STUDENT CYBERSECURITY RESOURCES AND AWARENESS

WAYNE COMMUNITY COLLEGE

1. **PURPOSE**

   Faculty, staff, students and all other authorized users should gain a broad understanding of information security threats, risks, and best practices to assist the College in protecting the confidentiality, integrity, and availability of College information resources accessed, managed, and/or controlled by the College.
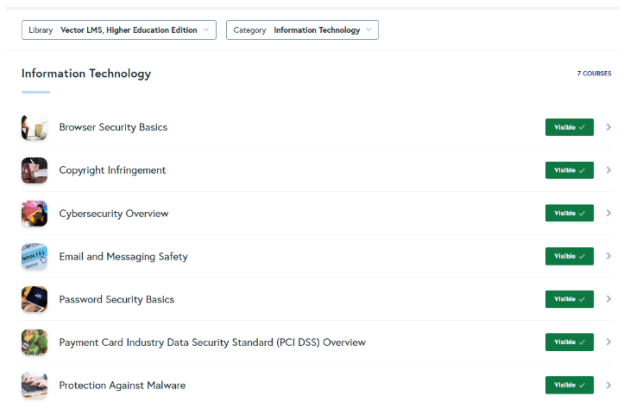
2. **SCOPE**

   The Chief Information Officer (CIO) will develop and implement an information security awareness program to be offered periodically to all College faculty, staff, students, and other authorized users of College information resources. To demonstrate basic competency in information security best practices, faculty and staff must complete this training as part of the onboarding process, annually thereafter, or as required by the CIO. Students will have the option (not the requirement) to complete the information security awareness training program. Each semester students are sent information on how to access this training.

   Information security awareness training will include, but not be limited to:

   - Information security awareness best practices.
   - Information security roles and responsibilities.
   - Acceptable use of College information resources.
   - Information classification and handling.
   - Causes of unintentional data exposure (e.g. losing a mobile device, emailing the wrong person due to autocomplete)
   - Enabling and utilizing security authentication.
   - How to identify different forms of social engineering attacks (e.g. phishing, phone scams, impersonation calls).
   - Security incident indicators, reporting, and response.
   - Security terms and definitions.

   Below is list of the trainings available to students. Students will have access to this training through the College's SafeColleges training portal. (Fig. 1)

(Fig. 1)