Western Dakota Technical College Procedure Number: 6040.Procedure.01

INFORMATION SECURITY PROGRAM

I. Procedure (Elements)

A. Qualified Individual

The Director of Information Systems is the Qualified Individual responsible for developing, implementing, overseeing, maintaining, and enforcing WDTC's Information Security Program.

B. Risk Assessment

1. The Information Security Program will be based upon an initial Risk Assessment. The Risk Assessment will be designed, conducted, and evaluated by the Director of Information Systems, and the Risk Assessment will:
    a. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Customer Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks; and
    b. Be presented to the President and VP for Data Strategy and Enrollment Management when completed and sent to the Protected Information Committee as an information item.

2. The Director of Information Systems will periodically perform additional Risk Assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Customer Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks. The Risk Assessment will be presented to the President and VP for Data Strategy and Enrollment Management when completed and sent to the Protected Information Committee as an information item.

3. Risk Assessments will be written and include:
    a. Criteria for the evaluation and categorization of identified security risks or threats WDTC faces;
    b. Criteria for the assessment of the confidentiality, integrity, and availability of WDTC Information Systems and Customer Information, including the adequacy of the existing controls in the context of the identified risks or threats WDTC faces; and
    c. Requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the Information Security Program will address the risks.

C. Safeguards

The Director of Information Systems will work with the applicable DSOs to design, document, and implement safeguards to control the risks identified through Risk Assessments, including by:

1. Implementing and periodically reviewing access controls, including technical and as appropriate, physical controls to:
    a. Authenticate and permit access only to Authorized Users to protect against the unauthorized acquisition of Customer Information; and
    b. Limit Authorized Users' access only to Customer Information that they need to perform their duties and functions, or, in the case of Customers, to access their own information.
2. Identifying and managing the data, personnel, devices, systems, and facilities that enable WDTC to achieve business purposes in accordance with their relative importance to business objectives and WDTC's risk strategy.
3. Protecting by Encryption all Customer Information held or transmitted by WDTC both in transit over external networks and at rest. To the extent WDTC determines that Encryption of Customer Information, either in transit over external networks or at rest, is infeasible, WDTC may instead secure such Customer Information using effective alternative compensating controls reviewed and approved by WDTC's Qualified Individual.
4. Adopting secure development practices for in-house developed applications utilized by WDTC for transmitting, accessing, or storing Customer Information and processes for evaluating, assessing, or testing the security of externally developed applications WDTC utilizes to transmit, access, or store Customer Information.
5. Implementing Multi-factor Authentication for any individual accessing any Information System, unless WDTC's Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.
6. Developing, implementing, and maintaining processes for the secure disposal of Customer Information in any format no later than two years after the last date the information was used in connection with the provision of a Financial Product or Service to the Customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained. This includes periodically reviewing WDTC's records retention policies to minimize the unnecessary retention of data.
7. Adopting procedures for change management.
8. Implementing policies, procedures, and/or processes plus controls designed to monitor and log the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Customer Information by such users.

D. Testing and Monitoring

1. The Director of Information Systems will work with the applicable DSOs to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures/processes, including those to detect actual and attempted attacks on, or intrusions into, Information Systems.
2. For Information Systems, the monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in Information Systems that may create vulnerabilities, the Director of Information Systems will conduct:
    a. Annual Penetration Testing of WDTC's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and
    b. Vulnerability assessments, including any systemic scans or reviews of Information Systems reasonably designed to identify publicly known security vulnerabilities in WDTC's Information Systems based on the Risk Assessment, at least every six months; and whenever there are material changes to WDTC's operations or business arrangements; and whenever there are circumstances WDTC knows or have reason to known may have a material impact on WDTC's Information Security Program.

E. Qualified Personnel and Training

The Director of Information Systems will stay current in knowledge and skills needed to manage WDTC's information security risks and to develop, implement, oversee, maintain, and enforce WDTC's Information Security Program. The Director will also ensure personnel are able to enact WDTC's Information Security Program by:

1. Providing personnel with security awareness training that is updated as necessary to reflect risks identified by the Risk Assessment;
2. Providing personnel with security updates and training sufficient to address relevant security risks; and
3. Verifying that personnel take steps to maintain current knowledge of changing information security threats and countermeasures as applicable.

F. Service Providers

The Director of Information Systems will oversee Service Providers by:

1. Taking reasonable steps to select and retain Service Providers that can maintain appropriate safeguards for the Customer Information at issue
2. Requiring Service Providers by contract to implement and maintain such safeguards; and
3. Periodically assessing Service Providers based on the risk they present and the continued adequacy of their safeguards.

G. Evaluation and Adjustment

The Director of Information Systems will evaluate and adjust WDTC's Information Security Program in light of:

1. The results of the testing and monitoring required in section D. of this procedure;
2. Any material changes to WDTC operations or business arrangements;
3. The results of the Risk Assessment performed under section B. of this procedure;
4. Or any other circumstances that WDTC knows or has reason to know may have a material impact on the Information Security Program.

H. Incident Response Plan

The Director of Information Systems will establish a written Incident Response Plan designed to promptly respond to, and recover from, any Security Event materially affecting the confidentiality, integrity, or availability of Customer Information. The Incident Response Plan will address the following areas:

1. The goals of the Incident Response plan;
2. The internal processes for responding to a Security Event;
3. The definition of clear roles, responsibilities, and levels of decision-making authority;
4. External and internal communications and information sharing;
5. Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
6. Documentation and reporting regarding Security Events and related incident response activities; and
7. The evaluation and revision as necessary of the Incident Response Plan following a Security Event.

I. Report

The Director of Information Security will report in writing, regularly and at least annually, to the Board of Trustees. The report will include the following information:

1. The overall status of the Information Security Program and WDTC compliance with 16 CFR Part 314; and
2. Material matters related to the Information Security Program, addressing issues such as Risk Assessment, risk management and control decisions, Service Provider arrangements, results of testing, Security Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.

J. Documentation

The Director of Information Systems will keep documentation of all elements of the Information Security Program.

K. 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 Information Systems and protected data and to ensure compliance with WDTC 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 Senior Human Resources Generalist and others as appropriate.

II. Definitions

A. "Authorized User" means any employee, Service Provider, contractor, agent, Customer, or other person/entity that is authorized to access Customer Information whether in paper, electronic, or other form.

B. "Consumer" means an individual who obtains or has obtained a Financial Product or Service from WDTC that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

C. "Customer" means a Consumer who has a Customer Relationship with WDTC.

D. "Customer Information" means any record containing Nonpublic Personal Information about a Customer of WDTC, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of WDTC or our affiliate.

E. "Customer Relationship" means a continuing relationship between a Consumer and WDTC under which WDTC provides one or more Financial Products or Services to the Consumer that are to be used primarily for personal, family, or household purposes. For example, Consumers who submit a FAFSA to WDTC are in a Continuing Relationship with WDTC until all records containing Nonpublic Personal Information about the Consumer are destroyed per records retention policies and procedures.

F. "Encryption" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

G. "Financial Product or Service" means any product or service that WDTC offers by engaging in financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

Examples of Financial Products or Services through WDTC include federal financial aid, payment plans, and Build Dakota Scholarships. (Scholarships that do not require repayment if certain conditions are not met are not considered a Financial Product or Service.)

H. "Information Security Program" means the administrative, technical, or physical safeguards WDTC uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Customer Information.

I. "Information System" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing Customer Information or connected to a system containing Customer Information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains Customer Information or that is connected to a system that contains Customer Information.

J. "Multi-factor Authentication means authentication through verification of at least two of the following types of authentication factors:

    1. Knowledge factors, such as a password;
    2. Possession factors, such as a token; or
    3. Inherence factors, such as biometric characteristics.

K. "Nonpublic Personal Information" means:

    1. Personally Identifiable Financial Information, and
    2. Any list, description, or other grouping of Consumers (and Publicly Available Information pertaining to them) that is derived using any Personally Identifiable Financial Information that is not publicly available. For example, a list of names and addresses derived by using Pell grant status.

    Nonpublic Personal Information does not include:

    1. Publicly Available Information, except as included on a list as described in K.2.
    2. Any list of individuals' names and addresses that contains only Publicly Available Information, is not derived, in whole or in part, using Personally Identifiable Financial Information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a Consumer of WDTC.

L. "Penetration Testing" means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside WDTC Information Systems.

M. “Personally Identifiable Financial Information” means any information:

1. A Consumer provides to WDTC to obtain a Financial Product or Service from WDTC;
2. About a Consumer resulting from any transaction involving a Financial Product or Service between WDTC and the Consumer; or
3. WDTC otherwise obtains about a Consumer in connection with providing a Financial Product or Service to the Consumer.

Examples include, but are not limited to,

1. Information a Consumer provides on an application for a loan or for federal financial aid such as name, address, birthdate, bank and credit card account numbers, income and credit histories, tax information, and social security numbers;
2. Account balance information, payment history, overdraft history, and credit or debit card purchase information tied to a Financial Product or Service through WDTC;
3. The fact that an individual is or has been one of WDTC’s Customers;
4. Any information about WDTC’s Consumer if it is disclosed in a manner that indicates that the individual is or has been WDTC’s Consumer;
5. Any information that a Consumer provides to WDTC or that WDTC or WDTC’s agent otherwise obtains in connection with collecting on, or servicing, a credit account;
6. Any information WDTC collects through an internet “cookie” in relation to a Financial product or Service through WDTC;

Personally Identifiable Financial Information does not include information that does not identify a Consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

N. “Publicly Available Information” means any information that WDTC has a reasonable basis to believe is lawfully made available to the general public from Federal, State, or local government records; widely distributed media; or disclosures to the general public that are required to be made by Federal, State, or local law. WDTC must take steps to determine the information is of the type that is available to the general public and that the Consumer has not blocked the disclosure of such information.

O. “Security Event” means an event resulting in unauthorized access to, or disruption or misuse of, an Information System, information stored on such Information System, or Customer Information held in physical form.

P. “Service Provider” means any person or entity that receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to WDTC.

III. Dissemination of Policy and Training

A. This policy shall appear on the WDTC website.

B. Training will be provided by Director of Information Systems, Data Security Officers (DSOs), and Supervisors upon new employee hire and at least annually thereafter.

Legal References: 16 CFR Part 314 – Standards for Safeguarding Customer Information
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

Board Approved 7/28/2023