|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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, Advanced AI Security is a 15-week advanced course preparing students who have completed SecAI I (or equivalent experience) to master defensive strategies, governance, and compliance for AI systems in preparation for the CompTIA SecAI+ certification exam. Students deepen their ability to secure AI environments and leverage AI tools for cybersecurity operations through extended labs, advanced frameworks, and a team-based capstone project.

The course begins with robust defensive measures, including guardrails, prompt firewalls, access controls, encryption, anomaly detection, and secure model interfaces. Students then learn to integrate AI-assisted security workflows, applying AI models for automated code analysis, log monitoring, vulnerability scanning, and CI/CD pipeline integration. Beyond technical defenses, students engage with responsible AI practices and governance structures, exploring human oversight, vendor risk management, and global regulatory frameworks such as the NIST AI Risk Management Framework, the EU AI Act, and ISO/IEC standards.

Weekly hands-on laboratories and performance-based drills reinforce technical skills, while a 7–10 week capstone project requires students to secure an AI-enabled application or design an AI-assisted defense strategy for a real-world scenario. Students conclude the course with practical, policy-aware expertise directly applicable to industry needs and the SecAI+ exam domains.

# **Welcome Message**

# Welcome to *Advanced AI Security*! 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 and case studies, 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 configured for Python with advanced libraries including scikit-learn, PyTorch, Hugging Face transformers, and the IBM Adversarial Robustness Toolbox. (4) Access to either cloud-based compute resources (e.g., Google Colab, AWS Academy, or equivalent) or a local machine capable of running medium-sized ML models. (5) Optional: a USB drive to save work if you complete work on a public computer. Note: SecAI II labs and the capstone project may involve larger models or extended runtime; cloud resources are recommended for these tasks.

# **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:

# **Design and implement** defensive strategies for AI systems (guardrails, prompt firewalls, anomaly detection).

# **Apply and justify** advanced data security controls (encryption, minimization, redaction).

# **Utilize and assess** AI-driven tools for security operations (automated analysis, vulnerability scanning, CI/CD).

# **Develop and execute** monitoring, logging, and incident response procedures for AI.

# **Evaluate and apply** governance frameworks (NIST RMF, EU AI Act, ISO/IEC) in cybersecurity contexts.

# **Critique and integrate** responsible AI practices (fairness, transparency, accountability) into workflows.

# **Produce and present** a capstone project demonstrating integrated technical, ethical, and compliance skills.

# **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 |
| Quizzes (3 total) | 1–6 | 150 |
| Hands-on Labs & Performance-Based Drills (10 labs) | 1–5 | 250 |
| Final Exam (comprehensive) | 1–7 | 150 |
| Compliance Mapping Brief (Week 10) | 5 | 100 |
| Capstone Project (proposal, build, report, presentation) | 1–7 | 250 |
| Participation & Engagement (weekly + peer feedback) | 1–7 | 100 |
| 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. Contribute meaningfully to **team capstone work** and document weekly progress.
10. Attend **all peer capstone presentations** and provide at least **two substantive feedback comments/questions** per session.
11. Engage respectfully in discussions on governance, compliance, and responsible AI practices.
12. Failure to participate in capstone presentations or peer feedback will result in a loss of 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 II:** Active participation extends to the capstone project. Students are expected to contribute meaningfully to their project team, document progress weekly, and support classmates by being present and engaged during peer capstone presentations. Professional feedback and questions posed to peers during presentations are a graded component of participation.

|  |
| --- |
| **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 | 12 times | 18 hrs |
| Quiz prep & completion | 1 hr | 3 times | 3 hrs |
| Lab prep & write-ups | 1.5 hrs | 10 times | 15 hrs |
| Final exam prep & completion | 10 hrs | 1 time | 10 hrs |
| Compliance Mapping Brief | 12 hrs | 1 time | 12 hrs |
| Capstone project (proposal, build, report, presentation) | 45 hrs | 1 time | 45 hrs |
| Weekly reflections/discussions | 0.5 hrs | 15 times | 7.5 hrs |
| Peer presentation prep/feedback | 1 hr | 8 times | 8 hrs |
| Grand Total |  |  | **118.5 hrs (rounds to 120)** |

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 | Intro & review; defensive posture for AI | Lab 1: Guardrails refresher | Access control & auth for APIs | Lab 1 due Fri | 1, 2 |
| 2 | Encryption: rest, transit, in-use | Lab 2: Encryption & redaction | Data minimization strategies | Quiz 1 due Sun; Lab 2 due Fri | 2 |
| 3 | AI monitoring & anomaly detection | Lab 3: Drift detection setup | SIEM integration for AI | Lab 3 due Fri | 4 |
| 4 | Audit trails & IR playbooks | Lab 4: AI-specific IR design | Incident simulations | Lab 4 due Fri | 4 |
| 5 | AI-assisted security ops: code analysis | Lab 5: Automated code scanning | Use cases & risks | Quiz 2 due Sun; Lab 5 due Fri | 3 |
| 6 | AI-assisted ops: log & anomaly detection | Lab 6: Automated log triage | CI/CD integration | Lab 6 due Fri | 3, 4 |
| 7 | Governance structures: Centers of Excellence | Lab 7: Governance framework design (team) | Shadow AI & vendor risk | Capstone teams formed | 5 |
| 8 | Responsible AI: fairness & transparency | Lab 8: Bias audit | Accountability principles | Capstone proposal due Fri | 6 |
| 9 | NIST AI RMF deep dive | Lab 9: RMF risk assessment | Operational integration | Quiz 3 due Sun; Lab 9 due Fri | 5, 6 |
| 10 | Global compliance: EU AI Act | Lab 10: Compliance mapping (team) | OECD & ISO standards | Compliance brief assigned | 5 |
| 11 | Corporate audit readiness | Lab 11: Audit simulation | Documentation strategies | Compliance brief due Fri | 5 |
| 12 | Advanced defenses: layered AI security | Lab 12: Final defensive build | Case study application | Lab 12 due Fri | 1–6 |
| 13 | Capstone work week (team-based) | Capstone work session | Peer check-ins | Capstone progress report due | 1–7 |
| 14 | Capstone presentations (Groups A & B) | Capstone presentations (Groups C & D) | Peer feedback sessions | Capstone deliverables due Fri | 1–7 |
| 15 | Comprehensive review | **Final Exam** | Reflection & future learning | Course evaluations due | 1–7 |

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)*)*