







Best Practices for Achieving FERPA Compliance



IT, risk, and cybersecurity professionals can streamline their FERPA compliance journey, as well as maintain FERPA compliance longer-term with these best practices.

-  **1. Conduct a FERPA Audit:** Identify all locations where student data is stored, who has access, and how data is currently being protected. This audit will serve as the foundation for developing or refining your FERPA compliance strategy.
-  **2. Implement Access Controls:** Role-based access controls (RBAC) ensure that only authorized personnel have access to student records based on their roles within the institution. Strong authentication methods like multi-factor authentication (MFA) verify the identity of users accessing student records.
-  **3. Data Encryption:** Data in transit is typically achieved using protocols like Transport Layer Security (TLS) or Secure Sockets Layer (SSL), while encrypting data at rest involves transforming the data into an unreadable format using cryptographic algorithms like AES 256.
-  **4. Hold Regular Training and Awareness Sessions:** Regularly scheduled employee security awareness training sessions and ongoing security awareness campaigns can help keep FERPA compliance top-of-mind for all employees. Reinforce these messages with newsletters, posters, and other channels.
-  **5. Embrace Incident Response Planning:** A comprehensive incident response plan should detail specific procedures for the prompt investigation of incidents, including steps to identify the scope and nature of the breach. It should also outline clear mitigation strategies to contain and minimize the impact.
-  **6. Conduct Regular Audits and Assessments:** Regular internal and external audits that assess compliance with FERPA regulations should encompass all aspects of your data handling and storage processes. Use the findings from these audits to identify any gaps or weaknesses in your data protection practices.

