INFORMATION SECURITY

I. Procedure

A. Roles and Responsibilities

1. The Western Dakota Tech (WDT) Information Security Committee is responsible for the creation of and updating of the WDT Information Security Policy and Procedures to ensure WDT is in compliance with applicable information security 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 user(s) and functional unit(s) relative to their individual and collective responsibilities to protect data and information systems; and (3) take reasonable actions to mitigate incidents or concerns relating to security of protected information or to information systems which may include conducting security audits. The committee is responsible to designate Data Security Officers for specific Information Resources.

2. Data Security Officers are responsible for the safety and security of specific Information Resources. Data Security Officers determine who has authorized access to Information Resources, create policies and procedures specific to their area if applicable (e.g. FERPA, Identity Theft Red Flags, and Student Records Retention), establish written processes to secure information systems and protected data (e.g. encryption requirements and disposal methods), provide training to Users, monitor security of protected information and information systems, and report any potential, suspected, or known security breach or flaw to the appropriate party.

In cases where a Data Security Officer is not identified for an Information Resource, Users are to consult with the VP for Institutional Effectiveness and Student Success and the Information Systems Director for proper protocol.

3. The WDT Information Systems Director is responsible to conduct risk assessments of and oversee threat responses of WDT’s information technology infrastructure and to provide relevant information technology security training to Users. Additionally, the Information Systems Director has the authority to assume control over the response to any potential, suspected, or known security breach or flaw involving WDT’s information technology infrastructure, data, and computing.

4. The Human Resources Director is responsible for providing the Information Security Policy and Procedures to incoming employees, working with IT to ensure
employees who end employment with WDT no longer have access to technology information systems, and coordinating any disciplinary measures against an employee taken in response to a violation of WDT information security policies, procedures, and processes and applicable laws.

5. WDT Supervisors are responsible for promoting the institutional awareness of the Information Security Policy and Procedures, for ensuring overall compliance and training with their staff, for monitoring security of protected information and information systems, and for reporting any potential, suspected, or known security breach or flaw to the appropriate party.

6. User(s) are required to follow all policies, procedures, and processes to safeguard the information security of protected data and information systems.

Users are to:

i. Only access information systems and create, collect, store, access, use, share, and destroy protected information they have been granted authorized 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 WDT information security policies and procedures and applicable laws.

iv. Complete initial and ongoing employee training regarding information security.

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 Users 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 persons.

vii. Not share their passwords.

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 WDT information security policies, procedures, and processes and applicable laws irrespective of where the data might be located, including, for example, on home devices, mobile devices, on the Internet, or other third-party 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 (to include media such as DVD storage) should be deleted or destroyed.

B. Security Breach Response

1. Users, Supervisors, and Data Security Officers 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.

2. Notification must be made to the person’s supervisor and to the VP for Institutional Effectiveness and Student Success. The VP for Institutional Effectiveness and Student Success in collaboration with appropriate parties will investigate and review the incident with the appropriate Data Security Officer(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 Human Resources Director will 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 in collaboration with appropriate parties will determine what, if any, actions WDT is required to take to comply with applicable law to include required notifications to the feds through their FSA Cyber Security Team. If the event involves a criminal matter, WDT will work with local law enforcement to coordinate the appropriate response. The VP for Institutional Effectiveness and Student Success will report the incident to WDT’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. The VP for Institutional Effectiveness and Student Success will present a summary of data breach investigations and outcomes to the Information Security Committee. The committee will conduct a post-incident review of events and determine, what, if any changes should be made to WDT information security-related policies, procedures, and processes to prevent similar incidents.
5. The VP for Institutional Effectiveness and Student Success will present a summary of data breaches on an annual basis to the Information Security Committee.

C. Enforcement Sanctions

1. WDT 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 information systems and protected data and to ensure compliance with WDT information security 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 networks, 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 Human Resources Director and others as appropriate.

II. 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 Registrar, 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 VP 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. “Security Breach Team” is comprised of a minimum of two WDT Information Security Committee members who serve as auditors to an information security breach investigation and response.

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

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