Documentation		**Vendor Answers**	**Additional Information**
DOCU-01	Have you undergone a SSAE 18/SOC 2 audit?	No	Yellowdig plans to achieve SOC 2 audit certification. We are actively tracking progress towards compliance, audit timeframe is TBD
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	No	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	Yes	Yellowdig currently tracks security according to the CIS controls framework
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	No	
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?	Yes	https://drive.google.com/drive/folders/1iH7lckd6eYDWo4ld15e5dhxcG1LzyQvF?usp=sharing
DOCU-07	Does your organization have a data privacy policy?	Yes	https://drive.google.com/file/d/1mPqN39weXMyc3VVgsDzgLQ6US_5OCiX-/view?usp=sharing
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes	https://drive.google.com/file/d/1BbOztQd-J_5IY_I9JGiWyd1I6jFMiks8/view?usp=share_link
DOCU-09	Do you have a documented change management process?	No	Change management is covered as part of Yellowdig's larger software development process, which emphasizes continuous integration and automation https://drive.google.com/file/d/1OwRKXM5uFlt8Gkx3OITBrz_dOCc8D5t9/view?usp=share_link
DOCU-10	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	No	An updated VPAT is planned for 2023 but incomplete
DOCU-11	Do you have documentation to support the accessibility features of your product?	No	Updated accessibility documentation is pending
IT Accessibility		**Vendor Answers**	**Additional Information**
ITAC-01	Has a third party expert conducted an audit of the most recent version of your product?	No	
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	No	Accessibility is integrated into the development process but pending additional documentation
ITAC-03	Have you adopted a technical or legal standard of conformance for the product in question?	Yes	WCAG 2.0

ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	No	
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	Yes	Yellowdig's development team considers accessibility concerns in code review and in process. Yellowdig's frontend engineers generate storybook components which include automated accessibility scanning of HTML. UI components are maintained that consider screen reader, tab navigation and color contrast. Developers routinely use screen readers to assess application usability
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Yes	Yellowdig maintains an internal tracker of accessibility coverage. In certain cases the Yellowdig team will disucss issues directly with customers and end-users, implement changes and follow up for feedback
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes	
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	No	Certain administrative functionality requires some mouse interaction. Keyboard-only navigation is maintained for non-admin primary usage (e.g. the main community posting and feed interface)
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	Yellowdig uses only industry standard third party technology tools and services to assist in operational areas. No institution data or PII is shared with third parties. Adoption of third pary services is subject to an internal review process which involves requesting of audit information and risk analysis
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	Yellowdig does not share institution data with third parties. Various forms of application metadata (not PII) is shared to external services (Datadog, Launchdarkly) to enable operation and software maintenance as needed by the Development team	
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?	All third parties in use have liability caluses in their standard agreements which address data breach	
THRD-04	Do you have an implemented third party management strategy?	No	
THRD-05	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)	No	Yellowdig is a SAAS product which is exclusively delivered as a cloud application. Therefore there is limited hardware used by our team outside of company workstations which are managed via an MDM solution
Consulting		**Vendor Answers**	**Additional Information**
CONS-01	Will the consulting take place on-premises?		
CONS-02	Will the consultant require access to Institution's network resources?		
CONS-03	Will the consultant require access to hardware in the Institution's data centers?		
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?		
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?		
CONS-06	Will any data be transferred to the consultant's possession?		
CONS-07	Is it encrypted (at rest) while in the consultant's possession?		
CONS-08	Will the consultant need remote access to the Institution's network or systems?		
CONS-09	Can we restrict that access based on source IP address?		
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	Information is restricted based on user role and access level, e.g. learner, instructor, community administrators, network administrators. Access roles are inherited from the Learning Management System pass via secured channel (LTI/Oauth). Access follows a hierarchical design that maps to the institutions organizational structure
APPL-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Yes	
APPL-03	Does the system provide data input validation and error messages?	Yes	Inputs are validated on both the client and server, with associated error messaging
APPL-04	Are you using a web application firewall (WAF)?	No	Adopting a WAF is part of Yellowdig's long term security roadmap and likely will be automated inside our AWS deployment
APPL-05	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Yes	Docker image layers are scanned as part of our CI/CD deployment workflow with identified CVEs blocking deployment. Similar automated analysis tools are used for dependent libraries and frameworks
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	Standard java ecosystem packages are used and kept up to date. Libraries in use are: Jetty, Java 11, Datomic (database vendor), AWS sdks. These depenencies are routinely updated. A full list of dependent software can be generated on request
APPL-07	If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?	N/A	
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	
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	Yellowdig employees in non-techinical roles are required to access administrative functionality via the web application and is thus subject to RBAC. Account owners are granted access to only the institution "networks" within Yellowdig to which they are assigned. Developer access is brokered via
APPL-11	Have your developers been trained in secure coding techniques?	Yes	OWASP, group discussions, code review
APPL-12	Was your application developed using secure coding techniques?	Yes	Specific design considerations were made to enhance security including: defence against SQL injection (we don't use SQL), tiered deployment architecture, audit-logging built in to the design
APPL-13	Do you subject your code to static code analysis and/or static application security testing prior to release?	Yes	Docker image layer scanning is run on each deployment. Application code itself is not yet subject to static testing
APPL-14	Do you have software testing processes (dynamic or static) that are established and followed?	Yes	Automated unit and integration tests are run as part of the CI/CD delivery pipeline
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**
AAAI-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	1) Yes	SAML authentication is supported
AAAI-02	Does your solution support local authentication protocols for user and administrator authentication?	3) Both modes available	
AAAI-03	Can you enforce password/passphrase aging requirements?	No	Password aging is not yet implemented

AAAI-04	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Yes	Yellowdig uses Dropbox's zxcvbn standard for enforcing password complexity. It may be customized on request https://github.com/dropbox/zxcvbn
AAAI-05	Does the system have password complexity or length limitations and/or restrictions?	Yes	See AAAI-04
AAAI-06	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	Yes	Password reset requests from the customer support team are processed by the development team and follow an automation playbook
AAAI-07	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	No	There are no plans in place to adopt either standard at this time
AAAI-08	Does your application support integration with other authentication and authorization systems?	No	Yellowdig plans to support Google authentication
AAAI-09	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	Yes	SAML authentication is supported, OIDC is used in the LTI 1.3 integrations but not outside of
AAAI-10	Do you support differentiation between email address and user identifier?	Yes	
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	User attributes can be customized in SSO and LTI integration configuration
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.)		
AAAI-13	Does your application automatically lock the session or log-out an account after a period of inactivity?	Yes	Session are invalidated after a specified window regardless of activity
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 using the Bcrypt algorithm with an additional salt
AAAI-16	Does your application support directory integration for user accounts?	No	
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes	Yellowdig's audit logging includes all database transactions and accessed data reports. Additional scope is planned
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.	Yellowdig audit logging for read data is implemented as an event stream. Application operations enqueue event data on an audit stream and the stream is automated to sink data into an Elasticsearch cluster which support filtration of audit events on multiple facets. Write based audit logging is implemented as metadata on all database transactions using Datomic, which is an append-only system and supports tagging of all transactions with additional details. No data deletion is implemented in the application, only append (like Git) operations	
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).	Audit events are stored in elasticsearch in monthly index patterns and retained for 12 months. Logs are protected by the AWS managed elasticsearch service which supports disc encryption and access restrictions. An export of log events can be prepared on-demand for customers as needed	
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	BCP is the responsibility of the security sub-team
BCPL-02	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Yes	
BCPL-03	Is there a documented communication plan in your BCP for impacted clients?	Yes	
BCPL-04	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes	
BCPL-05	Are specific crisis management roles and responsibilities defined and documented?	Yes	
BCPL-06	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	No	
BCPL-07	Does your organization have an alternative business site or a contracted Business Recovery provider?	Yes	All us operations are in us-west-2 with failover strategy that targets us-east-1 backup region

BCPL-08	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Yes	BCP is tested annually as part of a game-day exercise
BCPL-09	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	Yes	The core web application interface and supporting backends is considered in the BCP
BCPL-10	Are all services that support your product fully redundant?	Yes	Yellowdig deploys HA failovers of main database transaction process and ships replicas of all services. Backup regional deployments are used where applicable
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	Yellowdig follows a continuous integration (CI/CD) change strategy which minimizes risk. All changes introduced to the service go through a staged process which includes validation testing, automated testing, security analysis, and signed authorization via branch protections
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	Libraries and dependencies are maintained to their latest versions, including the primary database library, routinely as part of regular workflows
CHNG-03	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Yes	Any such notifications would be broadcast via existing communication channels for stakeholders (university contact list, security breach notification list, status/uptime availability list)
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	Yes	Client functionality may be brokered via our feature flagging system
CHNG-05	Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?	Yes	
CHNG-06	Does the system support client customizations from one release to another?	Yes	Client customizations are maintained as customization built into the product, which is not changed between releases
CHNG-07	Do you have a release schedule for product updates?	Yes	Yellowdig releases small, validated, minimal fixes every day
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?	Yes	May be provided upon request
CHNG-09	Is Institution involvement (i.e. technically or organizationally) required during product updates?	No	
CHNG-10	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	Yes	Critical patches are applied via deployment automation and may be expedited using explicitely granted branch overrides
CHNG-11	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	
CHNG-12	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Yes	Releases are automated to minimize customer disruption
CHNG-13	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	Yes	
CHNG-14	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	Yes	System configuration is reviewed and managed like regular code changes (git ops)
CHNG-15	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	Yes	Primarily managed as a cloud automation task, emphasizing infrastructure as code
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).	No	Yellowdig is a multi-tenant design with logical separations implemented in application code. Logical separation integrity is analyzed during penetration testing
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-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-05	Do all cryptographic modules in use in your product conform to the Federal Information Processing Standards (FIPS PUB 140-3)?	No	
DATA-06	At the completion of this contract, will data be returned to the institution and deleted from all your systems and archives?	Yes	Data is purged within 90 days of customer activity and an archive is delivered to the customer
DATA-07	Will the institution's data be available within the system for a period of time at the completion of this contract?	Yes	90 days
DATA-08	Can the Institution extract a full or partial backup of data?	Yes	Upon request and in a variety of formats depending on the data source
DATA-09	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	Yes	
DATA-10	Are these rights retained even through a provider acquisition or bankruptcy event?	Yes	
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	Yellowdig selects and maintains primary IT contacts for each customer. These contacts will be used to notify about data release
DATA-12	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Yes	Database backup is automated
DATA-13	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	Yes	Yellowdig's infrastructure is infrastructure is described in Docker image files and infrastructure as code and thus may be rebuilt on demand without special files
DATA-14	Are you performing off site backups? (i.e. digitally moved off site)	Yes	Offsite backups occur annually where data stores are exported to local storage media and stored securely
DATA-15	Are physical backups taken off site? (i.e. physically moved off site)	No	Not applicable
DATA-16	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	No	Backups remain in the regional cloud instance
DATA-17	Are data backups encrypted?	Yes	AWS managed encryption of the zipped backup archives
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	For employee key distribution, public/private PGP keys are used. Application secret values are stored in the AWS secrets manager and provided to applications via IAM permissions which are distinct from employee permissions. SSL certificates are also managed exclusively inside AWS and are not permitted to leave the platform
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?	No	
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	Media, for Yellowdig namely post attachments and uploaded content, remains in the cloud account. If/when archived, it's moved into parallel resources in the cloud
DATA-22	Will you handle data in a FERPA compliant manner?	Yes	
DATA-23	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) through any means?	No	Yellowdig receives only profile level information per user. Users create additional data within the platform, but the platform itself does not depend on Institutional data sources
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)	No	Yellowdig is in the process of procuring a MDM solution
Datacenter		**Vendor Answers**	**Additional Information**

DCTR-01	Does the hosting provider have a SOC 2 Type 2 report available?		
DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?	Yes	Yellowdig supports replication to alternative AWS regions as a contract enhancement. By default US customers are deployed to the us-west-2 datacenter. Yellowdig's Australian customers access an alternative deployment in ap-southeast-2
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?		
DCTR-04	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?		
DCTR-05	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?		
DCTR-06	Are your primary and secondary data centers geographically diverse?	Yes	Primary: us-east-2, secondary: us-east-1
DCTR-07	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	No	
DCTR-08	What Tier Level is your data center (per levels defined by the Uptime Institute)?		
DCTR-09	Is the service hosted in a high availability environment?	Yes	
DCTR-10	Is redundant power available for all datacenters where institution data will reside?		
DCTR-11	Are redundant power strategies tested?		
DCTR-12	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.		
DCTR-13	Do you have Internet Service Provider (ISP) Redundancy?		
DCTR-14	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?		
DCTR-15	Are you requiring multi-factor authentication for administrators of your cloud environment?	Yes	User accounts for the AWS cloud environment are provisioned with an MFA requirement in place. Yellowdig employees may select their MFA type upon first login, usually authenticator app
DCTR-16	Are you using your cloud providers available hardening tools or pre-hardened images?	Yes	
DCTR-17	Does your cloud vendor have access to your encryption keys?	Yes	Since Yellowdig stores certain keys in the AWS secrets manager, they techinically have access to them
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).	https://drive.google.com/file/d/1JceHLtZVCyWMx-uyvvQ5ibSnzefMjn18/view?usp=share_link	
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Yes	BCP and DRP are assigned to the Yellowdig Security sub-team
DRPL-03	Can the Institution review your DRP and supporting documentation?	Yes	Linked in DRLP-01
DRPL-04	Are any disaster recovery locations outside the Institution's geographic region?	No	Yellowdig's recovery plan targets the us-east-1 datacenter for US customers
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	Yes	The recovery site is a backup cloud region
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	Yes	Continuity playbooks are tested annually as part of a "game day" exercise
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	No	
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	Yes	
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.)	An annual test day is scheduled when the backend team dedicates the workday to invoking the process described in DRPL-10 and assessing the correctness and completeness of the automation and timing which components of the system become available	

DRPL-10	Has the Disaster Recovery Plan been tested in the last year?	Yes	Yellowdigs regional failover recovery automation entails running a set of Pulumi (https://www.pulumi.com) described stacks which boot up networking, EKS clusters, lambda functions etc. Provisioning of the EKS cluster is the most time consuming step in the stack as virtual servers take some time to boot. Last test run completed in about 5 hours
DRPL-11	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes	
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**
FIDP-01	Are you utilizing a stateful packet inspection (SPI) firewall?	No	
FIDP-02	Is authority for firewall change approval documented? Please list approver names or titles in Additional Info	Yes	Due to infrastructure-as-code model, network related changes require code review from security team members and are subject to associated merge restrictions. Jem, Brian and Xander on the YD team are marked as code onwners of this domain
FIDP-03	Do you have a documented policy for firewall change requests?	Yes	FIDP-02 describes, firewall changes are seldom necessary in our latest infrastructure design
FIDP-04	Have you implemented an Intrusion Detection System (network-based)?	Yes	Datadog Cloud Workload Security
FIDP-05	Have you implemented an Intrusion Prevention System (network-based)?	No	
FIDP-06	Do you employ host-based intrusion detection?	Yes	Since Yellowdig's primary applications run in a Kubernetes cluster via EKS, the "host" is an EC2 instance which is running one or more docker containers. Intrusion detection is implemented to detect unrecognized or abnormal command invocation via a linux kernel extension
FIDP-07	Do you employ host-based intrusion prevention?		
FIDP-08	Are you employing any next-generation persistent threat (NGPT) monitoring?		
FIDP-09	Do you monitor for intrusions on a 24x7x365 basis?	Yes	Intrusion detection is connected to an on-call rotation in Pagerduty
FIDP-10	Is intrusion monitoring performed internally or by a third-party service?	Yes	Third party service
FIDP-11	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	Yes	AWS maintains configuration change logs
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?	No	Yellowdig's security program is operated as as sub-team within the larger development team. This sub-team consist of three individual developers: Jem McElwain, Alexander Goldman and Brian Hurlow who shape the security roadmap and integrate security tasks into development sprints
PPPR-02	Do you have a documented patch management process?	Yes	
PPPR-03	Can you accommodate encryption requirements using open standards?	Yes	
PPPR-04	Are information security principles designed into the product lifecycle?	Yes	Security voices are included when making product design decisions
PPPR-05	Do you have a documented systems development life cycle (SDLC)?	Yes	https://drive.google.com/file/d/1OwRKXM5uFlt8Gkx3OITBrz_dOCc8D5t9/view?usp=share_link
PPPR-06	Will you comply with applicable breach notification laws?	Yes	
PPPR-07	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	Yes	
PPPR-08	Is your company subject to Institution's geographic region's laws and regulations?	Yes	
PPPR-09	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	Yes	
PPPR-10	Do you require new employees to fill out agreements and review policies?	Yes	

PPPR-11	Do you have a documented information security policy?	No	This is covered partially by other policies
PPPR-12	Do you have an information security awareness program?	Yes	Security awareness training is managed via https://www.curricula.com and required by all employees to complete annually
PPPR-13	Is security awareness training mandatory for all employees?	Yes	
PPPR-14	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	Privledged accounts include developer profiles for accessing infrastructure, and application accounts which administer multiple institutions. Developer accounts follow a key rotation and git-ops management policy. Application accounts are reviewed semi-annually and purged when needed
PPPR-15	Do you have documented, and currently implemented, internal audit processes and procedures?	No	
PPPR-16	Does your organization have physical security controls and policies in place?	No	
Incident Handling		**Vendor Answers**	**Additional Information**
HFIH-01	Do you have a formal incident response plan?	Yes	https://drive.google.com/file/d/1BHjfpYX9l1vQOazGhuejyvPkJE38JHgy/view?usp=share_link
HFIH-02	Do you have either an internal incident response team or retain an external team?	Yes	Internal response team
HFIH-03	Do you have the capability to respond to incidents on a 24x7x365 basis?	Yes	
HFIH-04	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes	
Quality Assurance		**Vendor Answers**	**Additional Information**
QLAS-01	Do you have a documented and currently implemented Quality Assurance program?	Yes	
QLAS-02	Do you comply with ISO 9001?	No	
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?	Yes	
QLAS-04	Do you incorporate customer feedback into security feature requests?	Yes	
QLAS-05	Can you provide an evaluation site to the institution for testing?	Yes	Evaluation sandboxes are offered as scratch networks in the production deployment and can be used to test out a variety of functionality including optional flagged features
Vulnerability Scanning		**Vendor Answers**	**Additional Information**
VULN-01	Are your systems and applications regularly scanned externally for vulnerabilities?	Yes	Yellowdig underlying systems are scanned for vulnerabilities via Docker image scanning supported by ECR, which runs any time a Docker image layer has been changed in the CI pipeline. Yellowdig's application undergoes annually recurring penetration tests by our partners at https://www.cobalt.io
VULN-02	Have your systems and applications had a third party security assessment completed in the last year?	Yes	2022 penetration test results may be found here: https://drive.google.com/drive/folders/1D8RFQl-ejiJTgNsUvOHHiV_qHiDbsBIx?usp=share_link
VULN-03	Are your systems and applications scanned with an authenticated user account for vulnerabilities [that are remediated] prior to new releases?	No	Yellowdig does not yet implement automated vulnerability scanning of application code, though there are automated unit tests which assess permissions in API code which are run with each build
VULN-04	Will you provide results of application and system vulnerability scans to the Institution?	Yes	

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	Yellowdig considers OWASP level risks during all parts of the software development process. Initially this takes place in code review where reviewers are trained to look for common security oversights. SQL injection is addressed primarily by not using SQL at all, but also by ensuring that any database values are correctly santized when rendered (though almost all rendering is managed by react.js). Additional XSS protection is implemented by requiring authenticity tokens to be submitted along with application data
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?	Yes	This can be arranged on request. Additional deployments would need to be set up to ensure no disruption to production