Policy Manual
# Table of Contents

Introduction ........................................................................................................................................... 3
Confidentiality........................................................................................................................................ 3
FERPA Policies ..................................................................................................................................... 3
Data Management Policies ................................................................................................................ 4
  Passwords and Login Information ...................................................................................................... 4
  Data Handling/Retention/Storage ......................................................................................................... 4
GradesFirst and Facebook ................................................................................................................... 5
Data Backup/Recovery Policies ........................................................................................................... 5
Architecture .......................................................................................................................................... 6
Data Breach Policies and Procedures ................................................................................................. 7
Security Policies and Procedures .......................................................................................................... 8
  Network/Internet Access to the GradesFirst Servers Hosted by AWS .............................................. 8
  Physical Security of the GradesFirst Data Center Hosted by AWS .................................................. 9
  AWS Employee Access ...................................................................................................................... 9
  Access Security to the GradesFirst Application ................................................................................. 10
Supported Browsers ............................................................................................................................. 11
GradesFirst Releases/Updates ............................................................................................................. 11
Appendix ............................................................................................................................................... 12
References .............................................................................................................................................. 12
Introduction

GradesFirst delivers a secure and safe environment for which our users can safely record sensitive student information. We here at GradesFirst realize that our application is only as good as its security. Knowing this, we have allocated a tremendous amount of time and resources to ensure our client’s data is as protected as technically possible. The ensuing document provides an overview of our policies.

- Confidentiality
- FERPA Policies
- Data Management Policies
  - Passwords and Login Information
  - Data Handling/Retention/Storage
  - GradesFirst and Facebook
  - Data Backup/Recovery Policies
- Architecture
- Data Breach Policies and Procedures
- Security Policies
  - Network/Internet Access to the GradesFirst Servers Hosted by AWS
  - Physical Security of the GradesFirst Data Center Hosted by AWS
  - AWS Employee Access
  - Access Security of GradesFirst Application

Confidentiality

All employees at GradesFirst are required to sign a non-disclosure agreement (NDA).

Only GradesFirst developers have access to institution or university data.

Background checks are performed on employees that have root access to client’s data.

GradesFirst will not share or sell any information from our customers. If in the case of legal action, we will submit to the necessary rules and regulations of the local, state or federal entity as required by law and will coordinate all of our actions (as much as is feasibly possible) with the institution or university in question.

FERPA Policies

FERPA Compliant. GradesFirst takes steps to provide the granular permissions necessary to ensure that only educational representatives that have legitimate need and right to see a student’s information can access that information.

All employees are required to read, acknowledge and comply with the Family Educational Rights and Privacy Act (FERPA). GradesFirst has, on record, a signed copy for each employee stating they will abide by the FERPA Act.

GradesFirst understands the sensitive nature of all client data that we handle and any required need to disclose data that was not specifically authorized by our clients would have to be approved in writing (either by letter or email) by said clients before it would be disclosed unless required to do so by law.

GradesFirst does not request/store any medical or financial information. Therefore neither the HIPPA nor the Gramm-Leach-Bliley Act (GLBA) Acts apply to our model.
Data Management Policies

Passwords and Login Information

- GradesFirst passwords must be at least 6 characters and no more than 40 characters in length. Your GradesFirst Administrator may set a minimum password length as well.

- GradesFirst also allows the GradesFirst Administrator to determine when and if user passwords will expire. Options for this setting include: Never, 45 days, 90 days, 180 days or 365 days.

- Initial GradesFirst passwords are automatically generated when a user account is created and then stored in the application database in an SHA-1 irreversible hash format.

- Upon a password update, the same process of transforming the password in an irreversible hash will occur before the password is stored in the application database.

- All passwords are filtered out of log files so they only show up as [FILTERED] so they are not compromised there as well.

- When a user account is first created, the user is assigned a default password that consists of eight random characters and symbols. As with any password they use, this automatically assigned password is not actually stored in the database, but an irreversible SHA-1 hash is stored in its place.

- GradesFirst IDs are stored in the application using Blowfish encryption.

- Our audit logs record all successful, and unsuccessful, log in attempts into GradesFirst.

Data Handling/Retention/Storage

Within the GradesFirst application, all data is transferred from the user to the application (and back) using a secure Camellia 256-bit Secure Sockets Layer (SSL) connection.

We maintain "Created At", “Updated At”, “Created By” and "Updated By" attributes on records in the database for our records when changes occur in our databases. This gives us the ability to easily identify who, what and when changes were made.

GradesFirst application data is stored indefinitely in our database until such a time that a client wishes to discontinue their use of GradesFirst.

In the event an institution or university decides to end their use of GradesFirst, we will remove any and all data associated with that entity. Their data will be deleted from the current production database within five business days and then, over the course of the next ten actual days, the customer’s data will only persist in backups until it has been replaced by subsequent data backups.

Laptop computers are never used to store or transport of university data. Furthermore, no computers used by our developers ever physically possess any actual client data.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that ensures customer data are not exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitation”) to destroy data, as part of the decommissioning process.
**GradesFirst and Facebook**

Students may access GradesFirst via their Facebook page upon loading our GradesFirst/Facebook application. However, before a student may load our GradesFirst/Facebook application, an invitation must be sent to them from the GradesFirst administrator. Once invited, the student(s) then has a choice whether to load this application.

GradesFirst does not store any information directly into Facebook, rather the GradesFirst/Facebook application simply “views” the GradesFirst data via a temporary portal or mirror. When the user logs out of Facebook, that portal or mirror is then subsequently closed.

GradesFirst users are authenticated via their Facebook Username and Password. In other words, no GradesFirst credentials are used to access our application via Facebook.

GradesFirst does not store user’s Facebook information anywhere on our servers.

**Data Backup/Recovery Policies**

GradesFirst has a data retention policy that maintains and backs up all production data for our active customers as long as they remain a customer. We do a full data backup each night on Amazon EC2. We also maintain ten days of backups that carries the same level of security as our entire GradesFirst infrastructure.

Along with our production data backup, we do two complete customer database backups per day. The first is a full drive backup and second is a specific SQL backup. While we do not have a formal procedure, we generally test our data backups at least once per month.

For further verification and testing of backup restorations, we have bi-annual emergency procedures testing where we restore the entire GradesFirst application from backups. This activity includes both a full and partial data restore for specific test institution(s).

In the unlikely event of data loss, recovery is handled by creating a new EC2 instance and restoring our drive backups. AWS also ensures business continuity by having multiple data centers across multiple geographic regions to help ensure maximum protection through redundancy. This is the same type of state-of-the-art redundancy used by Fortune 500 companies across the globe.
Architecture

GradesFirst is a 100% Web-Based application that is designed to run on a true Cloud Computing infrastructure. Perhaps the best definition of Cloud Computing comes from the National Institute of Standards and Technology and is as follows:

‘Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.’

And

‘Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).’

A great visual example of this Cloud Computing SaaS model is show on the next page:
Data Breach Policies and Procedures

As with any application that holds sensitive information, there is always a possibility of a data breach/theft. However we at GradesFirst, with the security infrastructure outlined below, feel confident that we have effectively reduced the chance of a breach as much as technically possible. In the unlikely event a breach occurs, the steps outlined below will be followed:

1. Identify breach
2. Notify client(s) within one business day of identified breach
   a. Inform the client to the best of our ability of how incident occurred
   b. Disclose what data was lost/stolen to the best of our ability
   c. Explain how this breach has/will affected them
3. Provide client with a verbal and/or written plan of action within three days
4. Implement that plan of action and take steps to ensure said breach does not re-occur as soon as reasonably possible
5. Lastly, determine whether or not a local law enforcement agency should be contacted based on the location and details of the incident.
Security Policies and Procedures

Network/Internet Access to the GradesFirst Servers Hosted by AWS

GradesFirst has built its entire infrastructure on top of the Amazon EC2/EBS which allows for system stability, security and data redundancy. We do not rely on individual servers or locations to host our data or services.

All servers run firewalls that allow only authorized traffic. Furthermore, all database servers only allow connections from inside the firewall by the App Servers.

The GradesFirst demo and production servers are protected by firewalls and intrusion detection systems. Also, the AWS network provides significant protection against traditional network security issues. The following are a few examples of said protection: Distributed Denial of Service (DDoS) Attacks, Man in the Middle (MITM) and Attacks & Port Scanning.

Servers use a login process that requires an SSH Key File using RSA authentication and only allow access from the internet to dedicated SSH, HTTP & HTTPS ports.

As part of its commitment to creating a world-class cloud computing environment, AWS has sought and successfully completed the SAS70 Type II Audit of their operational procedures and security.

Access to GradesFirst requires that a standard username/password pair authentication be used. For accessing our servers, computers must connect using Secure Sockets Layer (SSL) and an RSA public key authentication. Our development machines all have set passwords and sit behind a firewall for protection.

We review our server’s logs weekly to identify both unauthorized and attempted access to our servers.

We restrict access to production-level data to a select few developers at GradesFirst, not even the CEO has access to this data. Within GradesFirst, we only have three computers that have the ability to connect to our production servers.

GradesFirst employs a monitoring application (Nagios) that alerts our team if the GradesFirst servers become unavailable. Also, with our managed hosting, if we were to have reliability issues with any of our services (application, database, logging, etc.), we would be alerted and resolutions would be presented via AWS.

GradesFirst uses professional services from Engine Yard to ensure our servers and software have the latest and most critical patches available. This helps protect GradesFirst and our client’s data from even the most recent threats. Servers are also performance optimized for stability and efficient handling of the GradesFirst application and data. Engine Yard is considered “Best of Breed” amongst its peers. Datamonitor\(^\text{ii}\) gave its seal of approval to Engine Yard by naming them one of the “2009 top 10 Cloud Providers”

Our GradesFirst developers meet each month to internally evaluate the current status of tech trends, security developments, performance issues and scaling needs as they relate to our technology. When issues of concern arise, we conference with Engine Yard to address those issues and implement the most appropriate course of action to ensure adequate performance and protection of the GradesFirst system and our client’s data.

GradesFirst will perform a data intrusion audit each quarter to ensure your data is safe and secure from malicious attacks. We will examine log files, monitors system calls, examine flow of network packets and look for other evidence that are signs of intrusions, including network traffic.

See Appendix #5 to obtain more information on AWS as well as a link to their White Pages.
Physical Security of the GradesFirst Data Center Hosted by AWS

All GradesFirst servers are hosted with Amazon’s EC2/EBS platform. This is the same platform Amazon.com uses.

Data center is Tier 4, Class A, SAS70 Type II and Safe Harbor compliant.

Our GradesFirst application and client data are located in multiple data centers inside the United States, providing the necessary data redundancy in the event of a natural, man-made and/or environmental disaster.

Physical access is strictly controlled 24/7 both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Furthermore, all physical access to data centers by Amazon employees is logged and audited routinely.

AWS Employee Access

Data center access and information are granted to employees and contractors who have a legitimate business need for such privileges.

All staff with potential access to customer data are required to undergo an extensive background check (as permitted by law) commensurate with their position and level of access to data.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.

All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
Access Security to the GradesFirst Application

Perhaps, one of the best ways to describe how GradesFirst is accessed by our users is through a visual representation.

The GradesFirst application uses Secure Socket Layer (SSL) technology with up to 256-bit encryption.

All access to the GradesFirst system requires user name and password. Passwords in the GradesFirst database are hashed using a one-way hash. Student IDs in the GradesFirst database are encrypted with 256-bit encryption.

GradesFirst makes use of the latest role-based security features made available through modern development platforms. For application security, every feature is covered by granular permission or role-based security. This security is managed by the administrators of the institution's GradesFirst account.

Client data import files are automatically deleted after 5 days to ensure security of our customer’s data.

All institutions or universities are solely responsible in determining which personnel have access to GradesFirst.
Supported Browsers

Since GradesFirst is Internet Software, it is accessed through a web browser. We support these browsers:

- Chrome 18+
- Firefox 4+
- Internet Explorer 8+
- Safari 5.1+

GradesFirst Releases/Updates

*What kind of an affect do our releases/updates have on our clients?* Normal releases are scheduled as new features and fixes become available. While we do not have a specific day designated for software updates, we do have a specific time... approximately 3:00AM EST. These release windows will sometimes result in GradesFirst being unavailable for up to 30 minutes, but by performing this maintenance early in the morning, our goal is to ensure that the fewest people possible are using the application during that time.

*How are emergency releases/updates distributed and how can they affect our clients?* In very rare cases, we will perform an emergency update to GradesFirst during, what most people would consider, normal business hours. This only happens after much consideration of how this could affect our customers' use of GradesFirst. We do our best to ensure that the updates made to GradesFirst are well-tested and properly planned.

If an emergency release were to happen, customers could experience longer load times for various tasks, in some cases, tasks having to be restarted, users having to log back into GradesFirst, students briefly being unable to check in or out of study hall, etc. As was stated above, emergency releases are rarely approved and only occur if large areas of functionality in GradesFirst have ceased to be available.
Appendix

1. **FERPA – Family Educational Rights and Privacy Act**³
   The regulations provide that educational agencies and institutions that receive funding under a program administered by the U.S. Department of Education must provide students with access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records. With several exceptions, schools must have a student's consent prior to the disclosure of education records.

2. **SAS70 Type II**⁴
   Statement on Auditing Standards No. 70 (SAS70) Type II Audit, is an unbiased opinion from its independent auditors that certifies a service organization has had an in-depth audit of its controls (including control objectives and control activities), which in the case of AWS relates to operational performance and security to safeguard customer data.

3. **Title II of HIPAA**⁵
   Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. This is intended to help people keep their information private, though in practice it is normal for providers and health insurance plans to require the waiver of HIPAA rights as a condition of service.

4. **GLBA – Gramm-Leach-Bliley Act**⁶
   The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer’s right to opt-out of the information being shared with unaffiliated parties per the Fair Credit Reporting Act.

5. **Amazon Web Services Security Center**
   Additional information about AWS certifications, accreditations, security and background information of their services may be found at http://aws.amazon.com/security/#5. From within this site you may obtain an official copy of their Amazon Web Services Overview of Security Processes whitepaper PDF file.

References

³ The NIST Definition of Cloud Computing, 10/07/2009, National Institute of Standards and Technology
⁴ The Datamonitor Group is an independent, premium business information and market analysis company that delivers independent data, analysis and opinion across the technology industry.
⁵ Family Policy Compliance Office (FPCO) Home, 6/16/2009, U.S. Department of Education
⁶ Amazon Web Services; Certifications and Accreditations, 11/27/2009, Amazon.com
⁷ Health Insurance Portability and Accountability Act, 12/01/2009, Wikimedia Foundation, Inc.