Information Security Program

Trident University International (TUI) has established an information security program to safeguard student information.

This program includes administrative, technical and/or physical safeguards preventing the unauthorized access, use, collection, distribution or transmission of information. The aim of the program is to achieve the objectives of:

- Ensuring the security of confidential and 'internal use only' information
- Protecting against any anticipated threats or hazards to the security or integrity of such information
- Protecting against unauthorized access to or use of such information that could result in substantial harm or inconvenience

Designated Coordinators

TUI has designated the Chief Information Officer to coordinate its information security program with support from the Chief Financial Officer, Chief Compliance Officer, Director of Financial Aid and Registrar.

Risk assessment

TUI identifies reasonable foreseeable internal and external risks to the security, confidentiality, and integrity of 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. At a minimum, the school's risk assessment includes consideration of risks in each relevant area of operations including:

- Unauthorized access of information
- Unauthorized system access
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data as a result of disaster
- Corruption of data or systems
- Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
- Detecting, preventing, and responding to attacks, intrusions, or other systems failures

Safeguards

All access, use, storage and removal of data shall be consistent with the:

- Network and Acceptable Use policies
- Electronic and Social Media Policy
- Red Flag Policy
- Employee Code of Conduct
- Business Ethics training
- Compliance Training on
    - Retention of Student Records (FERPA)
    - State and federal laws regulating access and use of data/systems
- Non-Disclosure and Intellectual Property Rights Agreement

In addition, TUI has implemented the following information security safeguards to control the risks it identifies through risk assessment:

- Secure user authentication protocols
- Customized access based on levels of authority related to duties and responsibilities
- Increased logon security to access Finance, Financial aid and HR information
- All servers are protected through an Application Gateway which blocks all unauthorized access to core applications and data and 'hacking' attempts
- Access and interactions with Trident Learning Community, Email, Reporting, Information Hub, and Student Information System are protected through HTTPS.
- Operating system patches and security updates are installed regularly and in some cases automatically
- Antivirus and anti-malware software is installed and kept up to date
- Disabling passwords upon termination of employment or relationship with TUI
- Access to internal network from remote locations is only through Virtual Private Network running on TUI provided computers or virtual desktops running in TUI data center.

Employee Training

All employees who access confidential information shall read and execute the Network and Equipment Use policies of the university. Also, each employee shall receive training during on-boarding and annually thereafter. Employees shall also successfully complete an on-line ethics training module.

Testing & Monitoring

TUI regularly tests or otherwise monitors the effectiveness of the safeguards' key controls, systems, and procedures. Responsibility for testing and monitoring rests with the Chief Information Officer or designee. Any incident of possible or actual unauthorized access, use, disclosure, alteration, destruction or removal of information from computers or computer systems, or any other compromise of confidential information shall be reported to the Chief Information Officer, Chief Compliance Officer or both. Any verified attempt or successful compromise of confidential information, computers or computer systems shall be immediately reported to the Executive Leadership Team of the University, Board of Trustees and law enforcement officials where appropriate.

Evaluation & Adjustment

On an annual basis TUI will evaluate and adjust its information security program in light of the results of the required testing and monitoring, as well as for any material changes to its operations or business arrangements or any other circumstances that it has reason to know may have a material impact on the school's information security program. Responsibility for evaluation and recommendations for adjustment rests with the Chief Information Officer or designee.

Overseeing service providers

TUI takes reasonable steps and exercises appropriate diligence in selecting service providers capable of maintaining appropriate safeguards for the customer information at issue and requires the service providers to maintain such safeguards.

Policies Cross-referenced

The following policies provide guidance and direction relating to this program:

- Network and Acceptable Use Policy
- Electronic and Social Media Policy
- Retention of Student Records (FERPA)
- Red Flag Policy
- Employee Code of Conduct
- Non-Disclosure and Intellectual Property Rights Agreement