Effective Date: 5/19/23

Tulsa Community College
Information Security Program

Tulsa Community College (TCC) complies with the Gramm-Leach-Bliley Act (15 U.S.C. § 6801, et seq.) (GLBA) and the Federal Trade Commission Standards for Safeguarding Customer Information (16 C.F.R. § 314) ("Safeguards Rule"). TCC has adopted an information security program ("Information Security Program") with the following objectives:

1. To ensure the security and confidentiality of student and customer information;
2. To protect against any anticipated threats to the security or integrity of such information; and
3. To guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student and customer.

The TCC IT team launched a formal InfoSec program in 2017. This group is responsible for the cyber security processes which identify, manage and control the risks to system and data availability, integrity and confidentiality. Activities of this group include recurring scheduled meetings with a qualified third party to address program documentation status, review cyber security incidents, discuss project status relating to controls catalog assignments and plan college-wide communication and training requirements. This program is responsible for the creation and maintenance of an Acceptable Use Policy, Disaster Recovery Plan and Incident Response Plan. In addition, this group recommends the acquisition of hardware, software and services that improve the cyber security posture of TCC.

I. Definitions

Student and customer information means any record containing nonpublic personal information about a student and/or customer, whether in paper, electronic, or another form, that is processed by or on behalf of TCC or its affiliates.

Information Security Program means the administrative, technical, or physical safeguards used to collect, process, store, and dispose of student and customer information.

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 student and customer information or connected to a system containing student and 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 student and customer information or that is connected to a system that contains student and customer information.

Service provider means any person or entity that receives, processes, or otherwise is permitted access to student and customer information through its direct provision of services to TCC.

II. Qualified Individual

Michael Siftar, Associate Vice President of Administrative Operations and Chief Technology Officer, is the qualified individual designated by TCC to oversee and implement the Information Security Program (Qualified Individual).

III. Risk Assessment

The Information Security Program is a based on annual risk assessments conducted by TCC IT. InfoSec. Such risk assessments are written and include:

(i) Criteria for the evaluation and categorization of identified security risks or threats TCC faces;
(ii) Criteria for the assessment of the confidentiality, integrity, and availability of TCC information systems and student and customer information, including the adequacy of the existing controls in the context of the identified risks or threats TCC faces; and
(iii) 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. Areas for improvement are denoted by a future state gap score.

The most recent TCC risk assessment was completed on February 15th, 2023. TCC shall continue to annually conduct risk assessments to reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student and 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.

IV. Safeguards

TCC IT has implemented the following safeguards at TCC:

(1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of student and customer information; and

(ii) Limit authorized users' access only to student and customer information that they need to perform their duties and functions, or, in the case of students and customers, to access their own information;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable TCC to achieve business purposes in accordance with their relative importance to business objectives and TCC risk strategy;

(3) Protect by encryption all student and customer information held or transmitted by TCC both in transit over external networks and at rest. To the extent TCC determines that encryption of student and customer information, either in transit over external networks or at rest, is infeasible, it shall instead secure such student and customer information using effective alternative compensating controls reviewed and approved by the Qualified Individual;

(4) Adopt secure development practices for in-house developed applications utilized by TCC for transmitting, accessing, or storing student and customer information and procedures for evaluating, assessing, or testing the security of externally developed applications TCC utilizes to transmit, access, or store student and customer information;

(5) Implement multi-factor authentication for access to key enterprise information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6)

(i) Develop, implement, and maintain procedures for the secure disposal of student and customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the student and 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. TCC retains records in accordance with applicable federal laws, and the applicable retention periods in the Consolidated General Records Disposition Schedule adopted for State Universities and Colleges; and

(ii) Periodically review TCC data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, student and customer information by such users.

V. Testing and Monitoring

TCC regularly tests and monitors the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. (2) For information systems, the monitoring and testing includes continuous monitoring or periodic penetration testing and vulnerability assessments including:

(i) Annual penetration testing of information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances TCC knows or have reason to know may have a material impact on the information security program.

VI. Training

TCC shall provide its personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment. TCC shall utilize qualified information security personnel employed by TCC or an affiliate or service provider sufficient to manage its information security risks and to perform or oversee the information security program. TCC shall provide information security personnel with security updates and training sufficient to address relevant security risks. TCC shall verify that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

VII. Service Providers

TCC shall oversee service providers by 1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the student and customer information at issue, 2) requiring its service providers by contract to implement and maintain such safeguards, and 3) periodically assessing its service providers based on the risk they present and the continued adequacy of their safeguards.

VIII. Evaluation and Adjustment

TCC shall evaluate and adjust its information security program in light of 1) the results of the testing and monitoring, 2) any material changes to operations or business arrangements, 3) the results of risk assessments, and 4) any other circumstances TCC knows or has reason to know may have a material impact on its Information Security Program.

IX. Incident Response Plan

TCC has established a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of student and customer information in its control. This incident response plan addresses 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.

X. Regular Reporting

TCC's Qualified Individual shall regularly (and at least annually) provide a report in writing to the TCC Board of Regents including the following information:

(1) The overall status of the Information Security Program and TCC's compliance; 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.