ATS Institute of Technology

www.atsinstitute.edu

-

Student Information Security

with Risk Assessment and Response

2023-2024

Date Published: March 16, 2023
Updated May 18, 2023

25 East Washington, Suite 200
Chicago, IL 60602
Phone 312-300-0980

Fax 312-277-2500

Table of Contents

1. Family Educational Rights & Privacy ACT (FERPA) Page 3-4

2. Student Information Page 4

3. Student Record Storage Page 4-5

4. Employee Security policy and training Page 5-6

5. File Location and Security Policy Page 5-10
    a. Backup Page 5
    b. Campus Ivy Page 6
    c. College Office Page 6-7
    d. Basecamp Page 7
    e. D2L/Brightspace Page 8
    f. Google Suite Page 8-9
    g. Quickbooks Page 9
    h. Bubble Page 10

6. Cybersecurity Incident Response Plan Page 11-14
    a. Preparation Page 11
    b. Detection Page 11-12
    c. Identification Page 12-13
    d. Containment Page 13
    e. Eradication Page 13
    f. Recovery Page 13-14
    g. Post-Incident Review Page 14

7. Appendix A: Incident Response Contacts Page 15

8. Appendix B: Incident Response Flowchart Page 16

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

Student Information

Note: MDT College of Health Sciences dba ATS Institute of Technology will be referred to as "ATS" in this document

The ATS Registrar office is responsible for maintaining all admission and academic records. These records are kept in the "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 ledgers. 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 Storage

Record	Item in Record	Location of Record	Length of time	Final Disposition
	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

Program Student Files	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 a 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 fiscal year during which the student was last enrolled	Destroy after length of time
Program Graduate Records	Final Transcript with program completion date and credential granted	Registrar	Permanent	Permanent electronic record off-site fireproof storage

Employee Security and Training

Information Security Responsibilities

The staff, professors, and contractors of the institution are in charge of making sure that the data and systems are safe. This includes the following:

1.1. Keeping passwords secure and not sharing them with others
1.2. Reporting any security incidents or suspected incidents to the appropriate authority
1.3. Using only authorized software and hardware on the institution's systems
1.4. Keeping physical documents and devices containing sensitive information in a secure location
1.5. Complying with all applicable laws, regulations, and policies related to information security
1.6. Using encryption when transferring sensitive data over the internet

Access Control

Usernames and passwords are used to control access to the institution's data and systems. Access control is managed by the IT department, and permissions are regularly examined to make sure they are pertinent and current. Only those who require it to fulfill their job obligations have access to sensitive information.

Training and Awareness

To inform employees, faculty members, and contractors about information security best practices, the institution conducts regular training and awareness programs. All new staff, faculty members, and contractors must complete information security training during onboarding.

File Location & Security Policy

Backup.
All systems are 3rd-party and backed up as outlined in their backup policy to ensure no data will be lost. The 3rd party systems are as follows:

- Campus Ivy
- College Office
- Basecamp
- D2L/Brightspace
- Google Suite
- Quickbooks
- Bubble

Campus Ivy

ATS Financial Aid Advisors each have their own assigned username and password to Campus Ivy in order to access student financial aid records.

The Campus Ivy team maintains all student records associated with Student financial aid awards in electronic format 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 ATS 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 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 state-of-the-art 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 Directory 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.

Google G Suite Platform (including Gmail)

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. 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 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 built-in accessibility tools like closed-caption, Screen Reader, braille readers, screen magnification, and more
- Upload a file of any type to Google Drive, data is encrypted in-transit and at-rest. If a person chooses to access these files offline, info is stored on the person's device.

Quickbooks

ATS Business related staff are provided with a Quickbooks login by the ATS Directory of Instructional Technology & Online Learning. Each user has an individual username and password for login.

Quickbooks maintains student financial account records.

Quickbooks Student Information Security Overview

Security:

Quickbooks (QB) safeguards information by encrypting it. The type of encryption we use is called AES-256 (Advanced Encryption Standard with 256-bit keys), and it ensures the highest level of cryptographic security. QB also participates in established partnerships with multiple security organizations and alliances to help ensure we protect our customers' data with the best methods out there.

Bubble

ATS Business related staff are provided with a Bubble single sign-on (SSO) login by the ATS Directory of Instructional Technology & Online Learning. The ATS bubble system SSO are utilized with Gmail single sign on.

Bubble utilizes financial aid and student account data to maintain student financial account records.

Bubble Student Information Security Overview

Security

- Bubble uses automated code testing, vulnerability testing (including OWASP Top 10) and continuous monitoring technologies.
- Bubble uses AWS RDS's AES-256 encryption to encrypt data at rest.
- Bubble apps come with logs so that you can review what your app has done, even in the background.
- Bubble apps can access point-in-time data recovery for your own data at any time.

Compliance:
Meet rigorous compliance and accessibility standards

- Bubble is built on Amazon Web Services, which is itself compliant with certifications such as FERPA, SOC 2, CSA, ISO 27001, and more.

Cybersecurity Incident Response Plan
ATS Institute of Technology

This Cyber Security Incident Response Plan outlines the procedures that ATS Institute uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or serviced by the school. This document defines an Incident Response Team's roles and responsibilities, including identifying, isolating, and repairing data security breaches. The Director of IT will oversee the information security program.

This Response Plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information. Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly impact operations and/or result in the unintended disclosure of sensitive data. Minor events that have little impact on day-to-day operations are not considered an incident under this Plan.

The Incident Response Plan contact numbers and infrastructure information within this document should be printed, and easily accessible in hardcopy form. Digital resources may not be available during an incident.

Preparation

Employees will be trained regarding their incident response roles and responsibilities in the event of a data breach. See *Appendix A: Incident Response Contacts*

- Main role employees will attend annual training that include updates and implementation of cybersecurity.
- All other employees will receive training at hire and on an annual basis. The training will be provided by the IT department for review and completion.

Incident response drill scenarios and regularly conduct mock data breaches are conducted on an annual basis to evaluate the incident response plan.

If a user, employee, or student observes a potential security event they should notify the Director of IT immediately. If the Director of IT is not available, then the event should be immediately reported to another member of the Administrative Team.

A periodic assessment of the security practices of service providers will be reviewed on a yearly basis every Fall. The audit will include the following:

- 3rd party providers - review privacy policies and updates
- Servers - monitored daily. On campus servers only store directory based data.
- Website - MDT Institute website is secured and managed by Wix.

Detection

The Director of IT will immediately report the incident to the Administrative Team. The Director of IT is responsible for communicating the incident, its severity, and developing the action plan with consultation from the Administrative Team.

If the Director of IT or Administrative Team members are not available, a user should isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, the user should turn off the wireless connection. If isolating the machine from the network is not possible, then the user should unplug the machine from its power source.

If the Director of IT determines or suspects a cybersecurity breach, cyber extortion threat, or a data breach as defined in this Plan, then the team will proceed to the incident flowchart, *Appendix B: Incident Response Flowchart*

If the incident is determined not to be a security threat, then the Director of IT will work with the Administrative team to assess the incident, develop a plan to contain the incident, and ensure the action plan is communicated and approved to all users.

The Director of IT will ensure that all actions are documented as they are taken and the Administrative team, and outside support are updated.

Identification

During identification, the Director of IT will determine whether or not a breach has occurred. A breach or incident could originate from many different areas. A security incident is an event that is a cybersecurity breach, or a cyber extortion threat, or a data breach. In IT, an event is anything that has significance for system hardware or software, and an incident is an event that disrupts normal operations.

Questions to answer while identifying the security event:

- When did the event happen?
- How was it discovered and who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?

Types of breach:

- **Cybersecurity breach:** A cybersecurity breach is any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

- **Cyber extortion threat:** A cyber extortion threat is a threat against the network to:

    - Disruption to operations.
    - Alter, damage, or destroy data stored on the network.
    - Use the network to generate and transmit malware to third parties.
    - Deface the school's website.
    - Access personally identifiable information, protected health information, or confidential business information stored on the network, made by a person or group whether acting alone or in collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

- **Data Breach:** A data breach is the actual or reasonably suspected theft, loss, or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

Identification of Incident

Incident Type	Description
Malware	A computer virus, worm, and other malicious applications are computer programs that attack or infect another program. Malware can spread from computer to computer, infecting programs on each computer.

Denial of Service (DoS)	A DOS or a DDOS attack is an attack that prevents or impairs the use of network, system, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.
Malicious Code	A web application attack happens when hackers compromise an on-line form or application. One way this can happen is with a SQL injection attack. A SQL Injection attack occurs when hackers fill a field with malicious SQL code designated to execute specific commands against the forms or application's database.
Inappropriate Use	Inappropriate usage is when an individual or an entity violates acceptable use of any network, workstation, information, application, server, or data policies.
Ransomware	An attacker installs malware on a device and encrypts the hard drive. The malware announces the hard drive is encrypted and prompts the user to pay a ransom in exchange for the key to unencrypt the device.

Containment

Contain the breach so it doesn't spread and cause further damage to the organization. Disconnect affected devices from the Internet. Have short-term and long-term containment strategies ready. Use system back-up to help restore operations so that any compromised data is not lost. Update and patch systems and reset passwords.

Once contained complete the following:

- Note what was done to contain the breach
- How to contain the breach in the future
- Quarantine any discovered malware from the rest of the environment
- Note back-ups put in place
- Require multi-factor authentication for remote access
- Review access credentials for legitimacy
- Apply recent security patches and updates

Eradication

Eradication addresses the root cause of an incident after containment. Eradication is the removal of malicious code, accounts, or inappropriate access and also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred. Securely remove all malware, harden systems, and apply updates.

During Eradication complete the following:

- Securely remove artifacts/malware from the attacker been securely removed
- System has been hardened, patched, and updates applied
- Re-image the system if possible

Recovery

Recovery is the process of restoring affected systems and devices. It is important to restore normal operations without the fear of a recurring breach. Recovery allows processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications.
- Change all user and system credentials.
- Restore data to the system.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.

Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the Incident.
- A description of the response to the Incident and whether it was effective.
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents.

APPENDIX A: Incident Response Contacts

Incident Response Manager

Name Rumy Kabir	Email rkabir@atsinstitute.edu
Work Phone 312-283-5771	Alternate Phone

Backup Incident Response Manager

Name Gina Anadilla	Email ganadilla@atsinstitute.edu
Work Phone 773-672-8957	Alternate Phone

Technical Support Contacts

Name Brian Hedges	Email bhedges@atsinstitute.edu
Work Phone 312-481-8408	Alternate Phone
Name Misti Ludwig	Email mludwig@atsinstitute.edu
Work Phone 312-481-8403	Alternate Phone
Name Kaz Hasbun	Email khasbun@atsinstitute.edu
Work Phone 312-481-8412	Alternate Phone

APPENDIX B: Incident Response Flowchart