Western Dakota Technical College Procedure Number: 6045.Procedure.01

SECURITY OF PROTECTED INFORMATION

## I. Procedure

A. Roles and Responsibilities

1. The Western Dakota Technical College (WDTC) Protected Information Committee is responsible for the creation of and updating of the WDTC Security of Protected Information Policy and Procedures to ensure WDTC is in compliance with applicable protected information laws. The committee has the authority to: (1) develop and implement policies, procedures, and processes necessary to minimize the possibility of a Security Breach; (2) consult and educate Permitted User(s) and functional unit(s) relative to their individual and collective responsibilities to protect data and Data Systems; and (3) take reasonable actions to mitigate incidents or concerns relating to security of Protected Information or to Data Systems which may include conducting security audits. The committee is responsible to track Data Security Officers (DSOs) for specific Information Resources.

2. DSOs are responsible for the safety and security of specific Information Resources. DSOs determine who has Permitted Access to specific Information Resources; create more specific policies and procedures applicable to their area if applicable (e.g. FERPA – Policy 4300, Identity Theft Red Flags – Policy 6030, Student Records Retention – Policy 4310, and Information Security – Policy 6040 ); establish written processes to secure Information Resources, Protected Information, and Data Systems (e.g. encryption requirements and disposal methods); monitor security of Information Resources, Protected Information, and Data Systems; report any potential, suspected, or known Security Breach or flaw to the VP for Institutional Effectiveness and Student Success; and provide training to Permitted Users upon hire or at the time Permitted Access is granted and at minimum annually thereafter.

   DSOs are responsible to ensure those whom they grant Permitted Access are capable of maintaining appropriate safeguards for Protected Information. If Permitted Access is granted to contractors, agents, or other outside entities, a contract must be in place in which the contractor, agent, or other outside entity agrees to implement such safeguards. The President's Office is in charge of Protected Information language in all contracts, and DSOs must confirm contracts meet expectations with the President's Office.

In cases where a DSO is not identified for an Information Resource, Permitted Users are to consult with the VP for Institutional Effectiveness and Student Success for proper protocol.

3. The Director of Information Systems is responsible for WDTC's information technology infrastructure including designing, recommending and implementing security protocols, monitoring, and overseeing threat responses. The Director of Information Systems is responsible for designing and providing relevant information technology security training to Permitted Users. Additionally, the Director of Information Systems has the authority to assume control over the response to any potential, suspected, or known Security Breach or flaw involving WDTC's information technology infrastructure, data, and computing.

4. The Senior Human Resources Generalist is responsible for providing the Security of Protected Information Policy and Procedures to incoming employees, working with IT and department supervisors to ensure employees who end employment with WDTC no longer have access to Data Systems, and coordinating any disciplinary measures against an employee taken in response to a violation of WDTC Protected Information policies, procedures, and processes and applicable laws.

5. WDTC Supervisors are responsible for promoting the institutional awareness of the Security of Protected Information Policy and Procedures, for ensuring overall compliance and training with their staff, for monitoring security of Protected Information and Data Systems, and for reporting any potential, suspected, or known Security Breach or flaw to the appropriate party.

6. Permitted User(s) are required to follow all policies, procedures, and processes to safeguard the security of Protected Information and Data Systems.

   Permitted Users are to:

   i. Only access Data Systems and create, collect, store, access, use, share, and destroy Protected Information they have been granted Permitted Access to and need to fulfill a job duty.
   ii. Report any potential, suspected, or known Security Breach or flaw to the appropriate party.
   iii. Become familiar with and comply with all relevant WDTC Protected Information policies and procedures and applicable laws.
   iv. Complete initial and annual training provided by the DSO and ongoing employee training regarding Protected Information provided by the College.
   v. Provide appropriate physical security for information technology equipment, storage media, and physical data. Such equipment and files shall not be left

unattended without being secured (i.e. a locked cabinet drawer) or otherwise protected such that unauthorized parties cannot obtain physical access to the data or the devices storing the Protected Information.

vi. Ensure Protected Information is not distributed or accessible to unauthorized parties.

vii. Not share their passwords nor store their passwords where others can access.

viii. Avail themselves of any security measures, such as encryption technology, security updates, or patches.

ix. Lock computers when not in use.

x. Comply with WDTC Protected Information policies, procedures, and processes and applicable laws irrespective of where the data might be located, including, for example, on home devices, on mobile devices, on the Internet, or with other Service Providers. Protected Information, when removed from the campus or when accessed from off-campus, is subject to the same rules as would apply were the Protected Information on campus.

xi. Properly dispose of Protected Information to ensure against unauthorized interception of any Protected Information. Generally, paper-based copies of Protected Information should be properly secured and then shredded, and electronic Protected Information should be deleted or destroyed per IT requirements.

B. Security Breach Response

1. All employees, Permitted Users, Supervisors, and DSOs must report any potential, suspected, or known Security Breach or flaws plus any incident that could result in a Security Breach such as loss of keys, theft of computer devices, viruses, worms, or computer "attacks" that may lead to unauthorized access of Protected Information immediately. Notification must be made to the person's supervisor and to the VP for Institutional Effectiveness and Student Success. Notification to additional parties must also be made if directed to do so by more specific requirements in WDTC Board approved policies such as FERPA (Policy 4300) and Information Security (Policy 6040).

2. The VP for Institutional Effectiveness and Student Success or designee will in collaboration with appropriate parties investigate and review the incident with the appropriate DSO(s), department(s), and person(s) directly affected by the incident. (If the VP for Institutional Effectiveness and Student Success is a party to the breach, the Compliance Officer will be assigned to fulfill the duties of the VP for Institutional Effectiveness and Student Success for this section, *B. Security Breach Response*, of this procedure.)

3. The VP for Institutional Effectiveness and Student Success or designee will in collaboration with appropriate parties, and legal counsel if deemed needed,

determine what, if any, actions WDTC is required to take to comply with applicable state laws (SDCL 22-40-19 through 22-40-26; https://sdlegislature.gov/Statutes/Codified_Laws/2047710), the Federal Trade Commission guidelines https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business, and required notifications to the feds through their FSA Cyber Security Team. If the event involves a criminal matter, WDTC will work with local law enforcement to coordinate the appropriate response. The VP for Institutional Effectiveness and Student Success will report the incident to WDTC's insurance carrier when deemed necessary.

4. The VP for Institutional Effectiveness and Student Success will determine if a Security Breach audit is necessary. If an audit of the incident and how the incident was handled is deemed necessary, the VP for Institutional Effectiveness and Student Success will assign a Security Breach Audit Team and provide documentation of the incident, the investigation, and the response to the team. The Security Breach Audit Team will audit the investigation and response to ensure proper protocols were followed. The audit findings will be provided to the VP for Institutional Effectiveness and Student Success for final review.

5. The VP for Institutional Effectiveness and Student Success will present a summary of data breaches on an annual basis to the Protected Information Committee.

C. Enforcement Sanctions

1. WDTC reserves the right to monitor network traffic, data access, and email accounts, to perform random audits, and to take other steps to ensure the integrity of its Data Systems and Protected Information and to ensure compliance with WDTC Protected Information policies, procedures, and processes, and applicable state and federal laws.

2. Violations of this policy may result in disciplinary actions that may include temporary or permanent restrictions to access certain information or Data Systems, a warning, temporary suspension from duties with or without pay, or termination of employment. The nature and extent of these actions depend on a variety of factors, including the severity of the breach, willful or repeated violations, past work record, or any other consideration which may be considered relevant by the College. The need for disciplinary action and the appropriate penalty for employees will be handled accordingly by the Senior Human Resources Generalist and others as appropriate.

## II. 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 4300 – 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.

H. “Security Breach Team” is comprised of a minimum of two WDTC Protected Information Committee members who serve as auditors to a Protected Information Security Breach investigation and response.

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;

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 3/7/2023; Committee Reviewed 7/26/2023