FERPA Compliance

CrashPlan

TECH OVERVIEW

CrashPlan supports customer compliance with Family Educational Rights and Privacy Act (FERPA) requirements, giving organizations the critical data backup and recovery needed for safeguarding protected information and protecting that data from loss. In addition, CrashPlan provides a powerful data protection foundation that contributes to a long-term FERPA compliance strategy and prepares organizations to meet evolving regulations and complex compliance requirements.

What is FERPA?

FERPA is a U.S. federal privacy law that gives parents certain protections with regard to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information and class schedules.

FERPA applies to all educational agencies and institutions that receive funding under any program administered by the Department of Education. These institutions are required to ensure that third parties, like CrashPlan, that store or process protected information comply with FERPA requirements.

CrashPlan and FERPA

Unlike HIPAA and other similar federal regulations, FERPA does not require specific security controls. However, FERPA requires that information stored as part of their educational records will be kept confidential and disclosed only with permission or under provisions of the law. Additionally, students have the right to know about the purpose, content and location of information kept as part of their educational records.

How CrashPlan Gives You Control of Your Data

CRASHPLANS ENDPOINT DATA BACKUP AND RECOVERY SOLUTION DELIVERS SEVERAL KEY FUNCTIONS THAT PLAY A VITAL ROLE IN SUPPORTING FERPA COMPLIANCE:

- **Secure and protect your endpoint data.** Your employees, students and end users create and move an incredible amount of data on a daily basis. End users are creating, modifying, deleting data every second, on their laptops and in the cloud. Employees are being onboarded, enabled, empowered and offboarded, all in a remote world. CrashPlan gives you the ability to backup and recover all data that lives on your endpoints. This is the starting point of a comprehensive data security and data control strategy that supports FERPA compliance.
- **Maintain complete data security.** We protect customer data with end-to-end encryption: 256-bit AES encryption to secure data at rest and 256-bit AES Transport Layer Security (TLS) 1.2 encryption to secure all data in transit, utilizing FIPS 140-2 validated modules.

For most of today's businesses, your data IS your business. CrashPlan features protect your data from natural disasters, ransomware attacks, coffee spills, and even that employee that quits and deletes the team folder on the way out.

CrashPlan

Corporate Headquarters
400 S 4th St Suite 410
PMB 31083
Minneapolis, MN 55415-1419
612.464.2112

crashplan.com

CrashPlan® provides peace of mind through secure, scalable, and straightforward endpoint data backup. We help organizations recover from any worst-case scenario, whether it is a disaster, simple human error, a stolen laptop, ransomware or an as-of-yet undiscovered calamity. We continue to innovate as the landscape of work evolves, which makes CrashPlan foundational to organizations' data security. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds.

For more information, visit **crashplan.com**.