Course Number and Title: ISY 143 Introduction to Information Security

Campus Location:
Georgetown, Dover, Wilmington

Effective Date:
2018-51

Prerequisite:
ENG 090 or ENG 091, SSC 100 or concurrent

Co-Requisites:
None

Course Credits and Hours:
3.00 credits
3.00 lecture hours/week
0.00 lab hours/week

Course Description:
This course introduces students to information security terminology, the legal environment, risk management, security technologies, and security planning and implementation. Students prepare for further study in computer forensics and cyber network protection.

Required Text(s):
Obtain current textbook information by viewing the campus bookstore - https://www.dtcc.edu/bookstores online or visit a campus bookstore. Check your course schedule for the course number and section.

Additional Materials:
None

Schedule Type:
Classroom Course
Online Course

Disclaimer:
None

Core Course Performance Objectives (CCPOs):

1. Discuss computer security terminology. (CCC 5; PGC 6)
2. Identify security threats, vulnerabilities, and countermeasures. (CCC 4, 5: PCG 1, 2, 4)
3. Describe technical methods to implement and monitor defense strategies. (CCC 2; PGC3, 6)
4. Analyze basic network security issues and Web vulnerabilities. (CCC 5; PGC 6)
5. Explain the role of government in information security and information secrecy. (CCC 5; PGC 6)

See Core Curriculum Competencies and Program Graduate Competencies at the end of the syllabus. CCPOs are linked to every competency they develop.

Measurable Performance Objectives (MPOs):
Upon completion of this course, the student will:

1. Discuss computer security terminology.
    1. Define information security properties, services, and attacks.
    2. Explain the process to manage and improve information security.
    3. Describe critical information and infrastructure characteristics.
2. Identify security threats, vulnerabilities, and countermeasures.
    1. Describe general strategies for controlling access.
    2. Describe methods of authentication.
    3. Explain file security controls methods.
    4. Employ risk assessment.
3. Describe technical methods to implement and monitor defense strategies.
    1. Explain features and properties of effective file encryption.
    2. Identify public key cryptography concepts.
    3. Discuss basic network encryption concepts.
4. Analyze basic network security issues and web vulnerabilities.
    1. Describe Internet host addressing and network inspection tools.
    2. Describe host naming with the Domain Name System (DNS) and network address translation.
    3. Identify email security issues.
    4. Explain the security issues of web-based activities.
5. Explain the role of government in information security and information secrecy.
    1. Describe national information security policy issues and typical policy elements.
    2. Summarize the major facets of national information security policy.

Evaluation Criteria/Policies:
Students must demonstrate proficiency on all CCPOs at a minimal 75 percent level to successfully complete the course. The grade will be determined using the Delaware Tech grading system:

92	–	100	=	A
83	–	91	=	B
75	–	82	=	C
0	–	74	=	F

Students should refer to the Student Handbook - https://www.dtcc.edu/handbook for information on the Academic Standing Policy, the Academic Integrity Policy, Student Rights and Responsibilities, and other policies relevant to their academic progress.

Core Curriculum Competencies (CCCs are the competencies every graduate will develop):

1. Apply clear and effective communication skills.
2. Use critical thinking to solve problems.
3. Collaborate to achieve a common goal.
4. Demonstrate professional and ethical conduct.
5. Use information literacy for effective vocational and/or academic research.
6. Apply quantitative reasoning and/or scientific inquiry to solve practical problems.

Program Graduate Competencies (PGCs are the competencies every graduate will develop specific to his or her major):

1. Identify and remediate vulnerabilities.
2. Design, plan, and install network systems.
3. Install and configure operating systems.
4. Demonstrate the ability to write and debug scripts.
5. Demonstrate professionalism and ethical responsibility.
6. Communicate effectively to diverse groups of stakeholders.
7. Perform change management analysis and documentation.
8. Perform evidence collection and forensics analysis.
9. Create, modify, and/or implement security policies.

Disabilities Support Statement:
The College is committed to providing reasonable accommodations for students with disabilities. Students are encouraged to schedule an appointment with the campus Disabilities Support Counselor to request an accommodation needed due to a disability. A listing of campus Disabilities Support Counselors and contact information can be found at the disabilities services - https://www.dtcc.edu/disabilitysupport web page or visit the campus Advising Center.