STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CITA306 – Software Security

For available course numbers, contact the Registrar's Office at registrar@canton.edu

CIP Code: 15.1204

For assistance determining CIP Code, please refer to this webpage
https://nces.ed.gov/ipeds/cipcode/browse.aspx?y=55
or reach out to Sarah Todd at todds@canton.edu

Created by: Stacia Smith

School: Canino School of Engineering
Department: Decision Systems
Implementation Semester/Year: Fall 2026

A. TITLE: Software Security Fundamentals

B. COURSE NUMBER: CITA306

C. CREDIT HOURS (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity):

# Credit Hours per Week	**3**
# Lecture Hours per Week	**3**
# Lab Hours per Week	**0**
Other per Week	**0**

D. WRITING INTENSIVE COURSE:

Yes	
No	X

E. GER CATEGORY:

Does course satisfy a GER category(ies)? If so, please select all that apply.

[1-2] Communication	
[3] Diversity: Equity, Inclusion & Social Justice	
[4] Mathematics & Quantitative Reasoning	
[5] Natural Science & Scientific Reasoning	
[6] Humanities	
[7] Social Sciences	
[8] Arts	
[9] US History & Civic Engagement	
[10] World History & Global Awareness	
[11] World Languages	

F. SEMESTER(S) OFFERED:

Fall	
Spring	
Fall and Spring	X

G. COURSE DESCRIPTION:

This course introduces the foundational principles of securing software applications and systems. Students will explore the various threats that can compromise the functionality, integrity, and privacy of software, and learn how to design, implement, and maintain secure applications. Topics will include common vulnerabilities, secure coding practices, threat assessment, and risk management, along with tools and techniques for testing and evaluating software security.

H. PRE-REQUISITES: CITA180 Introduction to Programming
CO-REQUISITES: N/A

I. STUDENT LEARNING OUTCOMES:

Course Student Learning Outcome [SLO]	Program Student Learning Outcome [PSLO]	GER	ISLO & Subsets
a. Explain key principles of software security	Documents & Information		2 [CA], 5
b. Summarize the security development lifecycle	Documents & Information		2 [CA], 5
c. Describe common vulnerabilities in software	Documents & Information		2 [CA], 5
d. Perform threat assessment and risk management	Documents & Information		2 [CA], 5
f. Demonstrate secure coding practices	Tools		2 [CA], 5

KEY	Institutional Student Learning Outcomes [ISLO 1 – 5]
ISLO #	**ISLO & Subsets**
1	**Communication Skills** Oral [O], Written [W]
2	**Critical Thinking** *Critical Analysis [CA], Inquiry & Analysis [IA] , Problem Solving [PS]*
3	**Foundational Skills** *Information Management [IM], Quantitative Lit, /Reasoning [QTR]*
4	**Social Responsibility** *Ethical Reasoning [ER], Global Learning [GL],* *Intercultural Knowledge [IK], Teamwork [T]*
5	**Industry, Professional, Discipline Specific Knowledge and Skills**

J. APPLIED LEARNING COMPONENT:

Yes	X
No	

If yes, select [X] one or more of the following categories:

Non-Clinical Practicum	X	Community Service	
Internship		Civic Engagement	

Clinical Practicum		Creative Works/Senior Project	
Practicum		Research	
Service Learning		Entrepreneurship [program, class, project]	

K. TEXTS: Various online resources such as SUNY Canton Library Books24x7

L. REFERENCES: N/A

M. EQUIPMENT: Technology Enhanced Classroom

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- assignments
- exams
- quizzes

P. DETAILED COURSE OUTLINE:

1. Introduction to Software Security Principles
   A. Importance of security software systems
   B. Understanding security concepts: confidentiality, integrity, availability
   C. The security development lifecycle
   D. Security vs. functionality trade-offs
   E. Overview of software vulnerabilities

2. Secure Software Design Principles
   A. Defense in depth and layered security
   B. Least privilege and separation of duties
   C. Secure defaults and minimal attack surface
   D. Threat modeling and risk management in design

3. Secure Coding Practices
   A. Defensive programming techniques
   B. Input validation and output encoding
   C. Secure error handling and logging

4. Threat Assessment and Risk Management
   A. Identify and categorize potential threats
   B. Identify vulnerabilities and define security requirements
   C. Evaluate severity and likelihood of vulnerabilities
   D. Risk management strategies

Q. LABORATORY OUTLINE: