SECURITY AND COMPLIANCE SOLUTIONS FOR FERPA

IDERA's Solutions for the Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA) was introduced in 1974. This United States federal law mandates the confidentiality and protection of student information in any educational institution that receives funding from the US Federal Government from kindergarten through the university level. FERPA generally prevents an education agency or institution from sharing student records or personally identifiable information in those records with individuals who are not authorized to view that information. In some cases, authorized individuals need to be monitored to deter insider theft and unauthorized dissemination of information.

From an information technology perspective student information must be audited for access, changes to access, and changes to the data. FERPA requires institutions to maintain logs of all student information activity. Specifically, FERPA mandates that you must be able to address the following questions:

1 Who has access to my "student information"?

2 What has changed with SQL Server permissions, logins and access?

3 How do I define a secure baseline and maintain it across my SQL Server environment?

4 How do I audit permission, object, and data changes to student information on my SQL Servers?

5 How do I ensure that my FERPA data can be rendered unreadable wherever it is backed up and additionally restored whenever needed?

HOW IDERA PRODUCTS HELP YOU COMPLY WITH FERPA REGULATIONS

SQL Secure is a security analysis solution for both SQL Server and Azure SQL Database that helps IT organizations identify database security violations and ensure security policies are enforced.

- Find out who has access to what. Identify and manage users' assigned and effective rights and permissions at the server, database, and object level.

- Use customizable pre-built templates for FERPA compliance (which leverage guidelines from STIG and CIS) to extract the information needed to satisfy an auditor's requirements.

- Monitor changes continuously with snapshots of the security model on a regularly scheduled or ad-hoc basis to detect unwanted changes to access rights and security settings.

- Define exactly what SQL Server security information you want to collect and when. Gathers information from SQL Server, Azure SQL Database, OS, File System, Registry, Active Directory (AD), and Azure AD.

- Get alerts on violations of corporate policies to secure your environment from the most common methods of intrusion.

SQL Compliance Manager is a comprehensive auditing, alerting, and reporting solution that uses policy-based algorithms to track changes to your SQL Server objects and data.

- Get continuous auditing of all SQL Server activity by identifying who did what, when, where and how, whether the event is initiated by privileged users or hackers.

- Monitor and audit all data access, updates, schema modifications, and permission changes. Audited items include: DDL, DML (including SQL Statements), security changes, database SELECT operations, and sensitive columns.

- Ease the research and configuration required to comply with FERPA regulations via built-in templates with pre-configured audit settings that align with the regulatory citations.

- Set up alerts to track suspect server activity including flexible alert definition, custom messaging, and alert reporting. Additionally, alerts can be applied across the board, or to specific servers, databases, or tables as needed.

SQL Safe Backup is an automated SQL Server backup and recovery solution that provides customizable policies to help you facilitate backing up and restoring your FERPA data.

- Employ AES 128-bit and 256-bit encryption that will protect backups and render the backup files unreadable anywhere they are stored.

- Choose from flexible recovery options including: IntelliRestore™ providing point-in- time recovery, InstantRestore™ to stream data from backups on-demand while restoring in the background, or Virtual Database to access data or objects in backups instantly without restoring.

- Backups can be stored for both on-premise SQL Servers and in the Cloud including Amazon Web Services (AWS), Simple Storage Service (S3), and Microsoft Azure Blob.

HOW IDERA PRODUCTS ADDRESS SPECIFIC FERPA REQUIREMENTS

FERPA CFR	Requirement	IDERA Solution
§ 99.2	**What is the purpose of these regulations?** The purpose of this part is to set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended.	**SQL Secure** protects your FERPA data by identifying any permissions that are different from established baselines. **SQL Compliance Manager** audits all student / faculty logins to FERPA data and delivers reports to prove it. **SQL Safe Backup** ensures that your FERPA data is backed up and encrypted for added protection for data that may be in transit and easily facilitates restores when needed.
§ 99.31(a)(1)	**School officials** Institutions that allow "school officials, including teachers, within the agency or institution" to have access to students' education records, without consent, must first make a determination that the official has "legitimate educational interests" in the information. The list of officials must be included in the annual FERPA notification.	**SQL Secure** gives you the ability to assess permissions that are currently in force for a student's educational records and you can additionally run frequent snapshots that will inform you of any changes that have been made to those permissions. **SQL Compliance Manager** audits all activity to the education records. Authorized access to student information is captured and stored in a secure database repository.
§ 99.31(a)(1)(ii)	**Controlling access to education records by school officials** Institutions are now required to use "reasonable methods" to ensure that instructors and other school officials (including outside service providers) obtain access to only those education records (paper or electronic) in which they have legitimate educational interests. Institutions are encouraged to restrict or track access to education records to ensure that they remain in compliance with this requirement. The higher the risk, the more stringent the protections should be (e.g., SSNs should be closely guarded).	**SQL Secure** provides the ability to track and ensure that user permissions are within set policy, ensuring that instructors and other school officials only have the permissions granted to them. Any changes that stray from the established baselines will be identified and alerted. **SQL Compliance Manager** audits all (internal/external) activity to education records. With sensitive column auditing, SSNs can be specifically audited for access and changes.

HOW IDERA PRODUCTS ADDRESS
SPECIFIC FERPA REQUIREMENTS

FERPA CFR	Requirement	IDERA Solution
§ 99.31(a)(2)	**Student's new school** An institution retains the authority to disclose and transfer education records to a student's new school even after the student has enrolled and such authority continues into the future so long as the disclosure is for purposes related to the student's enrollment / transfer. After admission, the American Disabilities Act (ADA) does not prohibit institutions from obtaining information concerning a current student with disabilities from any school previously attended by the student in connection with an emergency and if necessary to protect the health or safety of a student or other persons under FERPA. A student's previous school may supplement, update, or correct any records it sent during the student's application or transfer period and may identify any falsified or fraudulent records and / or explain the meaning of any records disclosed previously to the new school.	**SQL Compliance Manager** audits all activity to education records, who has access to them, and additionally what has changed. In order to prove falsified or fraudulent records you must be able to capture the image of the data and prove it. SQL Compliance Manager accomplishes this by capturing "before" and "after" data on the column level and who made the change.
§ 99.32(a)(1)	**What recordkeeping requirements exist concerning requests and disclosures?** An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, as well as the names of State and local educational authorities and Federal officials and agencies listed in § 99.31(a)(3) that may make further disclosures of personally identifiable information from the student's education records without consent under § 99.33(b). (2) The agency or institution shall maintain the record with the education records of the student as long as the records are maintained.	**SQL Compliance Manager** provides "select" column access auditing that stores a record in instances where the data is from a table that contains personally identifiable information. Additionally, you can identify any combination of columns for sensitive data (alerting and reporting). **SQL Safe Backup** ensures you can back up your education records and store them for as long as needed. This data can be encrypted for added protection.

HOW IDERA PRODUCTS ADDRESS
SPECIFIC FERPA REQUIREMENTS

FERPA CFR	Requirement	IDERA Solution
§ 99.35	**What conditions apply to disclosure of information for Federal or State program purposes?** Authorized representatives of the officials or agencies headed by officials listed in § 99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs.	**SQL Compliance Manager** captures logins, failed logins, security, and privileged users for servers. It audits all activity to the education records. Authorized access to student information is captured and stored in a secure database repository for audit reporting purposes.
§ 99.35, § 99.35(b)(1)	**Audit or Evaluation Exception Protection of PII from Education Records** (b) Information that is collected under paragraph (a) of this section must— (1) Be protected in a manner that does not permit personal identification of individuals by anyone other than the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) and their authorized representatives, except that the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of § 99.33(b).	**SQL Compliance Manager** captures DDL, DML, security, SELECTS and sensitive data for database level activity. It also provides "select" column access auditing that stores a record in instances where the data is from a table that contains personally identifiable information. **SQL Secure** gives you the ability to assess permissions that are currently in force for a student's educational records. A flexible grid view can be used to audit and analyze user permissions. Sort, group, or export all SQL Server logins. View all users' assigned and effective rights and permissions at the server, database, and object level.

IDERA understands that IT doesn't run on the network — it runs on the data and databases that power your business. That's why we design our products with the database as the nucleus of your IT universe.

Our database lifecycle management solutions allow database and IT professionals to design, monitor and manage data systems with complete confidence, whether in the cloud or on-premises.

We offer a diverse portfolio of free tools and educational resources to help you do more with less while giving you the knowledge to deliver even more than you did yesterday.

Whatever your need, IDERA has a solution.

IDERA