FIVE TOWNS COLLEGE

DATA SECURITY POLICY & PROCEDURES PROGRAM

I. Introduction

The protection of sensitive College data and information is a top priority. 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/or 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 Individual Designated 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 Head of the IT Department to coordinate the data 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 Gram-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. Included in these are (1) the development, implementation and maintenance of a documented data security program; and (2) the designation of an employee to coordinate the program.

In furtherance of this compliance, the College has developed these policies, trained staff, and has reviewed its technology, including built-in systems safeguards as well as identifying areas to strengthen, if deemed necessary.

Here are the three elements required by 16 C. F. R. 314.4(b):

> In order to develop, implement, and maintain your information security program, you shall:
> (a) **Designate an employee** or employees to coordinate your information security program.
> (b) **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. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
> (1) Employee training and management;
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
> (c) **Design and implement information safeguards to control the risks** you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
> (d) 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; and
> (2) Requiring your service providers by contract to implement and maintain such safeguards.
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
> (Emphasis supplied) (16 C. F. R. 314.4(b)).

IV. Institutional Initiatives

In order to effectuate an improvement in procedures and be compliant, several institutional offices, including Admissions, Financial Aid and Registrar have implemented new processes to protect incoming data and design a paper flow that is primarily digital but is protected with appropriate safeguards. Part of this is demonstrated by changed procedures in the Admissions Office with an online application process with secure software in place as well as captcha software. Also, the Financial Aid Department has implemented a secure portal to upload important and sensitive documents with proper authentication and password protection. Further, the Registrar’s Office has both interactive or PDF versions of forms for important data requests.

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
- A firewall is in place to block unauthorized traffic and networking hardware is all password protected
- 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 must perform a risk assessment that addresses the three areas noted above. In addition to account security measures described above, the institution conducts information technology risk assessment. This assessment, at this time, is on demand and a regular schedule is available upon request from the Head of the IT Department.

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 as appropriate or required from the Head 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 IT Security Polices and Procedures Program and Schedule, please contact the Head of the IT Department, Craig Healy. 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 commence and a diagnostic plan would occur at once. A communications plan has been established among the institution's executive team that includes immediate notification from the IT Department to the offices of Public Safety and 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 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.

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

The College has several Articulation Agreements with area 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, 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 part and parcel of the underlying Articulation Agreement.

Further, and in conformance with this, the College understands and acknowledges that it has in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and that it is responsible for complying with state 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.