Turtle Mountain Community College Data Access Policy

Turtle Mountain Community College
10145 BIA Road 7
P.O Box 340
Belcourt, ND 58316
Phone 701-477-7862
Fax 701-477-7892
www.tm.edu

Table of Contents

Turtle Mountain Community College
10145 BIA Road 7
P.O Box 340
Belcourt, ND 58316
Phone 701-477-7862
Fax 701-477-7892
www.tm.edu

Data Access Policy

1. Purpose

The purpose of the data access policy is to ensure that employees have appropriate access to institutional data and information. While recognizing the College's responsibility for the security of data, the procedures established to protect that data must not interfere unduly with the efficient conduct of College business. This policy applies to all College units and to all uses of institutional data, regardless of the offices or format in which the data reside.

A. Statement of Policy

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuses, misinterpretation, and unnecessary restrictions to its access.

The College will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant data steward to have an appropriate access level. Data access will be conducted in accordance with the policies established by the Information Technology Department. Any employee or non-employee denied access may appeal the denial to the data stewards.

2. Secure Data Sharing

Secure file sharing is the act of sending documents digitally in such a manner that protects the shared information from being accessed by unauthorized users. Sharing files securely is most important when businesses need to ensure that confidential data can be shared only with select individuals or groups who have a legitimate reason to access this sensitive information.

Anytime you are sending or sharing personally identifiable information

(PII), you are required to share in a secure data sharing manner. To determine if the information is PII, please refer to section 3.D below.

Shared Network Folder

A shared network folder allows you to securely share a file or multiple files with select individuals. This network folder will need to be set up in advance by the IT Department.

Encrypted Emails

S/MIME is used to support enhanced encryption in transit, and automatically encrypts your outgoing emails if it can. You will need the users mobile phone number to enter as a security measure. Do not share PII in the body of an email, but rather include it as an attachment if you need to share information via Email.

10145 BIA Road 7
P.O Box 340
Belcourt, ND 58316
Phone 701-477-7862
Fax 701-477-7892
www.tm.edu

Etrieve/SoftDocs

Etrieve is used to support the process of sharing secured documents among defined departments based on need. This cloud-based software is also used as a document storage system that will be used across all necessary departments.

3. Data Usage Policy

The purpose of the data usage policy is to ensure that College data are not misused or abused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the data stewards.

B. Statement of Policy

College personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update, read-only, and external dissemination.

Authority to update data shall be granted by the appropriate data steward only to personnel whose job duties specify and require responsibility for data update. This will be granted based on positions and not individual requests. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with the college's desire to provide excellent service to faculty, staff, students, and other constituents.

Read-only usage to administrative information will be provided to employees for the support of college business without unnecessary difficulties/restrictions.

Only those data elements designated as "directory information" (as defined by FERPA) can be externally disseminated for official or "nonofficial" reporting. Even release of directory information should be guided by the need to respect individual privacy and to protect the integrity of the data. The release of all other data must be approved by the responsible data steward. Data usage will be conducted in accordance with policies established by the Information Technology Department.

C. Directory Information

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

D. Personally Identifiable Information (PII)

Personally identifiable information for education records is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or

10145 BIA Road 7
P.O Box 340
Belcourt, ND 58316
Phone 701-477-7862
Fax 701-477-7892
www.tm.edu

other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

E. Consequence of Noncompliance with Data Usage Policy

TMCC employees and students who fail to comply with the data usage policy will be considered in violation of the relevant College codes of conduct and may be subject to disciplinary action or to legal action if laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to data.

4. Data Classifications

Public:
Data that is in, or can be in, the public domain and can be openly shared with anyone outside of the organization.

Internal:
Company-wide data that is kept within the organization and, while not sensitive, should not be shared externally.

Confidential:
Domain-specific data that can be shared with specific people or teams and contains sensitive company information.

Restricted:
Highly sensitive information that should only be available on a need-to-know basis.

RELATED DOCUMENTS

Information Technology Policies:

The Family Educational Rights and Privacy Act (FERPA):

Data Integrity Policy

Data Governance Policy

CONTACTS

Data Trustees – jdelossantos@tm.edu, acharette1@tm.edu
Data Stewards – jenzabar_managers@tm.edu
Data Custodians / Security Officers – jdelossantos@tm.edu, mpoitra@tm.edu, cdavis@tm.edu