SOUTH DAKOTA SCHOOL OF MINES AND TECHNOLOGY

Policy Manual

SUBJECT: Database and Related Administrative Systems Security and Privacy

NUMBER: Policy VIII-05-05

POLICY

Each position that requires access to the Database and related administrative systems must be granted the minimum level of access needed to perform the specific job duties of the position. Access shall be granted only after the requestor has signed a confidentiality and privacy agreement, the supervisor or other appropriate authority has approved the request via an official request form (copies of form(s) shall be sent to and retained by IT and HR), and any prerequisite training has been completed. Access that is no longer necessary will be removed in a timely manner. Documents supporting access requests including confidentiality and privacy agreements with approval shall be stored in a secure location in electronic form.

PURPOSE

Develop a logical access control process and policy to protect University information systems and data by verifying and validating authorized users, authorizing user access to information systems and data, and restricting transactions (query, write, execute and delete) according to the user's authorized level.

The access policies and procedures must provide protection of University information systems and data commensurate with sensitivity and risk. All persons requesting access to University information systems shall (1) require the access to minimally perform their job duties; (2) only have the requisite level of access they need to perform those duties (query, write, execute or delete); (3) receive adequate training on how to use the system for which they have requested access; (4) receive adequate training on data security and student privacy.

SCOPE

This policy applies to all South Dakota School of Mines & Technology (SD Mines) faculty, staff, student workers, third party contractors and others who access the information database and related administrative systems.

DEFINITIONS

Database Security Officer (DSO): A DSO is a University employee who manages access to the informational database (i.e. Colleague and/or Banner) and related administrative systems.

Data Stewards: Vice presidents, associate vice presidents, directors, managers, or others authorized by the *Chief Networking and Security Officer* to manage a subset of data. The delegation of this authority and responsibility is accomplished by written instructions.

RESPONSIBILITIES:

Database Security Officer. The DSO is responsible for working with the data steward and department head or designee to design user access, for asking relevant questions in order to minimize unnecessary access, and for approving all user access within his/her Database module. The DSO is responsible for assigning access based on documented approval and confirmation that any prerequisite training has been completed. The DSO is responsible for reviewing a report of terminated employees, and for removing any related access. The DSO is responsible for periodically reviewing access changes made in his/her area of responsibility and making the appropriate Data Steward aware of any changes made by an unauthorized user. The DSO is responsible for reviewing and confirming with department heads at least annually, all user IDs associated with the database and related administrative systems access.

Data Steward. This person is responsible for ensuring that University data security policies are followed, and for developing internal controls to ensure security and privacy for data under their purview. Data Stewards are as follows:

Admissions: Director of Admissions and Associate Provost for Academic Administration
Finance/Student Accounts Receivable: Vice President for Finance and Administration
Financial Aid: Director, Financial Aid
Human Resources/Payroll: Vice President of Human Resources
Registrar: University Registrar
Database Support: Director, Information Technology Services

Department Head. The department head is responsible for evaluating and documenting the business needs of departmental employees in order to assist with the design of database and related administrative systems access. The department head is responsible for notifying the DSO of changes in job responsibilities which require access changes, including transfers within the department, transfers within the University, and terminations.

SOURCE: Office of the Registrar. University Cabinet May 2019.

BOR Reference: Policy 7:4 and 7:7