

GRADUATE COUNCIL: NEW COURSE PROPOSAL

Originating Unit: NEELY (INSC)

Type of action: New course Full online course**

Semester and year course will take effect: Fall 2024

New course title: Cybersecurity

Appropriate computer abbreviation (30 spaces or less): Cybersecurity

Course instructional methodology: Lecture

course component types: [ugradcouncil.tcu.edu/forms/Course Component Types.pdf](http://ugradcouncil.tcu.edu/forms/Course%20Component%20Types.pdf)

New course number: INSC 70440

Prerequisites for new course: *include an attachment if additional space is needed*

Graduate standing

Click here to attach a file

attached files can be seen and managed in Acrobat Pro by clicking on View > Show/Hide > Navigations Panes > Attachments

Description of new course (catalog copy): *include an attachment if additional space is needed*

This course provides the foundation understanding the key issues associated with protecting information assets. It teaches basic concepts and principles of information security and fundamental approaches to secure computers and networks.

Click here to attach a file

attached files can be seen and managed in Acrobat Pro by clicking on View > Show/Hide > Navigations Panes > Attachments

Fully Online Courses**

All online courses, and /or distance learning offerings must meet State Compliance regulations as defined by specific state legislation. TCU Distance Learning is any for-credit instruction provided to a TCU student outside the State of Texas. This includes internships, clinical, video conferencing, online, or any other delivery format that crosses state lines. Contact the Koehler Center for Teaching Excellence for guidelines. Include a letter of support from the Koehler Center with this proposal.

Supporting evidence or justification: (For a new course, attach proposed syllabus, including course objectives, course outline, and representative bibliography.)

Describe the intended outcomes of the course and how they will be assessed: *include an attachment if additional space is needed*

See attached syllabus

Click here to attach a file

attached files can be seen and managed in Acrobat Pro by clicking on View > Show/Hide > Navigations Panes > Attachments

Additional resources required:

Faculty: None

Space: None

Equipment: None

Library: None

Financial Aid: None

Other: none

Change in teaching load: No

Does this change affect any other units of the University? Yes No

If yes, submit supporting statement signed by chair of affected unit.

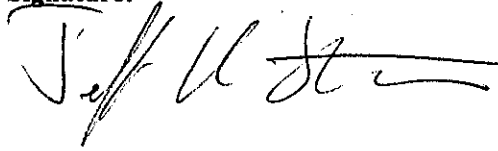
If cross-listed, provide evidence of approval by all curriculum committees appropriate to both the originating and the cross-listed units.

Chair of Originating Unit:

Name: Jeff Stratman

Unit: NEELEY - Information Systems and Supply Chain Management Department

Signature:

A handwritten signature in black ink, appearing to read "Jeff Stratman". The signature is written in a cursive style with a horizontal line at the end.

Neeley 
SCHOOL OF BUSINESS
INSC 70440: Cybersecurity
Course Syllabus

Instructor Name:
Semester and Year:
Number of Credits: 1.5
Class Location:
Class Meeting Day(s) & Time(s):
Office Location:
Office Hours:
Telephone:
Email:
Response Time:

Final Exam Date & Other Important Dates

The course's comprehensive final exam is held in accordance with the registrar's final exam schedule.

Rescheduling of Finals Policy: According to the *Faculty/Staff Handbook "Rescheduling of Finals"* section, rescheduling a final exercise must be made one week prior to the last day of classes. Rescheduling of finals is permitted for 1) graduating seniors whose faculty members must submit final grades by Wednesday 5pm of finals week, 2) students with more than two finals in a 24-hour period rule, and 3) students for whom a final examination conflicts with a major religious holiday or custom. Unless the student is graduating, the exam must be taken during final examination week

Course Description

This course provides the foundation understanding the key issues associated with protecting information assets. It teaches basic concepts and principles of information security and fundamental approaches to secure computers and networks.

Learning Objectives

Upon completion of this course, the student will obtain an understanding and will apply key concepts, including:

- Foundational concepts of cyber and information security and the key practices and processes for managing security effectively.
- Basic network fundamentals – including (but not limited to) topologies, protocols, address conservation, and services, and the security issues that affect networks.
- Basic cryptology and why it is fundamental to computer and information security.
- Software program deficiencies and the vulnerabilities associated with them.

- Access controls and authentication as they are used to secure systems and how they can be mitigated.
- Security vulnerabilities that affect operating systems and how they can be mitigated.
- The use of risk management to plan, implement, and administer security programs and processes.
- The key elements of incident management; detection, remediation, and recovery.
- How to translate security into a business driver that is critical to meeting the organization's mission.
- Legal, ethical, and regulatory issues that shape policy development and the ways in which organizations implement and administer security.
- The organizational and societal costs of insecurity software.

Prerequisites

Graduate Standing

Required book

Principles of Information Security, Michael E. Whitman, Herbert J. Mattord, Seventh edition, (27 Jul 2021), ISBN: 9780357506431

Course Policies and Requirements

Grading

Your grade for this course will be based on evidence of your accomplishment of the course objectives that I will gather from each of the following:

Graded Item	Description	Point and % of Final Grade	Date Due
Watch and Respond video	Watch and respond to the content of 5 videos - covering different areas of cybersecurity.	200 (20%)	Posted on D2L
Mid-semester exam	Mid-semester exam (multiple choice questions) - Sunday evening at 11:59 PM.	200 (20%)	Posted on D2L
Cybersecurity exercises/ assignments	5 Cybersecurity exercises using due Sunday evening at 11:59 PM, Respond with a professionally written 1 to 2 pages Word document (Times New Romans, 12, and double-spaced).	300 (30%)	Posted on D2L
Final Exam	Comprehensive final exam	300 (30%)	Posted on D2L

	Total	1,000 points 100%	
--	--------------	----------------------------------	--

Final Numerical Grade Calculation (+/-) and Final Letter Grade Calculation:

Letter Grades will be assigned based on the below percentages:

A	94 – 100%	C	73 – 76%
A-	90 – 93%	C-	70 – 72%
B+	87 – 89%		
B	83 – 86%		
B-	80 – 82%		
C+	77 – 79%	F	< 60%

Assessment and Grading

Assignments

Five (5) weekly cybersecurity exercises /assignments will be assigned during the semester. Each assignment is a practical exercise on information security issues/challenges organizations face in protecting valuable information assets. Students will be expected to research topics in cybersecurity and document their findings in a professionally written, grammatically correct 1-to-2-page paper.

Exams: There are two exams: mid-term exams and a final exam.

Watch and respond videos

The short videos (10 to 20 minutes) expose students to some of the challenges faced by companies in security valuable information assets from both insider and external hackers. Students will be expected to watch the video and document their findings on a professionally written, grammatically correct 1-to-2-page paper.

Instructor Expectations

The instructors will give each of you 100% of our commitment to help you successfully complete the class, however, it is expected that you provide 100% of your commitment to this class, which includes reading the textbook, using the resources available in D2L, watching posted videos, posting questions in the discussion board, completing your assignments, reviewing your graded assignments, and following up with questions to the instructor.

Student Responsibilities

It is the student’s responsibility to ensure that assignments are submitted in the proper format as described in each assignment. Documents which the instructor is unable to open may result in zero credit. Students should submit assignments on due dates outlined on the course schedule, and may be deducted points for late submission. Please refer to the submission requirements in each assignment.

Late Work

Work must be submitted on time and via the method included in the assignment sheet. Late work will only be accepted with prior authorization and may result in a ½ percentage grade deduction.

Grading Concerns

I take grading very seriously and I strive to be as fair and as consistent as possible. However, if you decide to challenge a grade on an assignment or exam, please submit a written appeal to me **within seven days** after the graded item is handed back to the class. The originally graded work must be submitted with a detailed explanation for the reason for the appeal. Upon receipt of a grade appeal, I reserve the right to re-evaluate the entire assignment or exam in addition to the section in question. Please note that I cannot and will not engage in discussion regarding grades or grade appeals through e-mail or in class. All written communication must be in the form of a dated memo.

Attendance

- Regular and punctual class attendance is essential, and no assigned work is summarily excused because of absence, no matter what the cause.
 - If you are absent to represent the University (as in athletics, chorus, band, national or state meetings of organizations represented at TCU), for an Official University Absence through the Campus Life Office, please notify me immediately and prior to the absence date.
-

Technology Policy

- You will be required to bring your laptop to class to work on technology assignments each day. Specific projects will be announced in class and are included in the course schedule.
-

TCU Email

Email Notification: Only the official TCU student email address will be used for all course notification. It is your responsibility to check your TCU email on a regular basis.

Netiquette: Communication Courtesy Code

All members of the class are expected to follow rules of common courtesy in all email messages, discussions, and chats. If I deem any of them to be inappropriate or offensive, I will forward the message to the Chair of the department and appropriate action will be taken, not excluding expulsion from the course. The same rules apply online as they do in person. Be respectful of other students. Foul discourse will not be tolerated. Please take a moment and read the following link concerning "netiquette."

<http://www.albion.com/netiquette/>

Participating in the virtual realm, including social media sites and shared-access sites sometimes used for educational collaborations, should be done with honor and integrity:

<http://macaulay.cuny.edu/community/handbook/technology/honorable-technology/>

TCU Syllabus Policies & Resources

Please use this [link](#) or scan the QR code with a mobile device camera to access policies and resources including support for TCU students, student access and accommodation, anti-discrimination and Title IX information, and other important information.



Course Schedule

Date	Topic	To-do list or Assignment
Week 1	Module 1 Introduction to the course Module 1—Introduction to Information Security	(1). Student introduction via discussion board (2) Watch & Respond #1.
Week 2	Module 2—The Need for Information Security	(1) Watch & respond #2. (2) Cybersecurity exercise #1: Q1, 2, and 5 page 24
Week 3	Module 3—Information Security Management	Watch & respond #3. Cybersecurity exercise #2: Q1, 2, and 4 page 76
Week 4	Mid-term Exam (Module 1 – 3)	
Week 5	Module 5—Incident Response and Contingency Planning	Watch & respond #4. Cybersecurity exercise # 3; Q1, 2, and 3 page 119
Week 6	Module 4—Risk Management	Watch & respond #5. Cybersecurity exercise # 4; Q3, 4, and 5 page 173
Week 7	Module 9—Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools	Cybersecurity exercise # 5: read and respond per info security career - page 267 to 283
Week 8	Final Exam – Modules 1, 4, 5, 9	Final Exam

