CSC 181: ARTIFICIAL INTELLIGENCE SECURITY

In Workflow

1. CSC Committee Chair (abeer.abdelkhaleq@csus.edu)
2. CSC Chair (jouyang@csus.edu)
3. ECS College Committee Chair (tongren.zhu@csus.edu)
4. ECS Dean (arad@csus.edu)
5. Academic Services (catalog@csus.edu)
6. Senate Curriculum Subcommittee Chair (curriculum@csus.edu)
7. Dean of Undergraduate (gardner@csus.edu)
8. Catalog Editor (catalog@csus.edu)
9. Registrar's Office (k.mcfarland@csus.edu)
10. PeopleSoft (PeopleSoft@csus.edu)

Approval Path

1. 2026-09-29T01:17:59Z
   Abeer Abdel Khaleq (abeer.abdelkhaleq): Rollback to Initiator
2. 2026-09-29T16:59:12Z
   Abeer Abdel Khaleq (abeer.abdelkhaleq): Approved for CSC Committee Chair
3. 2026-09-29T17:24:21Z
   Jinsong Ouyang (jouyang): Approved for CSC Chair
4. 2026-10-02T17:33:54Z
   Tongren Zhu (tongren.zhu): Approved for ECS College Committee Chair
5. 2026-10-02T17:51:10Z
   Behnam Arad (arad): Approved for ECS Dean

New Course Proposal

Date Submitted: 2026-09-29T01:26:44Z

Viewing: CSC 181 : Artificial Intelligence Security

Last edit: 2026-10-02T17:32:59Z

Changes proposed by: Syed Badruddoja (223024854)

Contact(s):

Name (First Last)	Email	Phone 999-999-9999
Syed Badruddoja	badruddoja@csus.edu	9162787328

Catalog Title:
Artificial Intelligence Security

Class Schedule Title:
AI Security

Academic Group: (College)
ECS - Engineering & Computer Science

Academic Organization: (Department)
Computer Science

Will this course be offered through the College of Continuing Education (CCE)?
No

Catalog Year Effective:
Fall 2027 (2027/2028 Catalog)

Subject Area: (prefix)
CSC - Computer Science

Catalog Number: (course number)
181

Course ID: (For administrative use only.)
TBD

Units:
3

Is the ONLY purpose of this change to update the term typically offered or the enforcement of existing requisites at registration?
No

In what term(s) will this course typically be offered?
Fall, Spring, Summer

Does this course require a room for its final exam?
Yes, final exam requires a room

Does this course replace an existing experimental course?
No

This course complies with the credit hour policy:
Yes

Justification for course proposal:
Artificial Intelligence (AI) is used in every other organization in the industry through industry platforms or self-developed tools. The security of these AI applications are flawed and require skilled professional. As an attempt to develop skilled workers, this course will allow students to learn AI security to secure AI applications in the society.

Course Description: (Not to exceed 90 words and language should conform to catalog copy.)
Fundamentals of adversarial attacks in Artificial Intelligence (AI). Supply chain, poisoning, evasion, model stealing attacks. Defending AI attacks using data provenance and adversarial training. Overview of privacy-preserving AI techniques including differential privacy and federated learning. Generative adversarial networks for deepfakes and synthetic data generation. Generative AI attacks, large language model (LLM) vulnerabilities and defense strategies.

Are one or more field trips required with this course?
No

Fee Course?
No

Is this course designated as Service Learning?
No

Is this course designated as Curricular Community Engaged Learning?
No

Does this course require safety training?
No

Does this course require personal protective equipment (PPE)?
No

Does this course have prerequisites?
Yes

Prerequisite:
CSC136, STAT50, not currently enrolled in CSC181

Prerequisites Enforced at Registration?
Yes

Does this course have corequisites?
No

Graded:
Letter

Approval required for enrollment?
No Approval Required

Course Component(s) and Classification(s):
Discussion

Discussion Classification
CS#02 - Lecture/Discussion (K-factor=1WTU per unit)
Discussion Units
3

Is this a paired course?
No

Is this course crosslisted?
No

Can this course be repeated for credit?
No

Can the course be taken for credit more than once during the same term?
No

Description of the Expected Learning Outcomes and Assessment Strategies:

List the Expected Learning Outcomes and their accompanying Assessment Strategies (e.g., portfolios, examinations, performances, pre-and post-tests, conferences with students, student papers). Click the plus sign to add a new row.

	Expected Learning Outcome	Assessment Strategies
1	Identify attacks and vulnerabilities in AI-based applications.	Homework 1, Programming Assignment 1, Exam
2	Analyze adversarial threats, model development and deployed AI attacks in machine learning operations.	Homework 2, Programming Assignment 2, Exam
3	Apply defense strategies and techniques to protect AI systems from supply-chain, algorithmic, and other attack-surface threats.	Homework 3, Programming Assignment 3, Exam
4	Apply privacy-preserving techniques to design secure AI models that protect against data leakage and model-stealing attack.	Homework 4, Programming Assignment 4 Programming Project, Exam
5	Identify the advanced attacks against large language models and generative AI systems	Class Activities, Exam

Attach a list of the required/recommended course readings and activities:
Syllabus_CSC181_Form_A.docx

For whom is this course being developed?
Majors in the Dept

Is this course required in a degree program (major, minor, graduate degree, certificate?)
No

Does the proposed change or addition cause a significant increase in the use of College or University resources (lab room, computer)?
No

Will there be any departments affected by this proposed course?
No

I/we as the author(s) of this course proposal agree to provide a new or updated accessibility checklist to the Dean's office prior to the semester when this course is taught utilizing the changes proposed here.

I/we agree

University Learning Goals

Undergraduate Learning Goals:

Competence in the disciplines
Knowledge of human cultures and the physical and natural world
Intellectual and practical skills
Personal and social responsibility
Integrative learning

Is this course required as part of a teaching credential program, a single subject, or multiple subject waiver program (e.g., Liberal Studies, Biology) or other school personnel preparation program (e.g., School of Nursing)?

No

Is this a General Education (GE) or Graduation Requirement (GR) course or is it being considered for GE/GR?

Is this a General Education (GE) course or is it being considered for GE?

No

Please attach any additional files not requested above:

ABET_CSC181_AI_Security .docx

Reviewer Comments:

Abeer Abdel Khaleq (abeer.abdelkhaleq) (Tue, 29 Sep 2026 01:17:59 GMT): Rollback: Please fix credit policy

Key: 15620