Western Dakota Technical College Policy Number: 5007

SECURITY OF PROTECTED INFORMATION

I. Purpose

The purpose of this policy and associated procedures is to outline essential roles and responsibilities for creating and maintaining an environment that safeguards Protected Information.

II. General Statement of Policy

WDTC will safeguard Protected Information whether in paper, electronic, or other form through a comprehensive security program designed and implemented by the Protected Information Committee and Data Security Officers (DSOs). Protected Information will be safeguarded with Data Systems that are secure and monitored, through training Permitted 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 Protected Information created, collected, stored, accessed, used, shared, or destroyed by or on behalf of any department, program, operational support unit, employee, student, contractor, agent, or other person/entity in connection with WDTC operations. In the event that any particular Protected Information is additionally governed by more specific requirements under other Board approved WDTC policies and procedures such as the policies for Safeguarding Customer Information (Policy 5008), FERPA (Policy 4004), and Identity Theft Red Flags (Policy 6019), the more specific requirements shall take precedence.

The Protected Information Committee, DSOs, Director of Information Systems, Director of Human Resources, and Supervisors will serve the primary roles of ensuring Protected Information whether in paper, electronic, or other form is secure and monitored, of providing training to Permitted 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 Protected Information Committee and ensure Security Breaches involving Protected Information are reported to the proper state and federal authorities when applicable.

III. Definitions

A. “Data Security Officers (DSOs)” are responsible for the implementation, oversight, and coordination of security procedures and processes with respect to specific Information Resources. DSOs are identified/appointed by the applicable Leadership supervisor.

B. “Data System” means 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.

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 WDTC and used by those who have Permitted Access. Information Resources may be in paper, electronic, or other form.

D. "Permitted Access" means an employee, contractor, agent, student, or other person/entity that is authorized to access Protected Information for a particular purpose whether in paper, electronic, or other form. Permitted Access is granted by the applicable DSO or the applicable DSO's Leadership supervisor.

E. "Permitted User" means those who have Permitted Access to Protected Information for a particular purpose.

F. "Protected Information" means data or information that has been designated as private, protected, or confidential by law or by WDTC. Protected Information includes, but is not limited to, employment records, medical records, student education records, personal financial records including account numbers, and 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 WDTC Policy 4004 – FERPA. 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 VP for Institutional Effectiveness and Student Success.

G. "Security Breach" shall be defined as any compromise of the security, confidentiality, or integrity of Protected Information or Data 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 Information. Good faith access or acquisition of Protected Information by an individual or functional unit is not a Security Breach, provided that the information is not improperly used, or subject to subsequent unauthorized access, use, or disclosure.

IV. Dissemination of Policy and Training

A. This policy shall appear on the WDTC website.

B. Training will be provided by Supervisors, DSOs, Director of Information Systems, and/or the Protected Information Committee at least annually.

Legal References: 15 U.S. Code § 6801;
16 C.F.R. § 314.4;

34 C.F.R. § 99.3;
45 C.F.R. § 160.103;
South Dakota Codified Law 22-40-19 through 22-40-26;

Other References: National Institute of Standards and Technology, FIPS Pub 199;
National Institute of Standards and Technology, NIST SP 800-30;
National Institute of Standards and Technology, NIST SP 800-61;
National Institute of Standards and Technology, NIST SP 800-171;
U.S. Department of Education, Departmental Directive OM: 6-107

Board Approved 02/25/2019; Committee Reviewed 2/23/2021; Committee Reviewed 4/28/2021; Committee Reviewed 3/7/2023; Committee Reviewed 7/26/2023