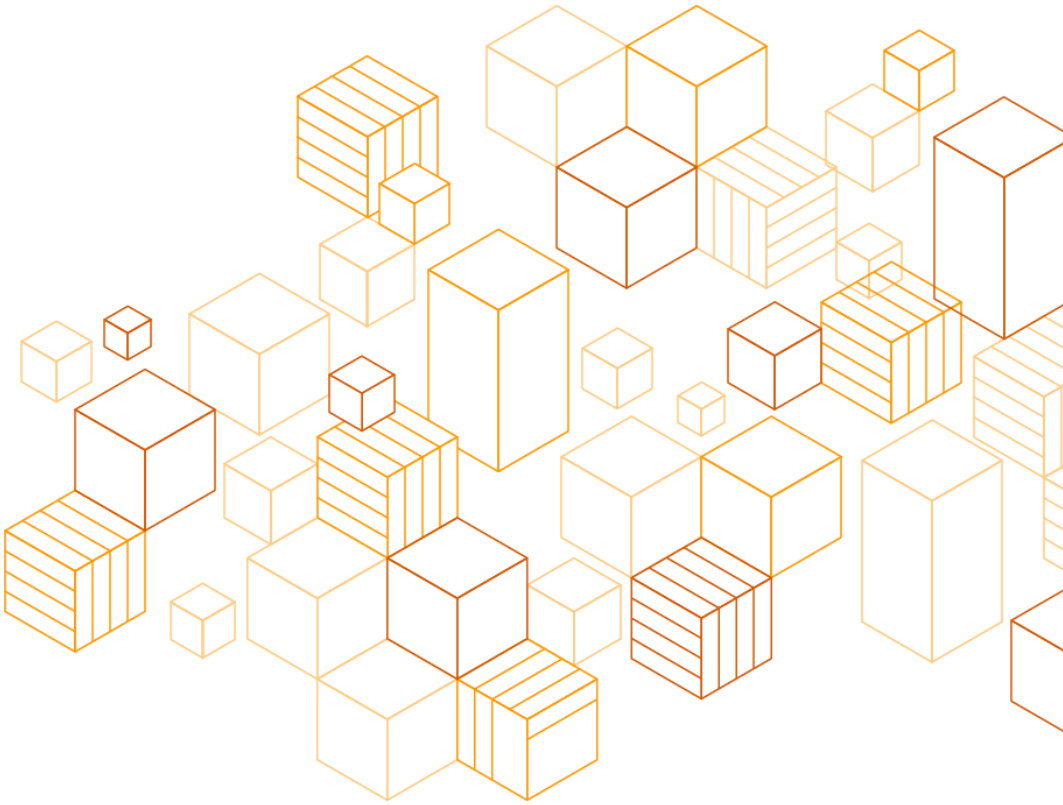
FERPA and Student Data Privacy Compliance on AWS

Resource Guide

September 23, 2021



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS 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

About this Guide

This document is designed to assist educational agencies and institutions that are considering building Family Educational Rights and Privacy Act (FERPA)-compliant workloads on Amazon Web Services (AWS). This document provides an overview of the AWS security and service capabilities (including security services and tools) that customers can utilize to help them meet data privacy and data security requirements under FERPA and other student data privacy laws and regulations.

Introduction

The FERPA of 1974 was enacted to support and promote the protection of privacy and reasonable governance of student education records.

FERPA provides the following to eligible students (i.e. students who have reached the age of 18 or who attend school beyond the high school level) and parents of all other students:

- 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 educational agencies and institutions to use reasonable methods to ensure the security of their information technology (IT) solutions. The law, in general, requires covered institutions and agencies to reasonably safeguard student education records from improper use or disclosure. FERPA defines "education records" as "records, files, documents, and other materials that are maintained by an educational agency or institution, or by a person acting for such agency or institution." Education records also include any record that pertains to an individual's previous attendance as a "student of an institution."

Securing student record information, including students' personal information , is essential for educational institutions and vendors that provide them with services which fall under the purview of FERPA and state student data privacy laws.

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

Our commitment to data privacy

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

We know that customers care deeply about privacy and data security. That's why AWS gives you ownership and control over your content through simple, powerful tools that allow you to determine where your content will be stored, secure your content in transit and at rest, and manage your access to AWS services and resources for your users. We also implement sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of your content.

AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might require to meet their compliance needs, depending on their applications. We recommend 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. TAMs and account teams can also provide customers and APN Partners with specific resources based on their environment and needs. AWS is not in the position to provide legal advice. We recommend that customers consult their legal counsel if they have legal questions.

Maintaining customer trust is an ongoing commitment. We strive to inform you of the privacy and data security policies, practices, and technologies we've put in place. These commitments include:

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

- **Storage** – You choose the AWS Regions in which your content is stored and the type of storage. You can replicate and back up your content in more than one AWS Region.

- **Encryption** – We offer you strong encryption for your content, in transit and at rest, as well as the option to manage your own encryption keys. These 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 you to choose whether to 1. Have AWS manage the encryption keys or 2. Keep complete control over your 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** – You can choose security services which can automatically assess applications for exposure, vulnerabilities, and deviations from best practices, and which you can configure to identify, analyze, and investigate potential security issues or findings, such as AWS Security Hub, Amazon GuardDuty, Amazon Macie, Amazon Inspector, and Amazon Detective.

- **Disclosure of customer content** – We do not disclose your information unless we're required to do so in order to comply with a legally valid and binding order. Unless prohibited from doing so, or if there is clear indication of illegal conduct in connection with the use of AWS products or services, AWS notifies you before disclosing content information.
- **Security Assurance** – We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our 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, see our 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.

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 in every new data center or service.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of our most security-sensitive customers. This means that you get a resilient infrastructure designed for high security, without the capital outlay and operational overhead of a traditional data center.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and you are responsible for securing workloads you deploy in AWS. This gives you the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information you want to make public.

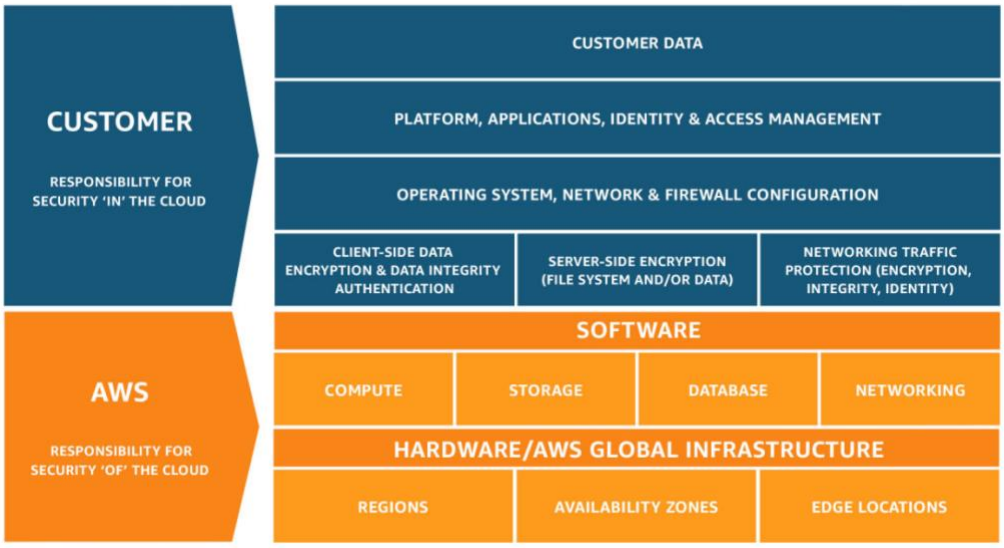


Figure 1 – AWS Shared Responsibility Model

For more information, see 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, see AWS Compliance.

AWS Regions

The AWS Cloud infrastructure 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, see Global Infrastructure.

AWS customers choose the AWS Region(s) 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 (US) can choose to deploy their AWS services exclusively in the US Regions and store their content on shore in the US, if this is their preferred location. If the customer makes this choice, their content will be located in US unless they choose to move that content.

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 and Student Data Privacy Laws when Building on AWS

Because FERPA was authored in 1974, it lacks clear guidance on modern technology use, which means that educational institutions are often left to create their own solutions. While some US state student data privacy laws and regulations are more prescriptive, the specific technical requirements vary by US state and are heavily dependent on the customer's security controls and system configuration.

As part of this solution, customers are encouraged to take steps such as: using encryption and access controls, and creating device compliance policies, threat protection plans, and data loss prevention plans, suitable for their organization, that protect sensitive information. Access controls also provide auditing and logging capabilities to customers in order 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 PII simpler to manage and audit; these features and services include the 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 student data privacy requirements.

Compute

AWS offers multiple compute products, which customers can use to deploy, run, and scale their applications as virtual servers, containers, or code.

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)	Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure 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 you 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 Amazon EC2 instances.	Security in Amazon EMR
Elastic Load Balancing (ELB)	ELB automatically distributes incoming application traffic across multiple Amazon EC2 instances.	Security in Elastic Load Balancing

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, databases, and backup and archive applications all rely on some form of data storage architecture.

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

Service	Description	Security Documentation
Amazon Elastic Block Store (EBS)	Amazon EBS is designed to provide persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.	Amazon Elastic Block Store (EBS) - User Guide
Amazon Elastic File System (EFS)	Amazon EFS is designed to provide simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud.	Security in Amazon EFS
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 customers' application requirements. These database services can be launched in minutes with just a few clicks.

Service	Description	Security Documentation
Amazon DynamoDB (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 (BI) tools.	Getting Started with Amazon Redshift

Service	Description	Security Documentation
Amazon Relational Database Service (Amazon RDS) Amazon RDS for Oracle Amazon RDS for MySQL Amazon RDS for PostgreSQL Amazon RDS for MariaDB	Amazon RDS makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. It also frees you to focus on your applications so you can give them 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 you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.	Security in Amazon RDS Amazon RDS for Oracle User Guide Amazon RDS for MySQL User Guide Amazon RDS for PostgreSQL User Guide Amazon RDS for MariaDB User Guide
Amazon Aurora	Amazon Aurora is a MySQL and PostgreSQL-compatible relational database, built for the cloud, which combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases.	Security in Amazon Aurora

Networking and Content Delivery

AWS networking products are designed to enable customers to isolate their cloud infrastructure, scale their request-handling capacity, and connect their physical network to their private virtual network.

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

Service	Description	Security Documentation
Amazon CloudFront (CloudFront)	CloudFront is a global content delivery network (CDN) 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)	Direct Connect makes it easy 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 our 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 beyond those described below, see: Security, Identity, and Compliance on AWS.

Service	Description	Security Documentation
AWS Identity and Access Management (IAM)	AWS IAM enables you to securely manage access to AWS services and resources. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny *their access* to AWS resources.	Security in IAM and AWS STS

Service	Description	Security Documentation
AWS Key Management Service (KMS)	AWS KMS is a managed service that makes it easy to create and control the encryption keys used to encrypt data, and uses Hardware Security Modules (HSMs) to protect the security of keys. AWS KMS is integrated with several other AWS services to help customers protect the data that they store with these services. AWS KMS is also integrated with AWS CloudTrail to provide customers with logs of all key usage to help meet their regulatory and compliance needs.	Security of AWS Key Management Service
AWS Shield	AWS Shield is a managed Distributed Denial of Service (DDoS) protection service designed to safeguard web applications running on AWS. AWS 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 your 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

Information Management

While FERPA does not require a records retention plan, it does have a direct impact on access to and use of existing records. Therefore, AWS encourages organizations to have an up-to-date records retention plan that complies with FERPA requirements. Privacy Technical Assistance Center (PTAC) has provided general guidance and best practices on information management and these resources can be found at Privacy - Office of Educational Technology.

Auditing

While FERPA does not specifically require formal audits, customers should put auditing capabilities in place to allow security analysts to examine detailed activity logs or reports to see information like who had access, IP address entries, what data was accessed, etc. This data may then be tracked, logged, and stored in a central location in compliance with an educational institution's data retention policy.

AWS Audit Manager helps customers continuously audit AWS usage and simplify how you 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 you to scale your audit capability in the cloud as your business grows. Customers can use additional services like Amazon EC2 or 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 does not require particular methods of 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. Within AWS media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST Special Publication (SP) 800-88, Revision 1, , "Guidelines for Media Sanitization." Media that stored customer data is not removed from AWS control until it has been securely decommissioned. Additionally, customers can always use encryption on their data to better that only authorized key material holders may decrypt the data.

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 and system replicated off-site, and enabling continuous access to both. AWS offers a variety of disaster recovery mechanisms.

For more information about disaster recovery, see http://aws.amazon.com/disaster-recovery.

Additional Resources:

Partner Network

APN is the global partner program for AWS. It is focused on helping APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support.
AWS Education Competency Partners have demonstrated success in building solutions for educational institutions that securely store, process, transmit, and analyze student information. Working with these Competency Partners gives you access to innovative, cloud-based solutions that have a proven track record for handling educational data. For more information, see 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. Section 4.3 of this document describes a list of security controls corresponding to PII.
Appendix J of NIST SP 800-53 document, Privacy Controls Catalog, provides further guidance on additional controls that customers are encouraged to consider while developing security systems for their organizations.

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 privacy measures and audit-friendly service features with applicable security compliance regulations or audit standards, AWS Compliance enables you to build on traditional programs and assists you in establishing and operating in an AWS security control environment.

Contributors

Contributors to this document include:

- Stephen Exley, Industry Specialist, AWS Security

- Patrick Woods, Principal Security Specialist, AWS Security

Further Reading

For additional information, see:

- 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)

Document Revisions

Date	Description
September 2021	Updated information throughout.
December 2017	First publication