Student Information Security

Family Educational Rights & Privacy ACT (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a Federal Law designed to protect the privacy of a student's education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student, or former student, who has reached the age of 18 or is attending any school beyond the high school level. Students and former students to whom the rights have transferred are called eligible students.

- Parents or eligible students have the right to inspect and review all the student's education records maintained by the school. Schools are not required to provide copies of materials in education records unless, for reasons such as great distance, it is impossible for parents or eligible students to inspect the records. Schools may charge a fee for copies.

- Parents and eligible students have the right to request that a school correct record believed to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record commenting on the contested information in the record.

- Generally, schools must have written permission from the parent or eligible student before releasing any information from a student's record. However, the law allows schools to disclose records, without consent, to the following parties:

    - School employees who have a need to know
    - Other schools to which a student is transferring
    - Certain government officials to carry out lawful functions
    - Appropriate parties in connection with financial aid to a student
    - Organizations conducting certain studies for the school
    - Accrediting organizations
    - Individuals who have obtained court order or subpoenas
    - Persons who need to know in cases of health and safety emergencies, and state and local authorities within a juvenile justice system, pursuant to specific state law.

Schools may also disclose, without consent, "directory" type information such as student's name address, telephone
number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose "directory" information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information or technical assistance, you may call (202) 260-3887 (voice). Individuals who use TDD may call the Federal Information Relay Service at 1-800-877-8339.

Or you may contact the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-5901

File Location

Students' records are kept electronically hosted by Microsoft Azure. Each financial aid officer has own username and password to access the student record. Students' academic information are kept in the "College Office" software. Business office uses QuickBooks Software on a campus server.

Back up.
All systems are backed up to ensure no data will be lost. The data is backed up every night and kept in 2 different locations. The data preserved for 45 days.
Security

- Weber & Associates, Inc. FERPA and PII Security Statement Appendix B
- College Office Security Appendix C
- Campus Ivy Information System Data Security Plan Appendix D

The Campus Ivy team maintains all student records associated with Student financial aid awards in electronic format in hosted by Microsoft Azure in the Cloud and are backed to secure locations. Student Files are password protected and made available 24/7/365.
These records include:

- An Institutional Student Information Record (ISIR)
- Application data submitted to the Department of Education
- Entrance Counseling
- Copies of any verification or comment code resolution documents.
- Citizenship documentation, if used for "C" code resolution
- Proof of High School Graduation, if used for conflict info resolution or part of verification process.
- The amount of the grant and loan; its payment period; its loan period, if appropriate; and the calculations used to determine the amount of grant or loan.
- Loan origination record, including the amount of the loan and the period of enrollment.
  The MDT Financial Aid office:
- Backup of any documentation submitted to VFAO/Campus Ivy system
- The cost of attendance, estimated financial assistance, and expected family contribution used to calculate the loan amount (and any other information that may be required to determine the borrower's eligibility, such as the student's Federal Pell Grant eligibility or ineligibility).
- The amount, date, and basis of the school's calculation of any refunds/returns or overpayments due to or on behalf of the student- an R2T4 form
- The payment of any refund/return or overpayment to the FSA program fund, a lender, or the Department, as appropriate.
- Exit loan counseling

The ATS Registrar office is responsible for maintaining all admission and academic records. These records are kept in "College Office" and include:

- Enrollment agreement
- Attendance
- Grades
- Transcripts
- Standards of Academic Progress
- Leave of Absence Records
- Special Appeals Circumstances

The ATS business office is responsible for maintaining student financial account records and ledger. These records include:

- The Date of The Charges
- The Purpose of the Charges
- The Amount of Each of The Charges
- The Date of Payments
- The Source of Payments i.e. Federal Pell, FDLS- SUB, FDLS- UNSUB, FDLS -Plus loan
- The Date and Amount of each disbursement of grant or loan funds
- The Date and Amount of funds returned to the Department of Education

Record	Item in Record	Location of Record	Length of time	Final Disposition
Program Student Files	Admission Records (Enrollment agreement, Proof of HS, Admission determination records)	Registrar/Admission Pro.	Records must be maintained for a minimum of five (5) years after the end of the institution's most recent fiscal year during which the student was last enrolled	Destroy after length of time
	Academic Transcript	Electronically in College Office	Permanent	n/a
	Advising/Counseling Notes / Progress Reports	Student Services	Records must be maintained for a minimum of five (5) years after the end of the institution's most recent fiscal year during which the student was last enrolled	Destroy after length of time
	Financial Aid	Financial Aid Office	Records must be maintained for three (3) years after the end of the institution's most recent fiscal year during which the student was last enrolled. Any records involved in any claim or expenditure, which has been questioned by federal audit are retained until the question is resolved.	Retain/After 3 years archive for 2 additional years/ Destroy after length of time
	Attendance Records	Attendance Software and Registrar Office for student physical or electronic signatures	Records must be maintained for a minimum of five (5) years after the end of the institution's most recent fiscal year during which the student was last enrolled	Destroy after length of time
	Placement Activity	Placement Coordinator Office	Records must be maintained for a minimum of five (5) years after the end of the institution's most recent	Destroy after length of time

			fiscal year during which the student was last enrolled	
Record	Item in Record	Location of Record	Length of time	Final Disposition
Program Graduate Records	Final Transcript with program completion date and credential granted	Registrar	Permanent	Permanent electronic record off-site fireproof storage

Student Information

The following platforms are used by ATS Institute employees to securely share and store sensitive student information.

College Office: Online Student Information System (SIS)

ATS students, faculty, and academic related staff are provided with a College Office login by the ATS Director of Instructional Technology & Online Learning. Upon first sign on the user will be prompted to create their own password.

Communication, such as announcements, academic records, admission records, student documents (such as proof of graduation, id's, registrar letters) are utilized and stored in College Office.

Faculty and staff are assigned to a role within the system that gives limited access to student records as designated by their role. Students have access only to their own student records. Faculty, staff, and students are deactivated upon exiting ATS Institute of Technology.

College Office Student Information Security Overview

Protected from unauthorized access

- Data is in the Cloud and therefore physically inaccessible to anyone.
- Data is encrypted via AES 256-bit encryption while it travels on the internet as well as while it is stored on College Office server.
- The system runs on an isolated and dedicated server which is locked down behind a very tight security policy and always kept current with the latest security patches.
- Data is never shared with a 3rd party data processor.
- Strive to fully abide by the latest European Data Protection Regulation law, the most stringent data privacy law in the world.

Protected from accidents and disasters

- Data is backed up every night to 2 different locations.
- College Office preserves each daily backup for 45 days.
- The system is hosted in a ISO-27001-2013 data center in the USA.

Always accessible

The client always has access to the latest backup of their data.

Basecamp Platform: secure online platform
ATS employees are provided with their own login and passwords to basecamp. Files and folders are created by the Operations Manager and assigned access to designated employees as needed. Third parties are only authorized by the ATS Operations Manager or CEO to specific folders that contain information that has been released and compliant with all FERPA and security regulations. The access is provided by a secure link, to the third-party designee and has an expiration date.

Basecamp Student Information Security Overview

All data are written to multiple disks instantly, backed up daily, and stored in multiple locations. Files that are uploaded are stored on servers that use modern techniques to remove bottlenecks and points of failure.

Whenever data are in transit, everything is encrypted, and sent using HTTPS. Within basecamp firewalled private networks, data may be transferred unencrypted.

Any files that are uploaded to are stored and are encrypted at rest. The application databases are generally not encrypted at rest — the information added to the applications is active in the databases and subject to the same protection and monitoring as the rest of the systems. The database backups are encrypted using GPG.

The servers — from power supplies to the internet connection to the air purifying systems — operate at full redundancy. The systems are engineered to stay up even if multiple servers fail.

The servers are protected by biometric locks and round-the-clock interior and exterior surveillance monitoring. Only authorized personnel have access to the data center. 24/7/365 onsite staff provides additional protection against unauthorized entry and security breaches.

The software infrastructure is updated regularly with the latest security patches. The products run on a dedicated network which is locked down with firewalls and carefully monitored. While perfect security is a moving target, basecamp works with security researchers to keep up with the state-of-the-art in web security.

Basecamp has a team dedicated to maintaining account security on the systems and monitoring tools that are set up to alert of any nefarious activity against the domains.

D2L/Brightspace Platform: Online Learning Management System (LMS)

ATS Faculty and academic related staff are provided with a D2L login by the ATS Director of Instructional Technology & Online Learning. D2L passwords are utilized with Gmail single sign on.

Student D2L login information is shared by the ATS Director of Instructional Technology & Online learning in a secure email to the student. Their password is utilized by Gmail single sign on.

Communication, such as announcements, messaging, and academic work are transmitted within the D2L platform securely.

D2L Student Information Security Overview

Environment Security

D2L partners with Amazon Web Services to provide a highly secure, durable and available infrastructure for deploying our Brightspace platform. AWS is a global world leader in delivering IaaS (Infrastructure-as-a-Service) solutions and, like D2L, demonstrates their compliance through a myriad of security and compliance certifications.

Security Monitoring

D2L uses an industry leading Security Information and Event Management (SIEM) solution to collect, aggregate and correlate millions of system events a day across D2L's infrastructure to provide monitoring teams with real time insight into potential security events.

LMS Security in the Brightspace Platform:

Access & Authentication

The Brightspace platform supports Single Sign On (SSO) and integration with various authentication solutions including Active Directory, LDAP, Kerberos, CAS and SAML.

Secure Transmission

Client connection to the Brightspace platform is via TLS cryptographic protocols with RSA encryption, so client data is transferred securely.

Application Security

Code for the Brightspace application is developed and tested following principles set out in the Open Web Application Security Project (OWASP) Top Ten framework to help ensure Brightspace is a secure platform.

Backup and Recovery

System and client data are backed up on a regular basis using asynchronous encrypted data transfer to offsite storage to ensure that client services can be restored in the event of a disaster.

Gmail Platform: E-mail communication

Gmail is the platform used for ATS emails. Students are assigned an ATS email by the ATS Director of Instructional Technology & Online Learning.

Student ATS email login information is shared in a secure email to the student. Upon first sign on the student is prompted to create their own password.

All email communication is made via ATS email between staff and between staff and students. Both messages and any attachments sent or received are secure. Any sensitive information that needs to be sent outside of the organization via email is password protected.

Gmail Student Information Security Overview

Gmail protects from spam, phishing, and malware, before they reach an inbox. The AI-enhanced spam-filtering capabilities block nearly 10 million spam emails every minute

Phishing protections
Gmail blocks more than 99.9% of spam, phishing attempts, and malware.

Safe Browsing
Safe Browsing protects by identifying dangerous links in email messages and warns before visiting the site.

Proactive alerts
Gmail warns before downloading an attachment that could put security at risk.

Account safety
Google protects accounts against suspicious logins and unauthorized activity by monitoring multiple security signals.

Confidential mode
Users can make messages expire after a set period of time and remove the option for recipients to forward, copy, download, or print a message from Gmail.

Email encryption
In Google infrastructure, messages are encrypted at rest and while in transit between data centers. Messages transiting to third-party providers are encrypted with Transport Layer Security when possible or required by configuration.

Google G Suite Platform: Cloud based productivity and collaboration tools

The google G Suite platform is utilized by staff to create, collaborate, store and share school documents and is FERPA compliant. The privacy and security for Google G Suite platform is listed.

Google Student Information Security Overview

Security
Secure foundation for digital learning

- Easily add users, manage devices, and configure security and settings so data stays safe
- Stays protected on any device, distribute apps on mobile devices, and can limit remote access to any endpoint
- Safeguards sensitive data in Gmail and Drive with automated data loss prevention (DLP)

Compliance
Meet rigorous compliance and accessibility standards

- Retain, hold, search, and export user data for compliance and eDiscovery in Vault
- In compliance with numerous requirements and industry standards including FERPA, COPPA, and GDPR
- Includes buil-in accessibility tools like closed-caption, Screen Reader, braille readers, screen magnification, and more

WEBER
& ASSOCIATES

11/01/2017

Weber & Associates, Inc.
FERPA and PII Security Statement

Synopsis

As a provider of Title IV Financial Aid Management services for postsecondary educational institutions, Weber & Associates, Inc. (Weber) faces the ongoing and growing global cyber security threat for both the Weber network and our customer's Personally Identifiable Information (PII). As part of our commitment to continuous improvement, Weber regularly monitors and addresses new and emerging threats as well as new cyber security technologies and best practices. The U.S. Department of Education (ED) has defined security and privacy requirements for all institutions that qualify for offering Title IV Federal Financial Aid (FFA) programs to their students. The requirements are defined as part of the Family Educational Rights and Privacy Act (FERPA). While FERPA is not a security specification, it does provide the minimum requirements that must be met and what data must be protected. As a third-party servicer that participates in the process of determining student eligibility, scheduling and ordering funds for Title IV aid, Weber addresses all requirements set forth in FERPA. Weber is in compliance with all the requirements set forth in FERPA for both the security of all FFA related data, as well as the protection of all Personally Identifiable Information (PII). Weber employs physical access controls, network security, cloud service security, application security, asset management controls, and continuous threat monitoring and assessments to ensure the privacy and protection of all our activities, and our customer's data and activities while using our systems and applications. For a more comprehensive description of Weber security, you may request a copy of the full Weber & Associates, Inc. Security Statement from your customer service representative. In the unlikely event of a breach of security at Weber, a full notification and disclosure will be sent at the earliest possible time to each school affected. It will include the details of what information was compromised, who was affected, and any recommended remediation steps for Weber, the school and any affected students or parents.

Information System Data Security Plan

Date Created: 11/9/2015

Date Revised: 1/14/2022

Note:

Introduction

At the core of its product design, Campus Ivy has implemented many data protection schemes that complies with the Federal and State regulations for protecting user/ student data. Every aspect of the Campus Ivy technology is hosted by Microsoft Azure (Hosting facility) which provides data redundancy in a secured environment. Many US and international companies use Microsoft Azure for deploying cloud based computing. This document outlines the IT security plan for Campus Ivy.

Access Control

- Client-server communication is always performed over secure protocols, such as HTTPS (HTTP over SSL) and FTPS (FTP over SSL)
- FTP access is secured by IP address whitelisting on the server and home directory level in addition to username/password
- Database connections are secured by IP address whitelisting and username/password
- Read/Write production access is available only to a subset of the Campus Ivy Information Technology team.
- Direct database access is not provided to clients.
- Production databases are replicated asynchronously to other geographic regions for disaster recovery
- Application configuration files are encrypted immediately after deployment using machine keys
- All application and database source code are stored and maintained in Azure DevOps (source control)
- Campus Ivy does not maintain a data center; all the technology resources are cloud based and hosted by Microsoft Azure
- Users access Campus Ivy web applications through a secure login (username and password) and configurable multi-factor authentication.
    - CI directors determine level of access for each employee and access is granted via a formal process governed by the principle of least privilege.
    - Clients are responsible for managing onboarding and offboarding as well as role-based access however client based role are limited based on the principle of least privilege.
    - School users can only access data for their schools
- Passwords are at least 8 characters in length, at least 1 digit, at least 1 upper case letter, at least one special character, and expires at a configurable date range up to 365 days
- The system supports hierarchical role-based access control, so only users with permission are granted access to sensitive data and system features
- The system is automatically logged off if inactive for more than 10 minutes

Awareness & Training

- Campus Ivy users are instructed not to store sensitive data on their local drives
- Campus Ivy's operation requires a clean desk policy via the use of password managers and cloud-based file repositories that offer version control and access limitation
- Employees are trained on malware and phishing email identification and handling
- All Campus Ivy employees and contractors are required to sign Data Privacy Agreement, below is an example of such language.

1. Data Privacy

   CAMPUS IVY engages in various student related activities which grants it access to sensitive and sometimes protected student information and data ("data"). Employee may have various levels of access to the student data in order to perform his/her daily activities.

   Employee hereby recognizes and understands the sensitivity of the data s/he interfaces with on a daily basis, and promises to protect that information to the best of his/her ability. Employee further understands and accepts that any intentional or unauthorized use of the data may result in an immediate termination of his/her employment.

   Unauthorized use of data may include, but is not limited to:

   - ✓ Sharing or selling students Social Security Number, name, date of birth and address with any other person firm or entity that does not possess proper access to such data
   - ✓ Removing student Personally Identifiable Information (PII) from company databases for any unauthorized use
   - ✓ Reverse engineering company's software to gain access to student PII

- Campus Ivy users are trained not to send sensitive data via email or other unsecure means

Audit & Accountability

- CEO and Head of IT perform random examination of users' computers
- All Campus Ivy employees are held accountable for protecting PII data, and understand that failure to do that may result in the termination of their position
- Network traffic is frequently monitored and compared against a baseline for each workstation and server
- Endpoint protection reports patch management, system configuration, device health, failed login, drive space, and malware scan status which are reviewed and resolved daily
- Microsoft Azure platform provides audit reports on security breaches
- Standard employee onboarding and offboarding process is followed to ensure limited access

Change Management

- Source code is branched by environment (E1_Dev, E2_QA, E3_Demo, E4_Prod) and is promoted from one environment to another in sequential order after stakeholder approval via a formal change management process.
- All deployments of source code are performed by remote build servers that are integrated to the source control repository for all environments. Last 5 successful builds and the last failure for DEV, QA, and DEMO are kept. All PROD builds are kept regardless of status
- Hardware and Software changes go through quality assurance testing, then a formal change management approval process with company stakeholders before the changes can be promoted to the Demo and Production environment
- Server configuration and security changes made internally are reviewed by a thirty organization to ensure avoid the introduction of misconfigurations and other security threats
- Due to the use of automated deployments and formal change management processes, server access is limited to IT leadership and the CEO, which reduces insider security threats.

Incident Response

- Campus Ivy users are required to notify the CEO and the Head of IT of any data security breach or phishing emails received
- CEO and Head of IT will take the appropriate actions to remedy the issue within 24 hours, and notify the users, state and federal agencies when necessary
- Employees with repeated security breaches will be written up, which may result in termination

Media, Physical Protection

- Local laptops and computers are meant to be used to access the Campus Ivy system and data residing in the secure Microsoft Azure platform
- All business documents, including those with sensitive data, are shredded
- Campus Ivy users are required not to keep sensitive data on their local hard drive, flash drives, or leave unattended on printers
- Clean desk policy requires all Campus Ivy employees to remove (shred) sensitive documents prior to leaving the office and to use password managers
- Data on servers are protected by disk level encryption using bitlocker

Protection of Personally Identifiable Information (PII)

- All student PII is masked from the user in the Campus Ivy CORE system, excluding the ISIR view which is controlled by user access rights
- Unique student id numbers are used to identify students throughout the database
- All PII related data is encrypted when data is transmitted between CORE and other systems

Ransomware Protections and Recovery

- Endpoint protection is installed on all Campus Ivy servers and work stations with the intend of identifying and resolving ransomware and other malware
- All servers and work stations are backed up daily, offering a recovery method in the event of ransomware activation
- Cyber Security Insurance is also maintained as a part of the company's disaster recovery and business continuity strategy to combat damage from ransomware and other types of malicious software

Risk Management

- There are many potential disruptive threats that can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included Appendix E. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Third Party Servicers

- Campus Ivy does not utilize the services of organizations or individuals based overseas; as such all third-party entities are required to abide by US rules and regulations governing data access, usage, and storage
- All third-party servicers are bounded by contracts that govern access, data use and sharing
- All third-party servicers utilize Campus Ivy administered technology that are subject to monitoring and revocation

Security Assessment

- CEO and Head of IT perform annual security and data protection assessment, and document the results. The assessment is normally performed during Q1.

Contact Information

CEO: Cid Yousefi, Office: 954 281-7003, Cell: 786 374-9564, Email: cidy@campusivy.com

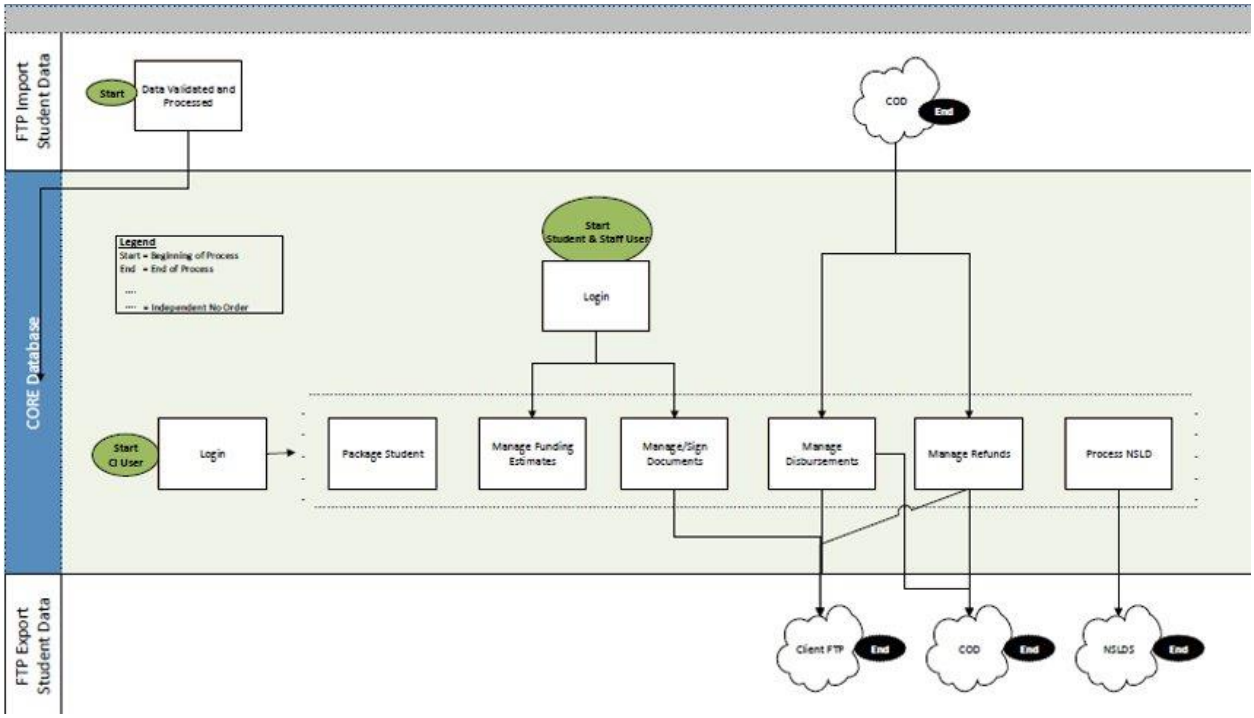
VP of IT: Kevon McNichol, Office: 844 848-5332 ext 308, Email: kmcnichol@campusivy.com

Disaster Recovery

- Campus Ivy building is damaged by hurricane, etc
  - Campus Ivy system is hosted by Microsoft Azure, without any applications running at the local office. This means that customers will continue to be able to use the application without any interruption, unless the customer is in a hurricane zone. Campus Ivy (CI) employees can connect to Core from anywhere as long as they have Internet access – Starbucks, etc.
  - Campus Ivy Core system, including the SQL Server and FTP Servers are hosted at the East Region (Virginia) center at Microsoft. The servers are replicated across multiple regions, with the FTP server being backed up nightly. In the event a server goes down within the Microsoft Azure environment, it can be hot swapped within minutes.
  - CI management will coordinate with essential employees (those doing processing and drawdowns) to use laptops and desktops to connect with the system remotely. This also includes purchasing or utilizing existing cell phones to connect with customers.
  - Each computer needs to have MS Office, MS Teams, Internet Explorer and FileZilla installed. This means that normal business operations can continue if all employees are working remotely.
- Building is damaged and communication/ power is not available
  - The same options as above will apply. If the building will not be repaired for more than two weeks, then CI management will locate a temporary office/ location to run the business from.
- See Appendix E for a full Risk Management breakdown

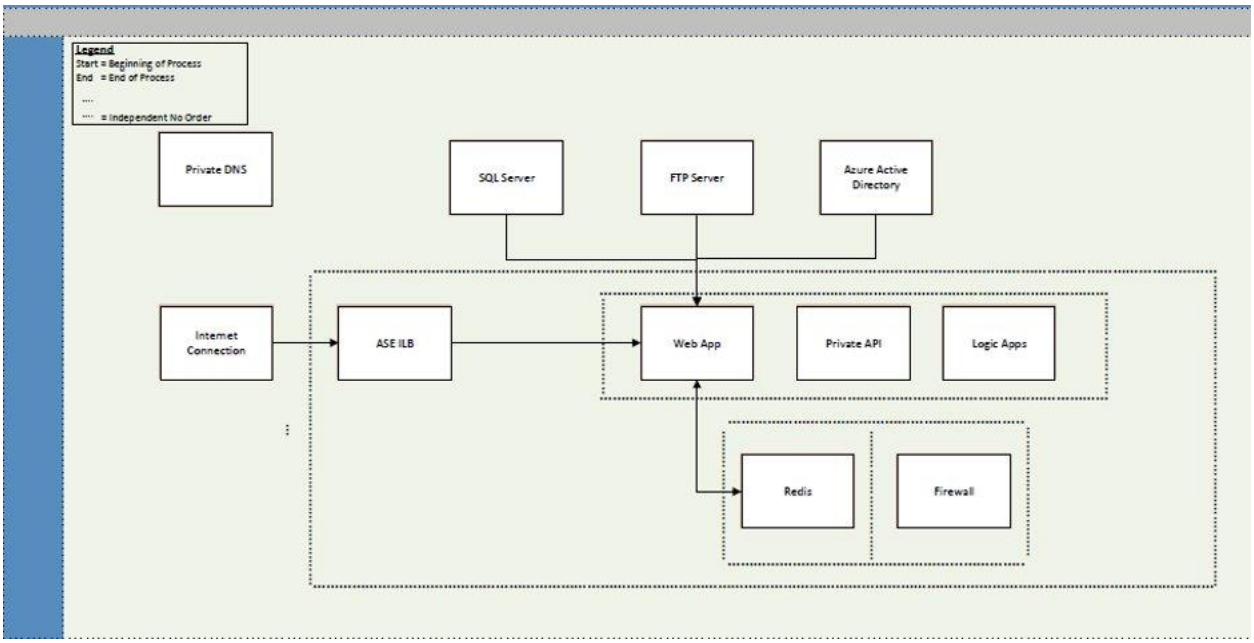
Appendix A

High Level Data Flow Diagram



Appendix B

Logical Architecture Diagram



Appendix C

Logical Architecture Inventory

Service / Server	Hosting Company	OS	Service name/version	Is it in a clustered configuration?	network protocol encryption	Storage encryption
Web hosting (App and API)	Microsoft Azure	Windows2019	Windows Server 2019	Yes	TLS1.2	Unknown
Core Database	Microsoft Azure	Azure Managed	Sql Server 2016	Yes	Azure managed	Azure managed
Redis	Microsoft Azure	Azure Managed	Redis	Yes	Azure managed	Azure managed
Reporting Platform	Campus Ivy	N/A	Core	No	TLS1.2	No storage at rest
FTP	SimplifyEd	Windows2012	Filezilla Server 0.9.49	No	Vendor managed	Vendor managed

Appendix D

Authentication and Authorization

Application auth and account management	
How are application users authenticated?	app-custom token system
Password complexity requirements / options:	At least 8 characters long, at least 1 number, at least upper-case letter, at least one special character
Is multifactor auth supported?	Currently in design for Login process
What lockout mechanisms exist?	App-custom
Who is responsible for administration of application user accounts?	IT and account reps
Does the applications support role-based access privileges?	Yes

Underlying infrastructure and services auth and account management	
How are OS and service admin users authenticated?	(AD, ADS, LDAP, etc..)
Do OS and service admin users have the technical capability to view client data?	Yes
Vendors that can view client data:	Microsoft and FTP Server vendor has access to files on their servers
Describe how the above access is monitored, provisioned, and if it is role based:	Not monitored but there is a contractual agreement about how data should be handled

Appendix E

Potential disasters have been assessed as follows:

Potential Disaster	Probability	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is hosted at Microsoft Azure; backed up at multiple data centers
Fire	3	4	All critical equipment is hosted at Microsoft Azure; backed up at multiple data centers. All employees can work from home without any interruption in service. All that's required is internet connection at home.
Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		All data can be restored from backup; new VM's and Web servers installed within Azure in less than 24 hours. Cyber insurance also protects against irreparable damage.
Electrical power Failure	3	4	All employees can work from home.
Loss of communications network services	4	4	Backup internet service provider is contracted to switch over in case of outage.
Hurricanes	2	4	All critical equipment is hosted at Microsoft Azure; backed up at multiple data centers. All employees can work from home without any interruption in service. All that's required is internet connection at home.

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance