DATA SECURITY POLICY & PROCEDURES PROGRAM

The Information Technology (IT) Department

I. Introduction

The protection of sensitive College data and information is of paramount importance. The Information Technology (IT) Department is dedicated to preventing the unauthorized access or disclosure of this information. To assure this, the IT Department has implemented several measures to minimize the risk of unauthorized access. Accordingly, and in response to federal, state and other regulations, including institutional policies, the College is determined to effectuate policies and procedures that safeguard the receipt, collection, storage and then, disposal of this data.

II. Role of IT Department and Qualified Individual to Coordinate the Information Security Program

Five Towns College IT Department is the institution's purveyor of both hardware and software and procures appropriate technology for the College. It is thus charged with the responsibility to manage and implement the data security policies and procedures program with the objective to ensure the protection of important and sensitive institutional data and information. Further, the IT Department complies with relevant federal, state, and other regulations and institutional policies. To this end, the institution has designated the Director of the IT Department as its qualified individual responsible for overseeing, implementing and enforcing the FTC information security program.

III. Relevant Laws and Regulations

As a recipient of Title IV funds, Five Towns College is classified as a financial institution under the Gramm-Leach-Bliley Act (GLBA, 2002), which is also known as the Financial Modernization Act of 1999. It is a federal law enacted to control the ways that financial institutions deal with the private information of individuals and, thus, there must be certain safeguards in place.

Following its enactment, the GLBA has been modified from time to time. In 2021, provisions considered as the Standards for Safeguarding Customer Information were modified and the effective date was extended to June 9, 2023. The College adheres to the requirements of this regulation. Provisions of 16 C.F.R. section 314.3 and 16 C.F.R. section 314.4 and its provisions are set forth below:

§314.3 Standards for safeguarding customer information.

(a) ***Information security program.*** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) ***Objectives.*** The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70307, Dec. 9, 2021]

314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

(b) Base your information security program on a risk assessment that identifies 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 assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; 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.

(2) You shall 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.

(c) Design and implement safeguards to control the risks you identify through risk assessment, including by:

(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 customer information; and

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

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

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

(5) Implement multi-factor authentication for any individual accessing any 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 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 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; and

(ii) Periodically review your 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, customer information by such users.

(d)

(1) Regularly test or otherwise monitor 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 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, you shall conduct:

(i) Annual penetration testing of your 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 your 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 you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

(2) Requiring your service providers by contract to implement and maintain such safeguards; and

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(h) 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 in your control. Such incident response plan shall 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) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

(1) The overall status of the information security program and your compliance with this part; 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) Notify the Federal Trade Commission about notification events in accordance with paragraphs (j)(1) and (2) of this section.

(1) ***Notification requirement.*** Upon discovery of a notification event as described in paragraph (j)(2) of this section, if the notification event involves the information of at least 500 consumers, you must notify the Federal Trade Commission as soon as possible, and no later than 30 days after discovery of the event. The notice shall be made electronically on a form to be located on the FTC's website, *https://www.ftc.gov*. The notice shall include the following:

(i) The name and contact information of the reporting financial institution;

(ii) A description of the types of information that were involved in the notification event;

(iii) If the information is possible to determine, the date or date range of the notification event;

(iv) The number of consumers affected or potentially affected by the notification event;

(v) A general description of the notification event; and

(vi) Whether any law enforcement official has provided you with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal

Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

(2) ***Notification event treated as discovered.*** A notification event shall be treated as discovered as of the first day on which such event is known to you. You shall be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent. [86 FR 70307, Dec. 9, 2021, as amended at 88 FR 77508, Nov. 13, 2023]

§314.6 Exceptions.

Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers. [8 FR 70308, Dec. 9, 2021]

IV. Institutional Initiatives

To effectuate continuing processes and procedures that align with the relevant regulations, FTC's administrative offices, including Admissions, Financial Aid, Registrar, Bursar, and Information Technology (IT) have implemented new processes and software to protect incoming data and design a system that is primarily digital and is protected with appropriate safeguards. This is demonstrated, in part, by changed procedures in the Admissions Office that include an online application process with secure software, and an updated Student Information System (SIS) as well as security software, i.e., reCAPTCHA for supplementary submissions and documents, if needed, as well as the use of an integrated student portal.

The Financial Aid Department has implemented a secure portal to upload important and sensitive documents with proper authentication and password protection. The Registrar's Office uses all safeguards available through the SIS and the institution's Learning Management System (LMS), Canvas, as well. It has also implemented the use of both interactive and PDF versions of forms for important data requests. All of these institutional processes and procedures are secured by the upgraded firewall that ensures current state of the industry technology to alleviate risks to the information systems and the protection of data.

V. Data Protection and Account Security Measures

The IT Department has implemented several data protection and account security measures. These security measures include but are not limited to the following:

- Password Policy requires passwords to be changed every six months and follow certain criteria.
- An updated, state of the art Fortinet firewall blocks unauthorized traffic and ensures that networking hardware is all password protected, in addition to providing backend data and assessment on all attempted and unauthorized access.
- Network accounts and permissions are implemented.
- Microsoft Active Directory controls Network Access.
- Public websites protected by secure socket layers.
- No access to computers/shared storage only to permitted staff.
- Computers lock after 10 minutes of inactivity.
- Anti-virus is installed on all computers.
- Users with personal computers are limited to Wi-Fi service which is restricted to outbound traffic to the Internet.
- Data is remotely backed up with security in place.
- All applications are password protected.
- Accounts and access for staff/faculty are verified with supervisors.
- Institutional policy not to email social security number or other personally identifiable information.

VI. Institutional Information Risk Assessment and Testing Schedule

Pursuant to the regulations stated above, the institution performs risk assessment that addresses the areas noted above. In addition to account security measures described, the institution conducts information technology risk assessment. This assessment is on demand, and also a more frequent data report is reviewed in addition to monthly risk assessment. An annual Risk Assessment Report is conducted by the Qualified Individual and available upon request to authorized parties and supplemented by firewall reports.

VII. Institutional Documentation of Information Risk Assessment/Testing Schedule Test and Results

To evidence that the stated risk assessment is conducted and that the testing schedule tests and results are recorded, the institution has developed a plan to record this information. Currently, this is performed monthly and the documentation is available upon written request if required from the qualified individual or the Director of the IT Department.

VIII. Information Security Policy and Procedures Program Schedule and Contact Information Available on Consumer Information and Compliance Website

For all questions or concerns related to the FTC IT Data Security Policies and Procedures Program and schedule, please contact the qualified individual/Director of the IT Department, Daoning Dai. He actively oversees this process and can be contacted at support@ftc.edu.

IX. Communications: Preparedness to Respond Immediately and Appropriately in the Event of Breach

In the event of a breach of these security measures, an internal investigation would be initiated at once and a diagnostic plan would follow. A communications plan has been established among the institution's executive team that includes immediate notification from the IT Department to the Public Safety Office, the Vice President of Finance and Administration and President. Once the source or area of the institution's data involved is determined, all heads of those and other administrative units are notified. The College's Administrative Council has met, discussed, reviewed, and is involved in all notifications that will be sent to the institution's constituents in this event, as well as to the local precinct and public, depending on the situation and in compliance with the notification requirements under the statute. The qualified individual reviews all processes and systems and provides the institution with updated recommendations, including the recommendation to install and implement new updated firewall.

X. Data Security Policies and Procedures Program Related to Third Parties Under Articulation and Dual Enrollment Agreements

The College has several Articulation and Dual Enrollment Agreements with high schools and/or community colleges. Under those agreements, any related data provided i.e., personally identifiable information as defined by New York Education Law Section 2-d, and/or the Family Educational Rights and Privacy Act (FERPA) is afforded the same protections and is managed under the terms and provisions of the College's Data Security Policies and Procedures Program detailed here and in compliance with state and federal law. Any requests to provide its institutional data security and privacy plan are herein contained and all third parties hereby have acknowledged that they have received actual and/or constructive notice of this as incorporated into the underlying Articulation and/or Dual Enrollment Agreement(s).

Further, and in conformance with this, the College understands and acknowledges that it has in place sufficient standards for safeguarding consumer information, protections and internal controls to ensure compliance with applicable laws and regulations, and that it is responsible for complying with state/federal data security and privacy standards for all personally identifiable information from education records, and it: (1) limits internal access to education records to those individuals that are determined to have legitimate educational interests; (2) does not use the education records for any purposes other than those explicitly authorized in those Agreements; (3) maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and (4) has adopted this institutional Data Security Policy and Procedures Program in compliance with the above that addresses confidentiality, data security and privacy standards and it is available at ftc.edu.