

A - New Course Proposal : Entry # 3687**DEAN Decision**

Approved

Date

09/21/2026

Is this course intracollegiate or intercollegiate?

Intracollegiate

SCHOOL EPC Decision

Approved

Date

10/15/2026

Begin Form**Today's Date**

09/02/2026

Your Name:

Kedrian James

Your Email:kjames4@highpoint.edu**Are you a Department Chair?**

No

Department Chair Name

Michael Oudshoorn

Email address of your Department Chairmoudshoo@highpoint.edu**By checking below, I certify that my department chair has seen and approved the new course that I am proposing.**

Yes

Please select the appropriate school overseeing this proposal:

Other

Please type the name of the school(s) overseeing this proposal

A - New Course Proposal : Entry # 3687

School of Engineering - Department of Computer Science

When should this proposal take effect?

Fall 2027

Information for the Registrar**Choose the department designator from the list below.**

CSC

Proposed Course Number?

2810

Is this course cross listed?

No

Does this course replace a current course?

No

What is the title of the new course?

Artificial Intelligence (AI) Security

Write the catalog description of your proposed course:

This course provides a practical, hands-on introduction to Artificial Intelligence (AI) and Large Language Model (LLM) security. Students examine the emerging threat landscape surrounding AI-enabled systems, including prompt injection, data leakage, model manipulation, and supply chain vulnerabilities. Emphasis is placed on understanding how AI systems expand the traditional attack surface and introduce novel risk categories not present in conventional software.

Through structured laboratory exercises, students will recreate AI-specific attacks, analyze real-world incidents, and design mitigation strategies, including input validation, output filtering, sandboxing, access control, and secure system architecture. The course prepares students to evaluate and secure AI-integrated applications in modern computing environments.

How many credit hours will this course be?

4

How will the course be graded?

Letter grade

Please select the course repeat option for this course:

Not repeatable for credit

What is the offering cycle for this course?

Fall semester

Does your course have any prerequisites?

A - New Course Proposal : Entry # 3687

Yes

Please list all prerequisites this course requires:

CSC 1720 Advanced Programming with Data Structures

Gen Ed and Academic Programs**Is this course part of Gen Ed?**

- No

Does this course count towards a major or a minor?

No, it does not count toward any particular major or minor

Is this course part of an academic program?

- This course does not fulfill academic program requirements

Does this course include any community engagement?

No

Does this course participate in the GoGlobal Program?

No

Information for Curriculum Review**Rationale and evidence for new course's consistency with departmental mission:**

CSC-2810 AI Security supports the Computer Science Department's mission by strengthening students' foundation in computing while preparing them to continually learn and respond to emerging technologies. The course introduces students to rapidly evolving security challenges in artificial intelligence and requires them to apply established computer science and cybersecurity principles to relevant problems involving AI-enabled systems. Through hands-on laboratories, threat modeling, vulnerability analysis, and secure system design, students develop the ability to evaluate computational problems and create solutions that are efficient, secure, and technically appropriate. The course also emphasizes responsible AI deployment, ethical decision-making, professional communication, and consideration of the broader consequences of insecure systems. In these ways, the course prepares students to adapt their knowledge to new technologies and solve modern computational problems securely and ethically.

Through applied laboratory exercises, assignments, and course projects, students will gain experience evaluating and securing AI-enabled systems for responsible deployment. Students will analyze security risks, make informed decisions about appropriate safeguards and mitigation strategies, communicate their findings through technical documentation and professional presentations, and consider the broader consequences of deploying insecure AI systems.

List all student learning outcomes for this course.

1. Analyze the AI/ML threat landscape and distinguish AI-specific security risks from traditional software vulnerabilities.
2. Evaluate vulnerabilities identified in the OWASP Top 10 for LLM Applications and assess their impact on AI-enabled systems.
3. Demonstrate prompt injection and jailbreak attacks in controlled laboratory environments and document the exploitation process.
4. Assess risks related to sensitive information disclosure, insecure output handling, and model misuse.

A - New Course Proposal : Entry # 3687

5. Implement mitigation strategies, including input validation, output filtering, sandboxing, and access control mechanisms.
6. Conduct structured security assessments of AI-integrated applications using basic threat modeling techniques.
7. Design secure AI system architectures that apply principles such as least privilege, isolation, and defense-in-depth.

List any units or content areas that will be required for all sections of this course.

Tentative Schedule of Topic Coverage:

Week Topics

- 1 AI Security Foundations & Threat Modeling
- 1 OWASP Top 10 for LLM Applications Overview
- 2 Prompt Injection Attacks & Mitigations
- 3 Insecure Output Handling & Data Leakage
- 4 Training Data Poisoning & Model Integrity
- 5 Model Denial of Service & Resource Attacks
- 6 Test 1
- 7 Supply Chain Vulnerabilities
- 8 Sensitive Information Disclosure
- 9 Insecure Plugin & Tool Design
- 10 Excessive Agency & Autonomous Agents
- 11 Overreliance & Hallucination Risks
- 12 Model Theft & Extraction
- 13 Test 2
- 14 AI Governance & Secure Architecture Design
- 15 Final Project Presentations

List any assignments, tests, or other assessments that will be required for all sections of this course.

Assessment: The final grade will be determined as follows:

Labs/Assignments/Quizzes: 25%
2-3 Major Tests: 30%
Class Project 20%
Final Project: 25%
Total: 100%

List any readings or other materials that will be required for all sections of this course.

Students will be expected to read and understand the OWASP Top 10 for Large Language Model Applications and explain the security risks, common vulnerabilities, and mitigation strategies associated with LLM-based systems. Additional readings, research articles, case studies, and technical documentation will be provided through the course learning management system.

List any course policies that will be required for all sections of this course.

The course will have the standard syllabus policies such as the following:

Academic Integrity Policy
Attendance Policy
Accessibility and Accommodations (Academic Services)
Title IX and Non-Discrimination Statement
Student Code of Conduct

If you would like to specify how requirements for contact hours must be met for all sections of this course, please indicate below. (e.g., if any experiential learning activities will replace seat time)

A - New Course Proposal : Entry # 3687

N/A

Sample Syllabus

- [CSC 2810 AI Security James-.pdf](#)