EBOOK

Ensuring FERPA Compliance With Wasabi

wasabi
hot cloud storage

Table of Contents

wasabi

Executive Overview

Wasabi is an affordable and fast cloud storage service. K-12 school systems, colleges and universities can use Wasabi hot cloud storage for a variety of purposes including primary storage, secondary storage for backup or disaster recovery, and cold storage for data archival. Wasabi is ideal for maintaining and storing a wide variety of education application data and content including electronic student records.

The U.S. Family Educational Rights and Privacy Act (FERPA) regulates access to student education records, imposing strict requirements on how electronic records are stored and protected. The Federal Government does not provide formal FERPA compliance auditing or certification processes. Instead, academic institutions are responsible for ensuring their IT systems and practices comply with the FERPA statute.

School districts and post-secondary institutions can use Wasabi to store and maintain electronic student education records in accordance with the FERPA mandate. Wasabi provides strong data privacy, security and integrity to ensure proper protection of electronic records. In addition Wasabi's Terms of Use Agreement ensures institutions maintain exclusive ownership of electronic records as required by FERPA.

This white paper provides an overview of the Family Educational Rights and Privacy Act and explains how Wasabi helps academic institutions comply with FERPA regulations for safeguarding the privacy of electronic student records.

Introduction – Family Educational Rights And Privacy Act Overview

FERPA is a U.S. federal law that protects the privacy of student education records. The law applies to all public and private schools that receive funds from the U.S. Department of Education, including K-12 schools and post-secondary institutions (colleges, universities, trade schools, vocational schools, etc.)

FERPA gives parents certain rights over a child's education records, which are in turn transferred to the student when he or she turns 18 or enrolls in a post-secondary school. In particular, FERPA gives parents and eligible students:

- The right to inspect and review their education records
- A formal remediation process to amend incorrect records
- Control over the disclosure of their education records

As a general rule, schools must have written permission from a parent or eligible student in order to disclose any personally identifiable information (PII) from a student's education record. Personally identifiable information includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

Wasabi Hot Cloud Storage Overview

Wasabi hot cloud storage is affordable, fast and reliable cloud object storage—for any purpose. Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi hot cloud storage is easy to understand and implement, and cost-effective to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Academic institutions can use Wasabi for:

- Low-cost primary storage for on-premises or cloud-based workloads
- Economical secondary storage for backup, disaster recovery in the cloud, or data migration initiatives
- Affordable and reliable archival storage for long-term data retention

Wasabi hot cloud storage is ideal for a wide variety of **education applications** including:

- Electronic records including student education records
- Content management systems
- Digital educational and online learning materials and video files
- Big data for academic research
- Campus security video
- Digital media for sporting events, fine arts performances, and speaking events
- Student and business analytics

4

Ensuring FERPA Compliance With Wasabi Hot Cloud Storage

School districts and post-secondary institutions can use Wasabi to store and maintain electronic student education records in accordance with FERPA regulations. The Wasabi cloud storage service is engineered to ensure the protection, privacy and integrity of customer data. The service is built and managed according to security best practices and standards, with U.S. Department of Education PTAC data security guidelines in mind.

Wasabi takes a "defense-in-depth" approach, employing multiple layers of security for ultimate protection in accordance with PTAC recommendations. Wasabi ensures the physical security of its data centers; institutes strong authentication and authorization controls for all its cloud compute, storage and networking infrastructure; and encrypts data at rest and in transit to safeguard confidential student information.

Physical Security

The Wasabi service is hosted in premier top tier data center facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance. Wasabi's products are also certified for ISO 27001 compliance, providing further assurance of the quality and security of Wasabi's storage regions and its products. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to Wasabi infrastructure and services.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and account security capabilities to prevent unauthorized disclosure of electronic education records. Access control lists (ACLs) and identity access management (IAM) policies selectively grant permissions to users or groups of users. These policies ensure that users only have access to the resources and actions they need, supporting least-privilege principles at scale. For enterprise environments leveraging existing identity providers, Single Sign-On (SSO) integration with solutions like Okta and Azure Active Directory allows for streamlined, secure user management without compromising usability.

Logs for account access and audit trails are maintained for robust incident response plans, both within Wasabi and to provide customers with the records they need to mitigate disruption in the case of an event. Multi-factor authentication (MFA) strengthens identity verification by requiring users to authenticate with a time-sensitive code generated on a trusted device, such as a smartphone. This ensures that access is granted only when both identity and possession factors are satisfied.

Wasabi encrypts data at rest and data in transit to prevent record leakage. All data stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect data in transit. Additionally, automatic logouts are applied to accounts with adjustable ranges for management to dictate access based on industry requirements.

Data Durability and Protection

Wasabi hot cloud storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone—including Wasabi. Wasabi data immutability protects the integrity of electronic student education records, mitigating the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Data Ownership and Disclosure

FERPA permits schools to use cloud services like Wasabi, but only if the school maintains direct control over the service provider's use and maintenance of education records. To that end, the Wasabi Storage Platform Terms of Use Agreement grants the school exclusive ownership and control of stored data. Under the terms of the agreement the subscriber (the academic institution) maintains ownership of all subscriber data. All data stored on Wasabi remains the exclusive and confidential property of the subscriber.

Customer Responsibilities

Wasabi customers typically interface with the Wasabi service using third-party file management applications and backup tools. To ensure FERPA compliance, IT personnel must ensure the storage management tools and applications they use are configured to take advantage of Wasabi security features. For example, HTTPS must be enabled to encrypt data in transit.

IT organizations must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure. The Wasabi storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage and networking components.

6

Additional Considerations

It is important to keep in mind that FERPA may not be the only statute regulating the security and privacy of electronic education records and data transactions. Academic institutions may need to comply with other federal and state data privacy laws, such as the Healthcare Insurance and Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS) that impose additional security requirements.

Conclusion

FERPA introduces stringent data privacy and security requirements for school districts and post-secondary institutions. The Federal Government does not provide formal FERPA certification mechanisms, so the onus is on every academic institution to ensure its IT systems and practices are compliant.

Wasabi's cloud storage service ensures the protection, privacy and integrity of electronic student education records, helping institutions comply with the FERPA statute. Wasabi ensures the physical security of its data centers, employs strong authentication and authorization controls to safeguard infrastructure and services, and encrypts data at rest and in transit to prevent unauthorized record disclosure.

Wasabi is typically used in conjunction with other compute, storage and networking platforms and services. IT organizations must implement strong security systems and practices across all on-premises and cloud-based infrastructure to fully protect electronic student education records.

Additional Information

For additional information about FERPA and Wasabi consult the following resources:

- U.S. Department of Education FERPA website
- U.S. Department of Education Privacy Technical Assistance Center website

About Wasabi

Wasabi provides simple and affordable hot cloud storage for businesses all over the world. It enables organizations to store and instantly access an unlimited amount of data with no complex tiers or egress or API fees, delivering predictable costs that save money and industry leading security and performance businesses can count on. Trusted by customers worldwide, Wasabi has been recognized as one of technology's fastest-growing and most visionary companies. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is a privately held company based in Boston. Wasabi is a Proud Partner of the Boston Red Sox, and the Official Cloud Storage Partner of Liverpool Football Club and the Boston Bruins.

Follow and connect with Wasabi on Linkedin, X, Facebook, Instagram, and The Bucket.