FERPA Compliance on AWS

Resource Guide

March 4, 2022

Notices

Customers are responsible for making their own independent assessment of the information inthis document. This document: (a) is for informational purposes only; (b) represents AWS's current product offerings and practices, which are subject to change without notice; and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This document is designed to assist educational agencies and institutions when running AWS workloads containing educational records subject to the Family Educational Rights and Privacy Act (FERPA). FERPA is a federal law that protects personally identifiable information (PII) in students' education records from unauthorized disclosure, and affords parents and eligible students the right to access and amend education records. This document describes the AWS Shared Responsibility Model and how this model allows for customers to use the AWS services to help them comply with applicable FERPA requirements.

Introduction

The Family Educational Rights and Privacy Act (FERPA) establishes privacy rules for schools and educational agencies that receive funding from the U.S. Department of Education ("Schools"). Importantly, FERPA does not directly regulate third-party contractors of Schools, but prohibits Schools from disclosing student data to contractors unless certain conditions are met.

FERPA provides the following to parents of students and to eligible students (that is, students who have reached the age of 18 or attend school beyond the high school level):

- The right to review the student's education records.
- Governance over disclosure of the student's education records.
- A mechanism with which to amend incorrect education records.

FERPA requires Schools to use reasonable methods to ensure the security of student educational records within their information technology (IT) solutions. The law, in general, requires Schools to reasonably safeguard student education records from improper use or disclosure.

FERPA defines *education records* as "records that are (1) directly related to a student; and (2) maintained by an educational agency or institution, or by a person acting for such agency or institution." These records include but are not limited to transcripts, class lists, and student course schedules.

Securing education records under FERPA is essential for Schools and their IT providers. AWS implements physical and logical controls for internal services, and provides customers with access to security, identity, and compliance services to help them build solutions that comply with FERPA requirements.

AWS offers a comprehensive set of features and services that make encryption of data easier to manage and simpler to audit, including AWS Key Management Service (AWS KMS). Customers with student data privacy compliance requirements have a great deal of flexibility in how they can use AWS to help them meet data encryption requirements.

Our commitment to data privacy

At AWS, earning customer trust is critically important. AWS delivers services to millions of active customers, including enterprises, educational institutions, and government agencies in more than 190 countries. AWS customers include financial service providers, healthcare providers, and governmental agencies, who trust AWS with some of their most sensitive information.

AWS knows that customers care deeply about privacy and data security. That's why AWS gives customers ownership and control over their content through simple, powerful tools that allow customers to determine where their content will be stored, secure their content in transit and at rest, and manage their access to AWS services and resources for customer's users.

AWS also implements sophisticated technical and physical controls designed to prevent unauthorized access to, or disclosure of, customer's content.

AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools customers might require to meet their compliance needs, depending on their applications.

AWS recommends that customers and AWS Partner Network (APN) Partners with general questions about AWS data protection services contact their AWS account manager first. If customers have signed up for enterprise support, they can reach out to their technical account manager (TAM) as well. TAMs work with solutions architects to help customers identify potential risks and mitigations associated with a variety of solutions and deployments. TAMs and account teams can also provide customers and APN Partners with specific resources based on their environment and needs.

Maintaining customer trust is an ongoing commitment. AWS has built important privacy and data security policies, practices, and technologies that include:

- **Access** – Customers maintain control of their content and responsibility for configuring access to AWS services and resources. AWS provides an advanced set of access, encryption, and logging features to help customers do this effectively (for example, AWS Identity and Access Management (IAM), AWS Organizations, and AWS CloudTrail). AWS provides API operations for customers to use to configure access control permissions for any of the services customers develop or deploy in an AWS environment.

- **Storage** – Customers may specify the AWS Regions in which customer content will be stored and the type of storage. Customers can replicate and back up their content in more than one AWS Region.
- **Security** – Customers choose how their content is secured. AWS offers strong security features customers can use to secure their content, in transit and at rest, as well as the option to manage their own encryption keys. These security features include:
    - Data encryption capabilities, available in AWS storage and database services such as Amazon Elastic Block Store, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), and Amazon Redshift.
    - Flexible key management options, including AWS KMS, which allow customers to choose whether to (1) have AWS manage the encryption keys; or (2) keep complete control over their keys.
    - Server-side encryption (SSE) with Amazon S3 managed encryption keys (SSE-S3), SSE with AWS KMS managed keys (SSE-KMS), or SSE with customer-provided encryption keys (SSE-C).
- **Security services** – Customers can implement security features (such as AWS Security Hub, Amazon GuardDuty, Amazon Macie, Amazon Inspector, and Amazon Detective) which can automatically assess applications for exposure, vulnerabilities, and deviations from best practices, and that customers can configure to identify, analyze, and investigate potential security issues or findings.
- **Disclosure of customer content** – AWS does not disclose a customer's information unless required to comply with law or binding government order. If AWS is required to disclose information about a customer's account, Amazon will first notify the customer to the maximum extent permitted by law.
- **Security Assurance** – AWS has developed a security assurance program that uses best practices for global privacy and data protection to help customers operate securely within AWS, and to make the best use of AWS's security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

To learn more about AWS data privacy, refer to the Data Privacy FAQ.

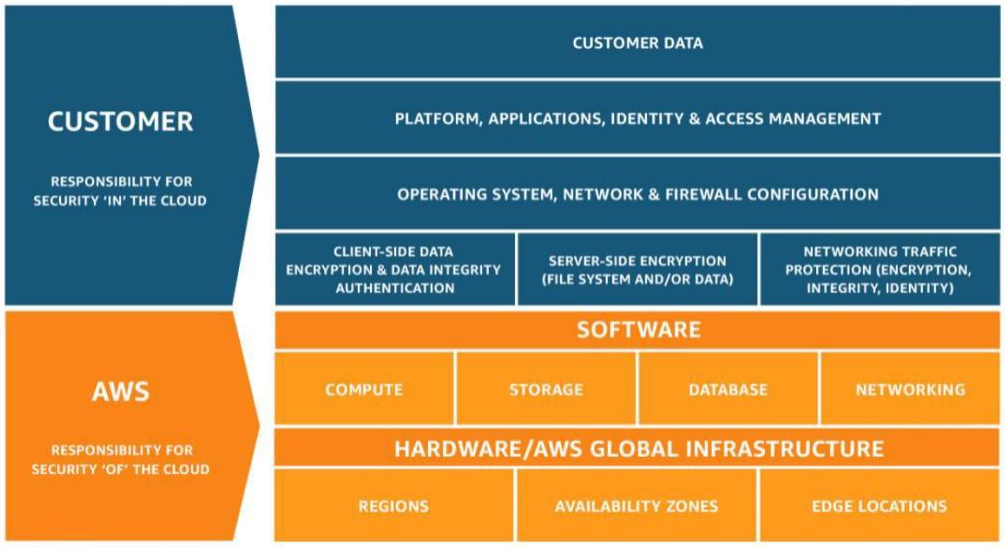
Security of the AWS infrastructure

The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable infrastructure that enables customers to deploy applications and data quickly and securely, and to customize controls to satisfy security requirements, such as those in FERPA.

This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, nearly continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24/7. AWS ensures that these controls are replicated throughout the AWS infrastructure.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and customers are responsible for securing the workloads they deploy in AWS. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles and how a customer can architect a solution in compliance with applicable regulatory standards, including FERPA.

This model gives customers the flexibility and agility they need to implement the most applicable security controls for their business functions in the AWS environment. Customers can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information they want to make public.



AWS Shared Responsibility Model

For more information, refer to Introduction to AWS Security and Shared Responsibility Model.

AWS Artifact

Customers can use AWS Artifact (the automated compliance reporting portal available in the AWS Management Console) to review and download reports and details about more than 2,500 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, as well as certifications and attestations from accreditation bodies across geographies and compliance verticals, including Service Organization Control (SOC) reports, International Organization for Standardization (ISO) reports, Payment Card Industry (PCI) reports, Federal Risk and Authorization Management Program (FedRAMP), FedRAMP Authorization, and Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR), to name a few.

For more information about AWS cloud compliance, refer to AWS Compliance.

AWS Regions

The AWS Cloud is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world that is made up of multiple Availability Zones.

Availability Zones consist of one or more discrete data centers that are housed in separate facilities, each with redundant power, networking, and connectivity. These Availability Zones offer customers the ability to operate production applications and databases at higher availability, fault tolerance, and scalability than would be possible from a single data center. For current information on AWS Regions and Availability Zones, refer to Global Infrastructure.

AWS customers choose the AWS Regions in which their content and servers are located. This allows customers to establish environments that meet specific geographic requirements. For example, AWS customers in the United States can choose to deploy their AWS services exclusively in US Regions and store their content within the continental US, if this is their preferred location.

AWS Regions are designed and built to meet rigorous compliance standards globally, thus providing high levels of security for all AWS customers.

Compliance with FERPA when building on AWS

Educational agencies or institutions that use AWS services to run applications or solutions containing education records have the flexibility to build a solution that secures sensitive information in compliance with applicable regulatory standards, including FERPA. When creating a solution with AWS services, Schools are encouraged to create device compliance policies, threat protection plans, data loss prevention plans, and use encryption and access controls.

AWS offers many tools and services to assist Schools in their implementation of best practices when looking to secure education records in compliance with FERPA. For example, AWS's access controls provide auditing and logging capabilities to customers to validate privacy and data protection policies that customers have in place.

AWS offers a comprehensive set of features and services to make encryption of content including PII simpler to manage and audit; these features and services include AWS KMS. Customers with student data privacy compliance requirements often have a great deal of flexibility in how they meet encryption requirements for PII. The following section provides a high-level overview of services and tools that educational agencies, institutions, and customers should consider as part of their solution built on AWS.

Note: The list of services below is not exhaustive, but covers a wide variety of services that customers can configure to help achieve compliance with FERPA requirements.

Compute

AWS offers multiple compute services, which customers can use to deploy, run, and scale their applications as virtual servers, containers, or code. The following table describes AWS's compute services and directs users to service-specific security information, which explains how those services can be used by customers to help protect their content, which may include education records or PII.

Service	Description	Security documentation
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.	Security in Amazon EC2
AWS Systems Manager	Systems Manager is a management service that helps customers automatically collect software inventory, apply OS patches, create system images, and configure Microsoft Windows and Linux operating systems.	Security in AWS Systems Manager
Amazon Elastic Container Service (Amazon ECS)	Amazon ECS is a highly scalable, high-performance container management service that supports Docker containers and allows customers to efficiently run applications on a managed cluster of Amazon EC2 instances.	Security in Amazon Elastic Container Service
Amazon EMR	Amazon EMR provides a managed Hadoop framework that makes it simple, fast, and cost- effective to process vast amounts of data across dynamically-scalable EC2 instances.	Security in Amazon EMR

Service	Description	Security documentation
Elastic Load Balancing (ELB)	ELB automatically distributes incoming application traffic across multiple EC2 instances.	Security in Elastic Load Balancing
AWS Lambda	AWS Lambda is a serverless, event-driven compute service that lets you run code for virtually any type of application or backend service without provisioning or managing servers.	Security in AWS Lambda

Storage

AWS offers a range of cloud storage services to support both application and archival compliance requirements. Big data analytics, data warehouses, Internet of Things (IoT), databases, and backup and archive applications all rely on some form of data storage architecture.

The following table describes AWS's storage services and directs users to service-specific security information, which explains how those services can be used by customers to help protect their content, which may include education records or PII.

Service	Description	Security documentation
Amazon Simple Storage Service (Amazon S3)	Amazon S3 is an object storage service built to store and retrieve any amount of data from anywhere, such as websites and mobile apps, corporate applications, and data from IoT sensors or devices.	Amazon S3 security
Amazon Elastic Block Store (Amazon EBS)	Amazon EBS is designed to provide persistent block storage volumes for use with EC2 instances in the AWS Cloud.	Amazon EBS User Guide
Amazon Elastic File System (Amazon EFS)	Amazon EFS is designed to provide simple, scalable file storage for use with EC2 instances in the AWS Cloud.	Security in Amazon EFS

Service	Description	Security documentation
Amazon S3 Glacier	Amazon S3 Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup.	Security in Amazon S3 Glacier

Database

AWS offers a wide range of database services to fit users' customer application requirements. These database services can be launched in minutes with just a few clicks. The following table describes AWS's database services and directs users to service-specific security information, which explains how those services can be used by customers to help protect their content, which may include education records or PII.

Service	Description	Security documentation
Amazon DynamoDB	DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale.	Security and Compliance in Amazon DynamoDB
Amazon Redshift	Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze data using standard SQL and existing Business Intelligence tools.	Amazon Redshift security overview
Amazon Relational Database Service (Amazon RDS)	Amazon RDS makes it simple to set up, operate, and scale a relational database in the cloud.	Security in Amazon RDS
Amazon RDS for Oracle		Amazon RDS for Oracle User Guide
Amazon RDS for MySQL		Amazon RDS for MySQL User Guide

Service	Description	Security documentation
Amazon RDS for PostgreSQL	It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. It also saves time for developers to focus on their applications so they can give customers the fast performance, high availability, security, and compatibility they need. Amazon RDS is available on several database instance types (optimized for memory, performance, or input/output (I/O)) and provides users with several familiar database engines, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.	Amazon RDS for PostgreSQL User Guide
Amazon RDS for MariaDB		Amazon RDS for MariaDB User Guide
Amazon Aurora	Amazon Aurora is a MySQL and PostgreSQL–compatible relational database built for AWS Cloud that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases.	Security in Amazon Aurora

Networking and content delivery

AWS networking services are designed to enable customers to isolate their cloud infrastructure, scale their request-handling capacity, and connect their physical network totheir private virtual network. The table below describes AWS's networking services and how those services can be used by customers to help protect their content, which may include education records or PII.

Service	Description	Security documentation
Amazon Virtual Private Cloud (Amazon VPC)	Amazon VPC provides functionality to provision a logically isolated section of the AWS Cloud where customers can launch AWS resources in a virtual network that they define.	Security in Amazon Virtual Private Cloud
Amazon CloudFront	CloudFront is a global content delivery network service that securely delivers data, videos, applications, and APIs to viewers, with low latency and high transfer speeds.	Security in Amazon CloudFront
AWS Direct Connect	Direct Connect makes it simple for customers to establish a dedicated network connection from their premises to AWS. Using Direct Connect, customers can establish private connectivity between AWS and their data center, office, or colocation environment.	Security in AWS Direct Connect

Security, identity, and compliance

Cloud security at AWS is the highest priority. AWS customers benefit from a data center and network architecture built to meet the requirements of the most security-sensitive

organizations. For additional services (other those described in the following table) refer to Security, Identity, and Compliance on AWS. The following table describes AWS security, identity, and compliance services, and how those services can be used by customers to help protect their content, which may include education records or PII.

Service	Description	Security documentation
AWS Identity and Access Management (IAM)	IAM allows customers to securely manage access to AWS services and resources. With IAM, you can manage AWS permissions for workforce users and workloads. For workforce users, we recommend that you use AWS Single Sign-On (AWS SSO) to manage access to AWS accounts and permissions within those accounts. AWS SSO makes it easier to provision and manage IAM roles and policies across your AWS organization. For workload permissions, use IAM roles and policies, and grant only the required access for your workloads.	Security in IAM and AWS Security Token Service
AWS Key Management Service (AWS KMS)	AWS KMS makes it simple for customers to create and manage cryptographic keys and control their use across a wide range of AWS services and in user applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect user keys. AWS KMS is integrated with CloudTrail to provide users with logs of all key usage to help meet their regulatory and compliance needs.	Security of AWS Key Management Service

Service	Description	Security documentation
AWS Shield	AWS Shield is a managed distributed denial of service (DDoS) protection service designed to safeguard web applications running on AWS services. Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.	Security in AWS Shield
Amazon Inspector	Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices.	Security in Amazon Inspector
Amazon Macie	Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect user's sensitive data in AWS.	Security in Amazon Macie
Amazon GuardDuty	Amazon GuardDuty provides threat intelligence and monitoring of a customer's account and VPC resources.	Security in Amazon GuardDuty
AWS Security Hub	AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation.	Security in AWS Security Hub

Information management

AWS encourages Schools to have an up-to-date records retention plan that complies with FERPA requirements. The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a one-stop resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-

level longitudinal data systems and other uses of student data. PTAC provides general guidance and best practices on information management, and these resources can be found at Privacy - Office of Educational Technology.

Auditing

AWS encourages Schools that are subject to FERPA to implement auditing capabilities to allow security analysts to examine detailed activity logs or reports involving education data. The activity logs or reports might allow security analysts to have greater visibility into the individuals or entities that have accessed a School's education data, see the education data that has been accessed, and track IP address entry. The results of the auditing capabilities may then be tracked, logged, and stored in a central location in compliance with a School's data retention policy.

AWS Audit Manager helps customers continuously audit AWS usage and simplify how customers assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to reduce the *all hands-on deck* manual effort that often happens for audits and enable customers to scale their audit capability in the cloud as their business grows. Customers can use additional services like Amazon EC2 or Amazon EMR to process activity log files and audits down to the packet layer on their virtual servers, just as they do on traditional hardware. Customers may also track any IP traffic that reaches their virtual server instance. Administrators can back up the log files into Amazon S3 for long-term reliable storage.

Data destruction

FERPA is silent on specific technical requirements governing data destruction. However, other applicable laws or local privacy regulations may require specific secure data disposal methods. Customers should check with their legal counsel to fully understand their data destruction requirements.

Backup and disaster recovery

Disaster recovery is the process of protecting an organization's data and IT infrastructure in times of disaster. This involves maintaining highly available systems, keeping both the data andsystem replicated off-site, and enabling continuous access to both. AWS offers a variety of disaster recovery mechanisms.

Customers choose the AWS Regions in which their content is stored. They can replicate and back up their content in more than one AWS Region.

AWS Backup is a service designed to allow customers to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed, policy-based service that further simplifies data protection at scale. AWS Backup also enables customers to support their regulatory compliance or business policies for data protection. Together with AWS Organizations, AWS Backup enables customers to centrally deploy data protection policies to configure, manage, and govern their backup activity across their organization's AWS accounts and resources, including EC2 instances, Amazon EBS volumes, Amazon RDS databases (including Aurora clusters), DynamoDB tables, Amazon EFS file systems, Amazon FSx for Lustre file systems, Amazon FSx for Windows File Server file systems, and AWS Storage Gateway volumes.

For more information about disaster recovery, refer to AWS Elastic Disaster Recovery and Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

Conclusion

This document has summarized AWS service capabilities, including security services and tools,which customers can utilize to help them meet data privacy and data security requirements designed to provide protection of education data in compliance with FERPA.

AWS Compliance enables understanding of the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS Cloud infrastructure, compliance responsibilities will be shared. By tying together student data privacymeasures and audit-friendly service features with applicable security compliance regulations or audit standards, AWS Compliance enables customers to build on traditional programs and assists them in establishing and operating in an AWS security control environment.

Contributors

Contributors to this document include:

- Stephen Exley, Industry Specialist, AWS Security

Additional resources

Partner Network

The AWS Partner Network (APN) is the global partner program for AWS. The program focuses on helping APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support.

APN includes AWS Education Competency Partners, which are APN Partners that have demonstrated success in building solutions for educational institutions that securely store, process, transmit, and analyze student information. By working with these AWS Education Competency Partners, customers receive greater access to innovative, cloud-based solutions that have a proven track record for handling educational data. For more information, refer to AWS Education Competency Partners.

NIST guidance on PII

NIST publishes 800 series documents that provide guidance to federal agencies on computer security policies. NIST SP 800-53 Rev 4 and NIST SP 800-122 (April 2010 publication) are part of this family of publications. NIST SP 800-53 is a comprehensive security controls catalog developed for federal agencies, and NIST SP 800-122 is designed to assist federal agencies in protecting confidentiality of PII in information systems. NIST SP 800-122 deals specifically with protection of PII, and NIST SP 800-122 Section 4.3 describes a list of security controls corresponding to PII.

Appendix J of the NIST SP 800-53 (Privacy Control Catalog) provides further guidance on additional controls that customers are encouraged to consider while developing security systems for their organizations.

Further reading

For additional information, refer to:

- AWS Documentation
- AWS Security Documentation
- AWS Compliance
- Amazon Web Services: Overview of Security Processes

- Family Educational Rights and Privacy Act (FERPA) Compliance on AWS
- Family Educational Rights and Privacy Act (FERPA)
- PTAC Best Practices for Data Destruction

Document revisions

Date	Description
March 2022	Global update
September 2021	Global update
December 2017	First publication