fullmeasure

1140 3rd St NE, Suite 330 | Washington, DC 20002 | 202.363.1100 **fullmeasure.io**

Full Measure Education Security Overview

Full Measure Education (FME) understands that the confidentiality and integrity of your student's information is both important to your business operations and vital to our success as a potential partner organization. Through our multi-layered approach, FME protects key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Full Measure Education's software solution, a cloud-based infrastructure, provides a majority of the computing power necessary to configure and implement our system successfully.

Policies and Personnel

Contractual Privacy Protection for Customers

- FME contracts include confidentiality provisions that prohibit us from disclosing private customer information, including customer data, except under narrowly defined circumstances, such as when required by law.
- FME agrees not to access customer's accounts, including student data, except to maintain the service, prevent or respond to technical or service problems, at a customer's request in connection with a customer support issue, or when required by law.
- FME fully intends to comply with all applicable laws, including the Family Educational Rights and Privacy Act (FERPA). To that end, Section 9.2 of FME's Master Agreement provides that if a Customer releases

FERPA covered personally identifiable information ("PII") to FME in connection with FME services, FME shall maintain the confidentiality of such information in accordance with the applicable provisions of FERPA. This includes the obligations of third parties that receive student record PII pursuant to section 99.33 of Title 34 of the Code of Federal Regulations.

- Thus, (i) FME will only use such PII for the purposes for which it was disclosed by the Customer,(ii) only those officers, employees and agents of FME that are authorized to use the PII shall have access to the PII (including authorized independent contractors acting on behalf of FME), and (iii) FME will not disclose the PII to additional third parties without the prior consent of the parent or an "eligible student" (as defined in the FERPA regulations) in accordance with the applicable provisions of FERPA and FERPA regulations.

Confidentiality Agreements, Information Security Policies and Security Awareness

- Every FME employee, contractor or third party partner must comply with confidentiality agreements and FME information security policy.
- FME provides training around confidentiality, privacy, and information security for all new employees during its new hire orientation and tested on the materials presented.
- FME personnel are required to complete an annual privacy and security training.

Technology

Data Security

Data Integration

- Data transport is secured by three layers of redundant security: HTTPS, an API Key, and Secret Key Encryption.
- Scope of student data transported to the cloud is strictly limited to the data required to provide services.

Data in the Cloud

- All cloud infrastructure is hosted with Amazon Web Services in the United States which are designed and managed according to security best practices.
- AWS firewall rules are used to limit access to cloud infrastructure.

- Sensitive student data, including PII is encrypted with AES-256 when at rest.

Network security is the joint responsibility of FME and AWS and conforms to AWS FERPA governed data best practices.

(/https://d0.awsstatic.com/whitepapers/AWS_FERPA_Whitepaper.pdf)

Application features that protect customer data

- Connection to FME services are via secure socket layer/transport layer security (SSL/TLS), ensuring that our customers have a secure connection to their data. Individual user sessions are uniquely identified and re-verified with each transaction.
- Customers passwords are not accessible by FME personnel.

Identity Management

Authentication and Authorization

- Student and staff credential verification through existing institution authentication provider (LDAP, Active Directory, etc).
- Prospective student credentials are managed and verified by FME via one-way encryption.
- Credential verification establishes Identity.
- All user actions require role-based permission check.

Sessions

- All user activity occurs in the context of a session with a unique session token.

Customer-Controlled Privacy and Security Settings

- Customers may determine which of their respective designees can access different categories of data.

Redundancy and Scalability

- All services provided are highly scalable and redundant, allowing for fluctuation in demand and expansion of users while greatly reducing the threat of long-term outages. Load-balanced networks, pools of application servers, and clustered databases are features of our design.
- All customer data is hosted on AWS with hourly database backups. Backups are kept for 30 days before purging.
- Upon termination of contracts, customers are provided with data records necessary for business continuity.