I. Purpose

The purpose of this policy is to outline essential roles and responsibilities within the Western Dakota Tech (WDT) community for creating and maintaining an environment that safeguards protected information and information systems from threats to personal, professional, and institutional interests and to establish a comprehensive information security program.

II. General Statement of Policy

A. WDT will safeguard protected information through a comprehensive security program with information systems that are secure and monitored, through training Users, by monitoring the creation, collection, storage, access, use, sharing, and destruction of protected information, and by providing corrective action if a security breach occurs.

This policy applies to all WDT information systems, to all Users of WDT protected information and information systems, and to all protected information created, collected, stored, accessed, used, shared, or destroyed by or on behalf of any department, program, operational support unit, or person in connection with WDT operations.

The Information Security Committee, Data Security Officers, Information Systems Director, Human Resources Director, and Supervisors will serve the primary roles of ensuring protected information and information systems are secure and monitored, of providing training to Users, and of reporting potential, suspected, or known security breaches or flaws. The VP for Institutional Effectiveness and Student Success will serve as Chair of the Information Security Committee and ensure security breaches are reported to the proper state and federal authorities when applicable.

In the event that any particular protected information or information system at WDT is governed by more specific requirements under other Board approved WDT policies and procedures (such as the policy for Student Education Records), the more specific requirements shall take precedence.

B. It shall be a violation of this policy to not protect the security of WDT information systems and protected information, to not report potential, suspected, or known security breaches to the appropriate parties, to not train on and monitor protected data and information systems, and to create, collect, store, access, use, share, or destroy protected information without proper authorized access.
III. Definitions

A. “Authorized Access” means a person has been authorized by a Data Security Officer or the VP for Institutional Effectiveness and Student Success to access information systems or to create, collect, store, access, use, share, or destroy protected information. Authorized access only includes access to information that is required to fulfill a job duty.

B. “Data Security Officers” are those members of the WDT community who provide administrative support for the implementation, oversight, and coordination of security procedures and systems with respect to specific Information Resources. Examples include the Information Systems Director, the Director of Institutional Research and Student Records, the Admissions and Financial Aid Director, and other designated owners of specific data resources.

C. “Information Resources” are a discrete body of information created, collected, stored, accessed, used, shared, or destroyed in connection with the operation and management of WDT and used by members of the College who have authorized access. Information Resources include electronic databases and applications as well as physical files. Examples include student files, student account records, and financial aid records.

D. “Information Systems” include all systems used to create, collect, store, access, use, share, and destroy data. Examples include the student information system, learning management system, files and file rooms, spreadsheets, and any other sources used for data.

E. “Protected information” shall be defined as data or information that has been designated as private, protected, or confidential by law or by WDT. Protected information includes, but is not limited to, employment records, medical records, student education records, personal financial records including account numbers, or other personal identifiable information (PII) such as social security number (or any part of), student or employee ID number, driver’s license number, PINs, and passwords.

Protected information shall not include public records that by law must be made available to the general public or directory information as defined in the WDT Student Handbook. To the extent there is any uncertainty as to whether any data constitutes protected information, the data in question shall be treated as protected information until a determination is made by the Vice President for Institutional Effectiveness and Student Success.

F. “Security Breach” shall be defined as any compromise of the security, confidentiality, or integrity of protected information or information systems that
could result in, results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of, and/or access to protected data. Good faith access or acquisition of protected data by an individual or functional unit is not a breach of the security of the system, provided that the information is not improperly used, or subject to subsequent unauthorized access, use, or disclosure.

G. “Users” include all members of the WDT community to the extent they have authorized access to protected data or information systems.

IV. Dissemination of Policy and Training

A. This policy shall appear on the WDT website.

B. Training will be provided by Supervisors, Data Security Officers, Information Systems Director, and/or the Information Security Committee at least annually.

Legal References: 15 U.S. Code § 6801; 16 C.F.R. § 314.4(b); 34 C.F.R. § 99.3; 45 C.F.R. § 160.103; South Dakota Codified Law 22-40-19 through 22-40-26;


Board Approved 02/25/2019; Committee Reviewed 2/23/2021; Committee Reviewed 4/28/2021