

**Information Technology Committee  
Meeting Agenda  
January 17, 2025  
9:10 a. m.- 11:00 a.m.  
T-14**

➤ **Action Item**

1. Approve the Minutes from November 22, 2024

➤ **Information and Discussion Items**

1. Exploration of Improving Cybersecurity: Training
2. Make recommendations for resources in the classroom
3. Review of Acceptable Use Policy (AP 3720):

<https://www.taftcollege.edu/about/campus-leadership/board-of-trustees/policies-procedures/files/ch-3/AP-3720-Computer-and-Network-Use-Procedure-Employees-3-17-23.pdf>

➤ **ITS and DE Updates**

➤ **Additional Agenda Items**

➤ **Meeting Time**


@@@@@@@@@@@@@@@@

AP 3720

Title IV Information Security Compliance (Optional)

In accordance with the Gramm-Leach-Bliley Act for entities that participate in Title IV Educational Assistance Programs, the District will develop, implement, and maintain a comprehensive information security program containing administrative, technical, and physical safeguards.

- A designated employee or employees to coordinate the entity's information security program.
- Identification of 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 the entity's operations, including:

- 
- Employee training and management;
  - Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
  - Detecting, preventing and responding to attacks, intrusion, or other systems failures.
- Design and implementation of information safeguards to control the risks the entity identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
  - Oversee service providers, by
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
    - Requiring the entity's service providers by contract to implement and maintain such safeguards.
  - Evaluate and adjust the entity's information security program in light of the results of the testing and monitoring required; any material changes to the entity's operations or business arrangements; or any other circumstances that they entity knows or has reason to know may have a material impact on the entity's information security program.