FERPA Compliance on AWS

Resource Guide

July 2024

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 Amazon Web Services (AWS) 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 expressed 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 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.

Schools are required to use reasonable methods to ensure the security of student educational records within their information technology (IT) solutions and to 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.

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 200+ countries and territories. 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 KMS, and AWS CloudTrail). AWS provides Application Program Interface (API) operations for customers to use to configure access control permissions for any of the services customers develop or deploy in an AWS environment.

- **Locality** – Customers may specify the AWS Regions from across the globe in which their workloads (content and services) will be stored and operated. Customers can replicate and back up their content in more than one AWS Region or AWS Availability Zone.
- **Security** – At AWS, security is our top priority. We have a shared responsibility model with the customer; AWS manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate, and AWS customers are responsible for building secure applications. Customers choose how their content is secured. AWS helps organizations to develop and evolve security, identity, and compliance into key business enablers. AWS is architected to be the most flexible and secure global cloud infrastructure on which to build, migrate, and manage applications and workloads.
- **Security services** – Customers can implement security services. For example 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. These security services support customers in the identification, analysis, and investigation of 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

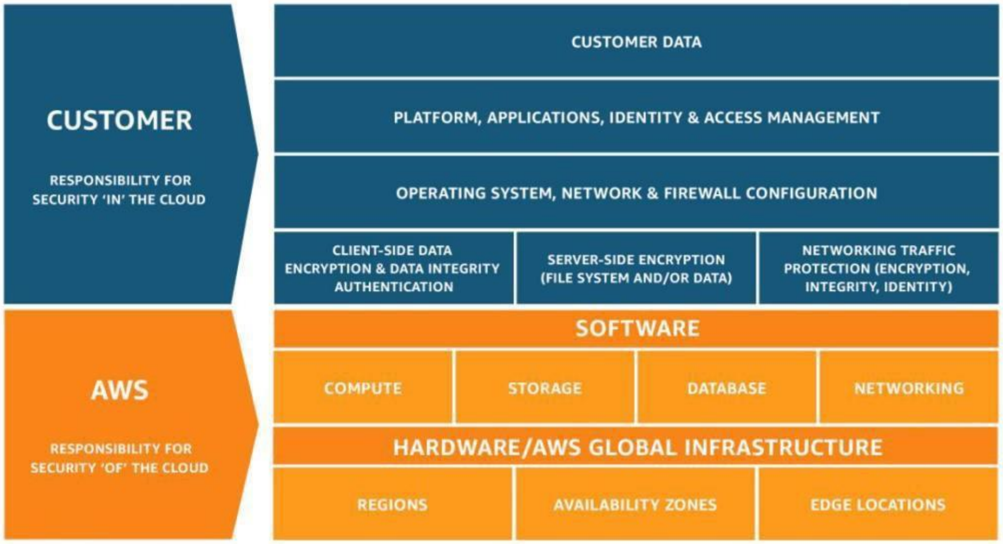
The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable infrastructure that enables customers to deploy applications and data quickly and securely, and to customize 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 (of the cloud) and customers are responsible for securing the workloads, they deploy in AWS (in the cloud). The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security principles and how a customer can architect a solution in compliance with applicable regulatory requirements, 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.


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

AWS Shared Responsibility Model

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

Enabling Compliance with FERPA on AWS

AWS provides a secure cloud computing environment and services that enable educational institutions to implement controls and safeguards to protect the confidentiality of student education records as required by FERPA. While FERPA does not certify or designate solutions as "compliant," AWS offers robust security services and features that can help schools meet FERPA's data protection requirements.

Some key ways AWS supports FERPA alignment include:

- Encryption services (AWS Key Management Services (KMS), AWS CloudHSM) to encrypt data at rest and in transit.
- Access control mechanisms (AWS Identity and Access Management (IAM), resource policies, security groups, and network access control list) to restrict access to authorized users.
- Auditing and logging capabilities (AWS CloudTrail, Amazon Virtual Private Cloud (VPC) flow logs) to monitor access.
- Data residency controls to store data in specific regions/locations.
- Guidance whitepapers on architecting and implementing well-architected secure solutions.
- AWS enables schools to implement industry best practices for securing sensitive student data, while providing the scalability, reliability, and breadth of services beneficial for education technology solutions. However, responsibility remains with the institution to configure AWS services appropriately to meet FERPA's requirements. Below we will briefly discuss some of the resources that can support this effort.

AWS Regions & Services

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 workloads (content and services) 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.

Security, Identity, & Compliance

AWS offers a wide range of services that help enable customers to align their cloud solutions with FERPA through the implementation of security, identity, and compliance capabilities. These can generally be categorized as identity and access management, detection and response, network and application protection, data protection, and compliance services. These services provide robust and scalable capabilities for securely managing and protecting sensitive data, while also enabling customers to demonstrate their compliance with regulatory requirements and standards through comprehensive monitoring, logging, and reporting capabilities. AWS encourages organizations that are subject to FERPA to implement these capabilities which allow security analysts to examine detailed activity logs and reports involving education data services and to support demonstration of their compliance to FERPA student information privacy requirements.

The services below provide a brief discussion of only some of the AWS services that support customers to meet their security, identity, and compliance needs.

- AWS Artifact provides on-demand access to AWS' security and compliance reports, enabling customers to assess the compliance status of their AWS environment and demonstrate adherence to regulations. 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.

- AWS Audit Manager is a service that helps organizations continuously audit their AWS usage to simplify how they assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection and makes it easier to manage and scale audits across an entire AWS environment.
- AWS CloudTrail is an AWS service that helps customers enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service (via API calls) are recorded as events in CloudTrail. Logging and monitoring with AWS CloudTrail help customers demonstrate alignment to regulatory record-keeping requirements.
- AWS Config continuously monitors and records resource configurations, allowing organizations to assess their compliance status and identify any deviations from desired configurations. AWS Config enables organizations to assess, audit, and evaluate the configurations of their AWS resources, ensuring that they comply with regulations and best practices for data protection.
- Amazon EC2 or Amazon Elastic Map Reduce (EMR) allow customers to process activity log files and audit files down to the packet layer on their virtual servers just as they do on traditional hardware.
- AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior, helping customers to protect their systems and sensitive data from potential threats.
- AWS Identity and Access Management (IAM) allows customers to create and manage user identities and access permissions, ensuring that only authorized personnel can access student data.

- AWS Key Management Service (KMS) enables customers to create, manage, and control cryptographic keys across their applications and AWS services to encrypt sensitive student information at rest and in transit, protecting it from unauthorized access.
- AWS Security Hub provides a comprehensive view of the security and compliance status of AWS accounts, helping schools identify and remediate potential security risks and compliance issues related to FERPA.
- The AWS Well-Architected Tool provides guidance and best practices to help customers design and operate secure, efficient, and cost-effective systems in the cloud. While the framework itself does not directly address compliance with specific regulations like FERPA, it can help customers align their cloud architecture with FERPA requirements. The framework's Security pillar emphasizes the importance of data protection, identity and access management, and incident response, which are crucial for safeguarding student records and personal information as required by FERPA. Additionally, the Operational Excellence pillar promotes the implementation of processes and procedures to ensure ongoing compliance, monitoring, and continuous improvement, which can aid in maintaining FERPA compliance over time.

By leveraging these AWS Security, Identity, and Compliance services, customers can ensure that they align their solutions with FERPA student information privacy requirements. These services, along with other AWS security and compliance offerings, enable organizations to maintain visibility, control, and accountability over their AWS resources and activities. They provide a comprehensive set of tools to streamline auditing processes, automate evidence collection, and ensure compliance with various regulations and standards such as FERPA.

For more information, refer to Security, Identity, and Compliance on AWS.

Compute

AWS offers a wide range of compute options to meet various workload requirements. For instance, Amazon Elastic Compute Cloud (EC2) provides scalable virtual servers in the cloud, allowing users to launch and manage instances with different configurations of compute, memory, storage, and networking resources. AWS Lambda is a serverless computing service that runs code in response to events or HTTP requests, eliminating the need to manage servers. Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS) enable users to deploy and manage containerized applications at scale. AWS Outposts brings AWS compute and storage services to on-premises facilities, while AWS Batch and AWS Parallel Cluster provide managed batch processing and high-performance computing (HPC) capabilities, respectively. Additionally, AWS offers specialized compute options like AWS Inferentia for machine learning inference and AWS Graviton for Arm-based workloads.

The above is not a comprehensive list. However, each of these AWS compute services are designed with robust security features and controls, enabling customers to build and operate secure solutions that align with FERPA requirements for protecting student data. Services like EC2, Lambda, ECS, and EKS provide encryption, access controls, network isolation to safeguard sensitive student information. AWS Outposts extends these security capabilities to on-premises environments, ensuring alignment with FERPA requirements.

For more information about each of AWS compute service offerings, refer to Compute for any workload.

Storage

AWS offers a range of cloud storage services that can assist educational institutions in building solutions that comply with FERPA. One key service is Amazon Simple Storage Service (Amazon S3), which provides secure, durable, and scalable object storage. S3 offers features like server-side encryption, access control lists, and bucket policies that can be configured by the customer to help protect sensitive student data. Another relevant service is Amazon Elastic File System (Amazon EFS), a fully managed, scalable file system that can be used to store and share student files and documents securely. EFS supports encryption at rest and in transit, ensuring that student data remains protected while being accessed or transferred. These are just a couple of the AWS storage services available.

The benefits of using AWS storage services include customer configurable data protection through robust security features like encryption, access controls, and auditing capabilities to safeguard sensitive student data. Additionally, the scalability and durability of these services allow schools to store and manage growing volumes of student data without worrying about capacity limitations or data loss. By leveraging AWS storage services, educational institutions can build robust, scalable, and secure solutions that meet FERPA requirements for protecting student privacy and data confidentiality.

For more information about AWS storage options, refer to Cloud Storage on AWS.

Database

AWS offers a comprehensive suite of database services that can assist schools in aligning their solutions with FERPA student information privacy requirements. Services like Amazon Relational Database Service (RDS), Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, and Amazon Redshift provide robust security features such as encryption at rest and in transit, network isolation through Virtual Private Cloud (VPC), and granular access control mechanisms integrated with AWS Identity and Access Management (IAM). These features enable schools to protect sensitive student data from unauthorized access and ensure alignment with FERPA.

Moreover, the AWS Database Migration Service (DMS) allows schools to securely migrate their existing databases to the AWS cloud while maintaining encryption and access controls throughout the migration process. By leveraging these AWS database services and implementing best practices for data security and access management, schools can create secure solutions for storing and managing student information.

For more information, refer to AWS Cloud Databases.

Networking and content delivery

AWS networking and content delivery services can help schools align their solutions with FERPA student information privacy requirements in several ways. For instance, VPC and security groups can be used to create isolated networks and control access to sensitive student data. AWS PrivateLink allows secure communication between VPCs and AWS services without exposing data to the public internet. AWS Web Application Firewall (WAF) can protect web applications from common web exploits that could lead to data breaches. Amazon CloudFront, a content delivery network (CDN), can cache and distribute content securely, reducing the need to store sensitive data across multiple locations. AWS also offers encryption services like AWS Key Management Service (KMS) and AWS Certificate Manager (ACM) to protect data in transit and at rest. These are just a few of the AWS Networking and Content Delivery services that customers can leverage and configure to ensure their solution is in alignment with FERPA's data security requirements.

For more information, refer to AWS Networking and Content Delivery.

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.

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.

However, the most common concerns related to data destruction often involve EC2 instance and S3 buckets. AWS provides various mechanisms to ensure data destruction when you release a virtual instance or delete an S3 bucket. For Elastic Block Store (EBS) volumes attached to EC2 instances, AWS offers secure data deletion by overwriting the data with random patterns before deleting the volume. For instance, storage volumes, AWS automatically overwrites the data with zeros before terminating the instance. For S3 buckets, AWS ensures that all data and metadata are securely deleted and cannot be recovered once you delete the bucket. More importantly, AWS provides encryption options like AWS Key Management Service (KMS) and Server-Side Encryption (SSE) to protect data at rest and in transit, ensuring that even if data is not securely deleted, it remains encrypted and inaccessible without the appropriate keys.

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.

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 Elastic Block Store (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.

Note: Each customer solution is unique and will require a variety and mix of services that customers can configure to help achieve alignment with FERPA requirements. Refer to AWS Cloud Products for a comprehensive list of services and for detailed information about a specific service.

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 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:

- Robert Siple, Security Assurance Specialist, AWS Security Assurance
- Stephen Exley, Security Industry Specialist, AWS Security Assurance
- Kevin Murakoshi, Principal Solution Architect, AWS WWPS EDU/SLG
- Abhijeet Lokhande, Sr. Solution Architect, AWS WWPS EDU/SLG
- Brian Galloway, Security Leader, AWS WWPS EDU/SLG

Additional Resources

AWS Partner Network (APN)

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.

AWS Managed Services (AMS)

AWS Managed Services (AMS) helps you adopt AWS at scale and operate more efficiently and securely. We leverage standard AWS services and offer guidance and execution of operational best practices with specialized automations, skills, and experience that are contextual to your environment and applications. AMS provides proactive, preventative, and detective capabilities that raise the operational bar and help reduce risk without constraining agility, allowing you to focus on innovation. AMS extends your team with operational capabilities including monitoring, incident management, AWS Incident Detection and Response, security, patch, backup, and cost optimization. AWS Incident Detection and Response is available in English for workloads hosted in eligible AWS regions.

For more information, refer to AWS Managed Services.

AWS Professional Services (ProServe)

Adopting the AWS Cloud can provide organizations with sustainable business advantages. Supplementing your team with specialized skills and experience can help you achieve those results. The AWS Professional Services is a global team of experts that can help customers realize their desired business outcomes when using the AWS Cloud. ProServe works with your team and your chosen member of the AWS Partner Network (APN) to execute and realize your enterprise cloud computing initiatives.

For more information, refer to AWS Professional Services.

NIST guidance on PII

NIST publishes 800 series documents that provide guidance to federal agencies on computer security policies. NIST SP 800-122 (April 2010) and NIST SP 800-53 are part of this family of publications. NIST 800-122 provides guidance on protecting confidentiality of PII in information systems. Section 4.3 describes a list of security controls corresponding to PII. The NIST SP 800-53 Rev.5 Personally Identifiable Information Processing and Transparency (PT) control family addresses processing of PII and provides further guidance on additional controls that customers are encouraged to consider while developing information systems for their organizations.

Additional privacy control mappings from NIST SP 800 Rev. 4 Appendix J to Rev. 5 can be found in Mapping: Appendix J Privacy Controls (Rev.4) to Rev. 5.

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
July 2024	Global update
March 2022	Global update
September 2021	Global update
December 2017	First publication