

FERPA Compliance

Our Insider Risk Management solution, Incydr, supports customer compliance with Family Educational Rights and Privacy Act (FERPA) requirements, giving organizations the critical data risk detection and response capabilities as well as data preservation needed for safeguarding protected information and protecting that data from improper disclosure. In addition, Incydr 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 Incydr, that store or process protected information comply with FERPA requirements.

Incydr 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 Incydr gives you control of your data

Incydr's endpoint data protection solutions deliver 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. This data can sit outside the traditional perimeter and beyond the visibility of traditional data security tools. Incydr gives you visibility to data exfiltration across a variety of vectors and protection against insider risk. 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.
- ▶ **Gain visibility, monitor data movement and spot risk sooner:** At Incydr, we believe FERPA compliance is about more than checking boxes; it's about choosing solutions that enable your organization to mitigate the risk of protected information falling into the wrong hands. With Incydr you have the ability to detect, mitigate and respond to data exfiltration and insider risks.

See how your users move data across vectors—including web browser uploads, cloud sync activity, cloud file sharing, email, and use of removable media. Leverage this powerful data visibility to enable a proactive and intelligent approach to data security and protection. Establish baselines of normal individual user behavior and detect deviations or unusual activity. In short, spot anomalies sooner. Take action faster.



About Code42

Code42 is the leader in Insider Risk Management. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss and speeds incident response without inhibiting employee productivity. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. For more information, visit code42.com.