Course Number and Title: ITN 170 Information Security

Campus Location:
Georgetown, Dover, Stanton, Wilmington

Effective Date:
2020-51

Prerequisite:
ITN 120, SSC 100 or concurrent

Co-Requisites:
None

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

Course Description:
This course provides a basic foundation in information security, including terminology, technologies, planning, and implementation. Students explore risk and legal issues related to information security.

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:
Access to high-speed Internet

Schedule Type:
Classroom Course
Video Conferencing
Web Conferencing
Hybrid Course
Online Course

Disclaimer:
None

Core Course Performance Objectives (CCPOs):

1. Describe the purpose of components used to secure information technology assets. (CCC 1; PGC 4)
2. Explain the various methods of attack and how to mitigate the risk. (CCC 1, 2; PGC 1, 3, 4)
3. Analyze the asset to determine the appropriate security controls given specific scenarios. (CCC 1, 2; PGC 1, 2, 3, 4)
4. Explain the basic concepts of forensics and incident response. (CCC 1, 2; PGC 1, 3)
5. Explain the purpose and function of cryptography. (CCC 1, 2; PGC 1, 3, 4)
6. Develop a disaster recovery and business continuity plan (DR/BC). (CCC 1, 2, 3, 5; PGC 1, 2, 3, 4)
7. Examine information security policies to protect information technology assets. (CCC 1, 2, 3, 5; PGC 1, 2, 3, 4)

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. Describe the purpose of components used to secure information technology assets.
    1. Define computer security terminology.
    2. Explain the purpose and function of key components in information security architecture.
2. Explain the various methods of attack and how to mitigate the risk.
    1. Explain the various types of attacks.
    2. Identify the indicators of compromise given a scenario.
    3. Identify the type of attack given a scenario.
    4. Explain penetration testing concepts.
3. Analyze the asset to determine the appropriate security controls given specific scenarios.
    1. Explain the types and purposes of security controls.
    2. Select appropriate mitigation controls given a scenario.
    3. Compare and contrast the function and purpose of authentication services.
    4. Select appropriate authentication authorization or access control given a scenario.
4. Explain the basic concepts of forensics and incident response.
    1. Describe basic concepts of forensics.
    2. Follow incident response procedures.
5. Explain the purpose and function of cryptography.
    1. Describe the application and use of symmetric, asymmetric, and public key infrastructure (PKI).
    2. Explain generalized cryptographic concepts.
    3. Use appropriate cryptographic methods given a specific scenario.
6. Develop a disaster recovery and business continuity plan (DR/BC).
    1. Describe types of disasters that compromise availability to information.
    2. Differentiate among the types of DR/BC implementations.
    3. Draft a DR/BC plan to meet an organization's needs.
7. Examine information security policies to protect information technology assets.
    1. Analyze security policies in accordance with an organization's requirements for accuracy and relevancy.
    2. Draft components of an information security policy to meet an organization's needs.
    3. Select appropriate data security and privacy practices to meet an organization's needs.

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. Solve technology-related problems using critical thinking and troubleshooting skills.
2. Articulate the role of the technology professional in organizations to support the ethical use of information technology.
3. Apply fundamental security concepts and strategies for maintaining and securing information technology.
4. Read and interpret technical information and effectively communicate to a wide range of audiences using oral, print, and multimedia strategies.
5. Demonstrate the importance of lifelong learning that empowers personal and professional growth.

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.