|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Quick Links** *(click to jump to section)* | | | | |
| [**Basic Info & Welcome**](#_Welcome_to_[INSERT) | [**Finding Resources**](#_How_to_Find) | [**Course Outcomes & Gen Ed Status**](#_Core_Learning_Outcomes) | [**Grades & Policies**](#_What_Will_You) | [**Assignments & Schedule**](#_How_Much_Time) |

# Welcome to the **AI Systems Protection and Governance** class at Frederick Community College!

|  |  |  |
| --- | --- | --- |
| **We Start:** 08/xx/202x | **We End:** 12/xx/202x | **We Meet:** Monday, Wednesday, Friday at 6:00 PM – 7:15 PM |
| **Our Classroom is:** C205, Catoctin Hall | | **Extra Fees:** N/A |

My name is Dr. Joshua Paiz**,** and I’ll be your instructor for this section. My contact info is below:

|  |  |
| --- | --- |
| **Email:** jpaiz@frederick.edu | **Phone:** (301) 624-2804 |
| **Office Room Number:** B228, Braddock Hall | **Mailbox:** B224 |
| **Office Hours:** Monday, Wednesday, Friday 4:30-5:30 PM and by appointment | |

# **Course Description**

CMIS 2XX *Introduction to Securing AI* is a 15-week course preparing students with CompTIA Security+ certification or equivalent cybersecurity experience for advanced study in AI security and, ultimately, the CompTIA SecAI+ certification exam. Students learn to secure AI systems and analyze adversarial risks through foundational concepts, hands-on labs, and real-world scenarios.

The course begins with core AI concepts including machine learning, deep learning, large language models, and retrieval-augmented generation to establish essential AI literacy. Students then focus on data and model protection strategies such as anonymization, watermarking, integrity validation, and secure lifecycle practices from development through deployment. Building on this foundation, students examine how attackers exploit AI, including through deepfakes, automated phishing, model poisoning, evasion, and prompt injection. Industry-standard frameworks such as the OWASP ML/LLM Top 10 and MITRE ATLAS are introduced to support structured threat modeling and risk assessment.

Weekly hands-on laboratories utilize accessible tools including Python/Jupyter Notebooks, scikit-learn/PyTorch, OWASP security frameworks, and the IBM Adversarial Robustness Toolbox. Assessments include quizzes, performance-based drills, and a midterm exam. Students leave the course prepared with the knowledge and practical skills to identify AI-specific threats and vulnerabilities and to continue into SecAI II for advanced defenses, governance, and compliance practices.

# **Welcome Message**

# Welcome to *Intro to Securing AI*! We are delighted to have you join us in exploring the critical intersection of artificial intelligence and cybersecurity, where we strive to create a collaborative and inclusive learning environment that highly values your diverse professional and academic backgrounds and experiences.

# Whether you come from traditional cybersecurity, software development, or other IT disciplines, we wholeheartedly encourage your active participation in discussions, hands-on laboratories, and the sharing of real-world scenarios, as your curiosity-driven questions about AI security challenges and defensive strategies will enrich our collective understanding of this rapidly evolving field.

# We are genuinely excited to support you as you develop specialized skills, prepare for CompTIA SecAI+ certification, and build both technical expertise and professional networks that extend beyond the classroom—let's create a supportive learning community where we can tackle complex problems together and help each other succeed in this high-demand specialization!

# **About FCC’s Commitment to Equity**

It’s FCC's mission to serve students from all diverse backgrounds and perspectives; to address students’ learning needs; and to respect students' identities, including sexuality, gender identity and expression, disability, age, religion, socio-economic status, ethnicity, race, and culture.

While I will do my part to ensure that all students are seen, heard, and valued, your suggestions on how to make this class an inclusive space are encouraged and appreciated. Please let me know ways to improve the effectiveness of the course for you personally or for other students or student groups. In addition, if any of our class meetings conflict with your religious events, please let me know so that we can make arrangements.   
*(adapted from FCC's Diversity statement and Montgomery College)*

# **What You’ll Need for This Course**

# Textbook: The required materials, provided by the instructor under the Fair Use Doctrine (17 USC 107), can be found on Blackboard. Other Learning Materials: Available on the course Blackboard site. Other Required Equipment or Materials: (1) Access to the internet to complete coursework on Blackboard. (2) The use of Microsoft Office 365 suite (including Word, Excel, and PowerPoint). FCC students and employees can install Microsoft Office 365 on their devices at no cost. To gain access to your free software, please go to Office365. (3) A coding environment set up for Python and with the requisite libraries installed/configured, including scikit-learn, PyTorch (CPU is sufficient), and Jupyter Notebooks. (4) Optional: a USB drive to save work if you complete work on a public computer. Note: Most labs in SecAI I will run on modest hardware; GPU access is not required.

# **How to Find Resources at FCC**

If you need any of the supplies listed above, the FCC Bookstore is a good place to start. But that’s not all! FCC has a wide range of resources available to you – from advising and tutoring, to mental health resources and food lockers, to a writing center and support services, and everything in between. Explore the options [online](https://www.frederick.edu/student-resources/student-resources.aspx), in [Navigate](https://www.frederick.edu/navigate.aspx), and in Blackboard, and don’t be afraid to use them; they’re here to help.

FCC’s also committed to making sure all students can get the most out of our courses, including those with disabilities (including learning, attention, hearing, vision, psychological, chronic medical, and more) in need of accommodations. If you have an accommodation plan, be sure to share it and discuss your needs with your instructor. **Do this as soon as possible** - the accommodations don’t happen until the plan is shared with your instructor. If you’re not yet registered for a plan and/or want more information on accommodations, you can learn details, find contact information, and [request services](https://frederick-accommodate.symplicity.com/public_accommodation/) at [our website](https://www.frederick.edu/student-resources/das.aspx).

*(Click to* [*return to first page*](#_top)*)*

# **Core Learning Outcomes**

By successfully completing this course, you will be able to:

# **Describe and explain** foundational AI concepts (ML, DL, LLMs, RAG) and their relevance to cybersecurity.

# **Identify and analyze** threats and vulnerabilities unique to AI/AI-enabled systems (e.g., poisoning, model theft, prompt injection).

# **Examine and explain** how attackers can leverage AI to carry out exploits such as deepfakes, phishing, and large-scale social engineering.

# **Apply and evaluate** basic data security practices across the AI development lifecycle (anonymization, watermarking, validation).

# **Conduct and interpret** AI-specific threat modeling and risk assessments using frameworks (OWASP, MITRE ATLAS, STRIDE).

# **Demonstrate competency** through exam-style MCQs, labs, and a practicum project.

# **Additional Course Info**

This course can also satisfy these Gen Ed requirements (if two are listed, it can only satisfy one or the other):

|  |  |
| --- | --- |
| Gen Ed Type 1: N/A | Gen Ed Type 2: N/A |
| FCC Cultural Competence? No | |

*(Click to* [*return to first page*](#_top)*)*

# **What’s Getting Graded?**

|  |  |  |
| --- | --- | --- |
| Tests/Papers/Projects/Participation | CLOs Assessed | Points |
| Bi-weekly Quizzes (5 total) | 1–5 | 150 |
| Hands-on Labs & Performance-Based Drills (10 labs) | 2, 3, 4, 5 | 250 |
| Midterm Exam (Domains 1–2) | 1–5 | 150 |
| Mini-Project: AI Threat Modeling (Week 4) | 2, 4, 5 | 100 |
| Practicum: Adversarial Attack & Defense (Week 12–14) | 2, 3, 5 | 200 |
| Participation & Engagement (weekly) | 1–6 | 150 |
| Grand Total |  | **1,000** |

# **Final Grade Scale:** 900–1,000 = A • 800–899 = B • 700–799 = C • 600–699 = D • ≤599 = F

# **Participation Policy and Expectations**

Note: Your instructors are required to report student attendance at the beginning of the session and no later than the day after the 100% refund date (you can find that later in the syllabus). FCC will not disburse Federal Student Aid to students until your instructor confirms your attendance.

1. This is a hybrid course. This means that the class will have both in-person and online components. Students are expected to participate fully in all instructional and educational activities across all modalities.
2. There are 15 weeks in this class. Each instructional week begins on **Saturday and ends on Friday**, which aligns with FCC’s academic calendar. This course meets on Mondays, Wednesdays, and Fridays. Students are expected to log into Blackboard and read assigned materials before the class for which they are assigned.
3. All quizzes, exams, labs, and assignments are due by **11:59 PM Eastern on the date listed in Blackboard**. In Week 15, due dates will follow the official end-of-term schedule; no assignments can be accepted after the college’s final grade submission deadline.
4. It is imperative that students engage and participate fully in all course activities and maintain the highest quality of academic work.
5. Time management is an important skill. Missed work cannot be made up without appropriate permission secured in advance—extensions are provided on a case-by-case basis based upon the merits of the case and at the professor’s discretion.
6. In case of serious illness, emergency, religious holidays, or participation in official college functions, students remain responsible for completing the requirements of the course.
7. Labs are designed to be started in class with instructor support. Depending on the lab, additional work outside of class may be required; students will typically have until the end of that instructional week (Friday at 11:59 PM Eastern) to submit lab write-ups.
8. As your professor has been called a “nerd” in the past, an ongoing bonus opportunity is available to you. He will wear a pin to each class from a classic Sci-Fi series. At the end of each class meeting, you will be awarded 1 point if you can ID what specific series/movie the pin comes from and 1 additional point if you can provide an additional detail about what the pin’s in-universe significance. Responses are to be sent from your FCC email to mine.
9. Be active contributors during **lab sessions** and group exercises.
10. Share troubleshooting and threat modeling strategies in team settings.
11. Submit **weekly reflection check-ins** via Blackboard.
12. Failure to engage in labs or discussions will reduce participation credit.
13. At the end of the course, students are expected to complete the course evaluation. Student feedback is anonymous. This information will be used to improve the course.

**Additional Expectation for SecAI I:** Active participation is especially important during lab sessions and in-class drills. Students are expected to work collaboratively with their peers, share troubleshooting approaches, and contribute to group threat modeling and adversarial exercises. Attendance and participation in these sessions are part of your overall engagement grade.

|  |
| --- |
| **College-Wide Expectations**  As an FCC student, you’ll be expected to abide by the [Code of Student Conduct](https://www.frederick.edu/jobs-hr/policies-and-procedures/policyproceduredocuments/code-of-student-conduct.aspx). Basically, we expect you to act with integrity, treat others with respect, and avoid plagiarism, cheating, and other academic dishonesty (visit the [link](https://www.frederick.edu/jobs-hr/policies-and-procedures/policyproceduredocuments/code-of-student-conduct.aspx), page 7, to see some examples of what counts).  And you can expect to be treated honestly, fairly, and respectfully, as well. Your records will stay private (see our [FERPA protections](https://www.frederick.edu/jobs-hr/policies-and-procedures/policyproceduredocuments/ferpa.aspx)), you’ll be free from discrimination in all we do, and you’ll always be empowered to participate and give honest feedback on your experiences. Thank you for helping make our FCC community one where everyone is able to thrive. |

# **Tracking How You’re Doing in the Course**

I will maintain grading information in Blackboard under the “My Grades” tab. Students are responsible for keeping track of this information. Likewise, I will provide feedback to the class on their work through Blackboard (“Feedback on Assignments” 🡪 “Feedback on Assignment X”). Students desiring additional/personalized feedback are required to make an appointment with me during my student hours so that we can discuss your work at length and work together to develop an actionable plan for your continued development and improvement. Typical turnaround times for short assignments (e.g., weekly assignments) is 3-5 business days; typical times for more intensive assignments is 7-10 business days.

Contacting Your Instructor

When you enrolled at FCC, you received a myFCC email address – be sure to [set up that email](https://myfcc.frederick.edu/portal.aspx) if you haven’t done so already. You’ll need to use that email when you’re communicating with your instructor or other FCC employees, and it’s the one they’ll use to contact you too. In addition to being listed [above](#_Welcome_to_[INSERT), you’ll also be able to find your instructor’s email in Blackboard. (Your classmates’ myFCC emails will be there as well.) You should expect your instructor to respond to regular email messages in about 1-2 business days.

**IMPORTANT:** All College email communication will use your myFCC email address, so be sure to check it often.

Final Grades

When your instructor submits your final grade, the Registrar's Office will post it in your PeopleSoft student account records. You can use that student account to see your grades, view your transcript, or request an official transcript anytime. The grades that appear in PeopleSoft—not the ones in Blackboard—are your official grades.

Thinking of Withdrawing?

If you’re considering [withdrawing from the course](https://www.frederick.edu/admissions/registration-records/withdrawal-advising.aspx), be sure to talk to your instructor, an advisor, and financial aid about it before you do! There are important deadlines that help determine what effect it might have on your transcript and whether you get a tuition refund. Withdrawing also doesn’t automatically stop you from being charged for the class; there are a lot of details that matter. Let us know your situation as soon as possible, and we can help ensure you’ve got all the information and support to make the best decision.

|  |  |
| --- | --- |
| **Last Day for 100% Refund:** 08/xx/20xx *The course will no longer appear on your transcript.* **Last Day for 50% Refund:** 09/xx/20xx *You’ll get a “W” on your transcript.* | **Last Day to Withdraw or Audit:** 10/xx/20xx *If you withdraw, you’ll get a “W;” if you audit, an “AU.”* |

# **How to Submit a Complaint**

If you have a negative experience, we’d love to learn more about what happened – feedback is an important part of making our courses better for everyone. Your first step should be reaching out to your instructor to try and resolve the issue. If you can’t find a solution with them, your next step is to contact the AVP/Dean of the School. Their contact information is:

|  |  |
| --- | --- |
| **Name:** Christanne Aranguren | **Role:** AVP/Dean, School of TTBH |
| **Email:** [caranguren@frederick.edu](mailto:caranguren@frederick.edu) | **Phone:** 240-624-2804 |
| **Office Room Number:** B225, Bradock Hall |  |

If you still can’t find a good solution, we also have an [official complaint process](https://www.frederick.edu/jobs-hr/policies-and-procedures/policyproceduredocuments/complaint-policy-procedure-for-students.aspx) that’s open to all students. We also have a specific procedure if your complaint is [related to Title IX issues](https://www.frederick.edu/jobs-hr/policies-and-procedures/policyproceduredocuments/titleix.aspx) (discrimination, harassment, etc. based on sex or gender), and another if your complaint is [related to discrimination for any other reason](https://www.frederick.edu/jobs-hr/policies-and-procedures/policyproceduredocuments/non-discrimination.aspx).

No matter what the result, thank you! We appreciate you taking the time to talk to us about the challenge.

*(Click to* [*return to first page*](#_top)*)*

# **How Much Time Should You Expect to Spend on this Course?**

|  |  |  |  |
| --- | --- | --- | --- |
| Out-of-Class Work Summary | Time Required | Frequency | Total Time |
| Reading & note-taking | 1.5 hrs | 15 times | 22.5 hrs |
| Quiz prep & completion | 1 hr | 5 times | 5 hrs |
| Lab prep & write-ups | 1.5 hrs | 10 times | 15 hrs |
| Midterm prep & completion | 8 hrs | 1 time | 8 hrs |
| Mini-project: Threat Modeling | 10 hrs | 1 time | 10 hrs |
| Practicum project (attack/defense) | 25 hrs | 1 time | 25 hrs |
| Weekly reflections/discussions | 0.5 hrs | 15 times | 7.5 hrs |
| Additional case study reviews | 1 hr | 10 times | 10 hrs |
| Grand Total |  |  | **103 hrs → scale up to 120 hrs with added lab reflections & practice sets** |

Note that these are *estimates*, the amount of time you need to spend on each item will vary based upon individual effects.

***Continued on Next Page***

# **Course Outline and Assignment Schedule:** What’s Happening and When?

Please know that your instructor may change this schedule if the need arises. If that happens, they’ll let you know what’s changing and why.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Week | Monday (Lecture) | Wednesday (Lab/Applied) | Friday (Lecture/Discussion) | Assessments & Milestones | CLOs |
| 1 | Course intro; SecAI+ domains; AI security vs. AI for cybersecurity; ethics overview | Lab 1: Environment setup + AI risk scavenger hunt (individual) | Real-world AI security examples; tooling landscape | Lab 1 due Fri | 1, 6 |
| 2 | AI fundamentals: ML, DL, transformers, NLP/CV basics | Lab 2: Train & evaluate simple classifier (individual) | Training concepts: supervised/unsupervised, validation, overfitting, fine-tuning | Quiz 1 due Sun; Lab 2 due Fri | 1, 3 |
| 3 | Data security: types, cleansing, integrity, provenance, watermarking | Lab 3: Data anonymization & integrity validation (individual) | AI lifecycle security: secure development through deployment; intro to RAG | Lab 3 due Fri | 1, 4 |
| 4 | Threat modeling: OWASP ML/LLM Top 10, MITRE ATLAS, STRIDE for AI | Lab 4: AI threat modeling workshop (team) | Risk assessment frameworks; threat-to-control mapping | Quiz 2 due Sun; Mini-Project assigned | 2, 5, 6 |
| 5 | AI in attackers’ hands: deepfakes, automated phishing, OSINT at scale | Lab 5: Adversarial content generation (team) | Malware optimization & exploit discovery | Lab 5 due Fri | 2, 3 |
| 6 | Model attacks: poisoning & evasion | Lab 6: Attack simulation (team) | Model inversion & membership inference | Quiz 3 due Sun; Lab 6 due Fri | 2, 3, 5 |
| 7 | Jailbreaking & prompt injection | Lab 7: Prompt injection defense (individual) | Model theft strategies & data exfiltration | Mini-Project due Fri | 2, 3, 5 |
| 8 | Securing models: guardrails, templates, safety evaluations | Lab 8: Guardrail & filter implementation (individual) | Securing interfaces: prompt firewalls & token limits | Lab 8 due Fri | 2, 4 |
| 9 | Access control for AI: roles, permissions, repository security | Lab 9: Access control workshop (individual) | Data protection: encryption, masking, minimization | Quiz 4 due Sun; Lab 9 due Fri | 2, 4 |
| 10 | Monitoring & logging for AI systems | Lab 10: Log setup & drift detection (individual) | Incident response playbooks for AI | Practicum assigned | 4, 6 |
| 11 | Midterm review & practice | **Midterm Exam (Domains 1–2)** | Debrief & reflection | Practicum work week | 1–6 |
| 12 | Case studies: adversarial ML in the wild | Lab 11: Adversarial ML case analysis | Defensive countermeasures (intro) | Practicum progress check | 2, 3 |
| 13 | Case studies: AI-enabled attacks (deepfake incidents, phishing) | Lab 12: Attack reproduction & analysis | Defensive implications | Quiz 5 due Sun; Lab 12 due Fri | 2, 5 |
| 14 | Pulling it together: AI-specific risk assessments | Lab 13: Group threat modeling exercise | Connecting course themes | Practicum prep & review | 1–6 |
| 15 | Student Practicum Presentations | Wrap-up discussion | Exam prep review | Practicum due; Final reflection | 1–6 |

Note 1: This is a living document and subject to update as needed at the discretion of the professor to meet the needs of our learning community.

Note 2: PBT 🡪 Performance-based; MCQ 🡪 Multiple Choice Questions

Note 3: If you feel that you are struggling, it is up to you to take advantage of the support resources made available to you (e.g., STEM Lab, Student Hours, etc.). You need to do so in a timely manner. My ability to effectively support you diminishes the closer we get to the end of term.

|  |  |
| --- | --- |
| **Important Date(s)** | **Description** |
| TBD | On-Campus Emergency Drills - see Drill Schedule for type of drill and time |
| TBD | College Holidays/Breaks with no Classes |
| TBD | Last Date to Drop with a 100% refund |
| TBD | Last Date to Withdraw with a 50% refund |
| TBD | Last Date to Withdraw/Audit the Course |
| TBD | Course Evaluation Dates |

*(Click to* [*return to first page*](#_top)*)*