Program Guidebook

Bachelor of Science, AI Security

Program Code: BSAISEC Catalog Version: 202701 Published Date: 9/2/2026

As organizations increasingly deploy artificial intelligence (AI) systems across industries, the Bachelor of Science in AI Security (BSAISEC) degree program prepares technology professionals to secure AI-enabled applications, models, data, and infrastructure. Courses deliver proven methods for protecting AI systems throughout their lifecycle through topics such as machine learning security, adversarial defense, secure software development, cloud security, data analytics, cryptography, privacy-preserving technologies, AI governance, risk management, and threat modeling. Students learn to identify, prevent, detect, and mitigate threats targeting machine learning models, data pipelines, autonomous systems, and AI-powered applications through hands-on application of cybersecurity and secure engineering practices. This program prepares graduates for emerging careers at the intersection of artificial intelligence and cybersecurity, equipping them with the skills needed to address the evolving security challenges of AI-enabled environments.

Understanding the Competency-Based Approach

How do competency-based programs like those offered at Western Governors University (WGU) work? Unlike traditional universities, WGU does not award degrees based on completing a certain number of credit hours or a specific set of required courses. Instead, you will earn your degree by demonstrating your skills, knowledge, and understanding of essential concepts.

Progress through a degree program is measured not by the amount of time you spend in class but by your ability to demonstrate competency as you complete required courses along a Standard Path. To help you acquire the knowledge and skills you need to demonstrate competency and complete your courses and program, WGU provides a rich array of learning resources. Your program mentor will work closely with you to help you understand your program's requirements and help you create a plan for completing your courses. You will also work closely with course instructors as you engage in each course. As subject matter experts, course instructors will guide you through the content you must learn to demonstrate competency through the course assessments.

The benefit of this competency-based system is that it enables students who are knowledgeable about a particular subject to make accelerated progress toward completing a degree, even if they lack college experience. You may have gained skills and knowledge of a subject while on the job, accumulated wisdom through years of life experience, or already taken a course on a particular subject. WGU will award your degree based on the skills and knowledge you possess and can demonstrate—not the number of hours spent in a classroom.

Accreditation

Western Governors University is the only university in the history of American higher education to have earned initial accreditation from multiple regional accrediting commissions at once—earning simultaneous accreditation from ACCJC, HLC, NWCCU, and WASC. The university's accreditation from the Northwest Commission on Colleges and Universities (NWCCU) was reaffirmed in March of 2024. In addition to institution-level accreditation, each school has at least one program that is accredited by a programmatic accreditation. All programmatic accreditations are managed by the Academic Engagement department. Contact compliance@wgu.edu for additional information.

The Degree Plan

The focus of your program is your personalized Degree Plan. The Degree Plan is a detailed blueprint of the courses you will need to complete in order to earn your degree. The Degree Plan also lays out the accompanying learning resources and assessments that compose your program. The list of courses in the Degree Plan is often referred to as the standard path. The amount of time it takes to complete your program depends on both the amount of new information you need to learn and the amount of time you plan to devote each week to study. Your program mentor and course instructors will help you assess your strengths and development needs to establish a study plan.

Students vary widely in the specific skills and information they need to learn. For example, some students may be highly knowledgeable in a particular subject matter and would not need to engage in new learning opportunities. Other students may find that portions of the program require them to learn new information and that they need to take an online class or participate in a study module to acquire the knowledge and skills needed to fulfill program competencies in that area. Some individuals may be able to devote as little as 15–20 hours per week to the program, while others may need to devote more time. For this reason, pre-assessments are there to help your program mentor form a profile of your prior knowledge and create a personalized Degree Plan.

How You Will Interact with Faculty

At WGU, faculty serve in specialized roles, and they will work with you individually to provide the guidance, instruction, and support you will need to succeed and graduate. As a student, it is important for you to take advantage of this support. It is key to your progress and ultimate success.

Upon your enrollment, you will be assigned a program mentor—an expert in your field of study who will provide you with regular program-level guidance and support from the day you start until the day you graduate. Your program mentor will set up regular telephone appointments (weekly at first) with you, which you will be expected to keep. The mentor will review program competencies with you and work with you to develop a plan and schedule for your coursework. Your program mentor will serve as your main point of contact throughout your program—helping you set weekly study goals, recommending specific learning materials, telling you what to expect in courses, and keeping you motivated. In addition to regular calls, your program mentor is available to help you resolve questions and concerns as they arise.

For many of the courses at WGU, you will be required to complete performance assessments. These include reports, papers, presentations, and projects that let you demonstrate your mastery of the required competencies. A separate group of faculty members, called evaluators, will review your work to determine whether it meets requirements. Evaluators are also subject matter experts in their field of evaluation. If your assessment needs further work before it “passes,” these evaluators, who review your work anonymously, will provide you with instructional feedback to help you meet evaluation standards and allow you to advance.

Connecting with Other Mentors and Fellow Students

As you proceed through your Degree Plan, you will have direct contact with multiple faculty members. These communications can take a variety of forms, including participation in one-on-one discussions, chats in the learning communities, and live cohort and webinar opportunities. As a WGU student, you will have access to your own personal MyWGU Student Portal, which will provide a gateway to your courses of study, learning resources, and learning communities where you will interact with faculty and other students.

The learning resources in each course are specifically designed to support you as you develop competencies in preparation for your assessments. These learning resources may include reading materials, videos, tutorials, cohort opportunities, community discussions, and live discussions that are guided by course instructors who are experts in their field. You will access your program community during your orientation course to network with peers who are enrolled in your program and to receive continued support through professional enrichment and program-specific chats, blogs, and discussions. WGU also provides Student Services associates to help you and your program mentor solve any special problems that may arise.

Orientation

The WGU Orientation course will introduce you to the fundamentals of WGU’s competency-based education (CBE) and the expectations, policies, and protocols for students enrolled in a WGU degree program. Orientation will introduce you to WGU’s wide range of support resources and success centers. It also will provide you with study strategies recommended by current students and faculty that will help you succeed as a WGU student. Orientation ends with your first assessment at WGU, providing an opportunity to experience WGU’s performance assessment process before you begin your degree-focused coursework. The Orientation course must be completed before you can start your first term at WGU.

Transferability of Prior College Coursework

Because WGU is a competency-based institution, it does not award degrees based on credits but rather on demonstration of competency. WGU undergraduate programs may accept transfer credits or apply a ‘Requirement Satisfied’ (RS) in some cases. Refer to your specific program transfer guidelines to determine what can be satisfied by previously earned college credits. Students

entering graduate programs must have their undergraduate degree transcripts verified before being admitted to WGU. In addition to a program's standard course path, there may be additional state-specific requirements.

WGU Student Policy Handbook

WGU does not waive any requirements based on a student's professional experience and does not perform a "résumé review" or "portfolio review" that will automatically waive any degree requirements. Degree requirements and transferability rules are subject to change in order to keep the degree content relevant and current.

Remember, WGU's competency-based approach lets you take advantage of your knowledge and skills, regardless of how you obtained them. Even when you do not directly receive credit, the knowledge you possess may help you accelerate the time it takes to complete your degree program.

Continuous Enrollment, On Time Progress, and Satisfactory Academic Progress

WGU is a "continuous enrollment" institution, which means you will be automatically enrolled in each of your new terms while you are at WGU. Each term is six months long. Longer terms and continuous enrollment allow you to focus on your studies without the hassle of unnatural breaks between terms that you would experience at a more traditional university. At the end of every six-month term, you and your program mentor will review the progress you have made and revise your Degree Plan for your next six-month term.

WGU requires that students make measurable progress toward the completion of their degree programs every term. We call this "On-Time Progress," denoting that you are on track and making progress toward on-time graduation. As full-time students, graduate students must enroll in at least 8 competency units each term, and undergraduate students must enroll in at least 12 competency units each term. Completing at least these minimum enrollments is essential to On-Time Progress and serves as a baseline from which you may accelerate your program. We measure your progress based on the courses you are able to pass, not on your accumulation of credit hours or course grades. Every time you pass a course, you are demonstrating that you have mastered skills and knowledge in your degree program. For comparison to traditional grading systems, passing a course means you have demonstrated competency equivalent to a "B" grade or better.

WGU assigns competency units to each course in order to track your progress through the program. A competency unit is equivalent to one semester credit of learning. Some courses may be assigned 3 competency units while others may be as large as 12 competency units.

Satisfactory Academic Progress (SAP) is particularly important to students on financial aid because you must achieve SAP in order to maintain eligibility for financial aid. We will measure your SAP quantitatively by reviewing the number of competency units you have completed each term. In order to remain in good academic standing, you must complete at least 66.67% of the units you attempt over the length of your program—including any courses you add to your term to accelerate your progress. Additionally, during your first term at WGU you must pass at least 3 competency units in order to remain eligible for financial aid. We know that SAP is complex, so please contact a financial aid counselor should you have additional questions.

Courses

Your Degree Plan includes courses needed to complete your program. To obtain your degree, you must demonstrate your skills and knowledge by completing each course's assessment(s). You may be asked to demonstrate competency in a course in several different ways, including proctored exams, projects, essays, research papers, and simulations, among others. Certifications verified through third parties may also be included in your program as a way to demonstrate competency. More detailed information about each assessment is provided in the course of study.

Learning Resources

WGU works with many different educational partners, including enterprises, publishers, training companies, and higher educational institutions, to provide high-quality and effective learning resources that match the competencies you are developing. These vary in type and may be combined to create the best learning experience for your course. A learning resource can be an e-textbook, online module, study guide, simulation, virtual lab, tutorial, or a combination of these. The cost of most learning resources is included in your tuition and Resource Fee. They can be accessed or enrolled for through your courses. Some degree-specific resources may not be covered by your tuition, and you will need to cover those costs separately. WGU also provides a robust library to help you obtain additional learning resources, as needed.

The following Student Handbook article provides additional details about the current state of mobile compatibility for learning resources at WGU:

Mobile Access for Learning Resources

Program Learning Outcomes

1. Navigate the legal and ethical considerations specific to AI security, including privacy, accountability, and the impact of AI on society.
2. Grasp the core principles of AI, including machine learning, neural networks, and data science, which underpin AI systems.
3. Identify and analyze potential vulnerabilities in AI models, including data poisoning, adversarial attacks, and model inversion.
4. Implement security measures throughout the AI development pipeline, from data collection and preprocessing to model training, deployment, and maintenance.
5. Develop strategies to protect AI models from adversarial attacks, which involve malicious inputs crafted to deceive the AI system.
6. Protect the integrity and confidentiality of the data used in AI systems, ensuring that the data is free from tampering and bias.
7. Identify and mitigate bias in AI systems to ensure fair and ethical outcomes, especially in high-stakes applications.
8. Create AI systems resilient to attacks, errors, and other disruptions, ensuring reliable and secure performance in various environments.
9. Monitor AI systems to detect and respond to security threats, performance degradation, and unexpected behaviors.
10. Produce professional security assessments that communicate AI system risk to both technical and non-technical stakeholders.

General Education Program Learning Outcomes

- Communication and Composition: The learner will be able to communicate through basic oral, written, visual methods, and contemporary digital communication technologies.
- Humanities and Social Sciences: The learner will be able to use concepts and methods of historical and humanistic inquiry to answer real-world questions.
- Science: The learner will be able to use the concepts and methods of scientific inquiry to solve real-world problems.
- Mathematics and Problem-Solving: The learner will be able to use quantitative reasoning and problem-solving skills in the analysis, interpretation, and explanation of real-world data and approaches to solutions.

Standard Path

As previously mentioned, competency units (CUs) have been assigned to each course in order to measure your academic progress. If you are an undergraduate student, you will be expected to enroll in a minimum of 12 competency units each term. Graduate students are expected to enroll in a minimum of 8 competency units each term. A standard plan for a student for this program who entered WGU without any transfer units would look similar to the one on the following page. Your personal progress can be faster, but your pace will be determined by the extent of your transfer units, your time commitment, and your determination to proceed at a faster rate.

Standard Path *for* Bachelor of Science, AI Security

Course Title	CUs	Term
Health, Fitness, and Wellness	4	1
Introduction to Computer Science	4	1
Composition: Successful Self-Expression	3	1
Practical Applications of Prompt	2	1
Foundations of Programming (Python)	3	2
Applied Probability and Statistics	3	2
Networks	4	2
Fundamentals of Information Security	3	2
Version Control	1	3
Mathematics for Programmers	3	3
Ethics in Technology	3	3
Object Oriented Programming in Python	3	3
Applied Algebra	3	3
Introduction to AI Coding Assistants	2	4
Python for IT Automation	3	4
Network and Security - Applications	4	4
Agile for Software Engineering	3	4
Critical Thinking: Reason and Evidence	3	5
American Politics and the US Constitution	3	5
Linux Foundations	3	5
Data Management - Foundations	3	5
Software Security and Testing	3	6
Applied Discrete Mathematics	3	6
Data Structures and Algorithms I	4	6
Introduction to Communication: Connecting with Others	3	6
Data Foundations for AI Security	3	7
Mathematics for AI Security	4	7
Foundations of Artificial Intelligence	4	7
AI Governance, Risk, and Ethics	4	7
Cloud AI Systems and Security	3	8
Machine Learning for Security Practitioners	3	8
Secure Software Lifecycle Management	4	8
Deep Learning for Security	3	8
Natural Science Lab	2	9
AI Systems Threat and Defense	4	9
AI Integration and Deployment	3	9
ML DevSecOps	4	9
Adversarial Learning	3	10
Model Selection, Evaluation, and Specification	3	10
Enterprise AI Security	3	10
Capstone: AI System Deployment and Security Validation	4	10
Total CUs	**130**	

Prerequisites

The standard path at WGU is essential for students to achieve success in their academic pursuits. By following the required sequence of courses, students pace their progress and build the necessary skills and competencies for future success. Prerequisite courses ensure that students have a comprehensive understanding of fundamental concepts and competencies necessary for completing advanced coursework.

The program requires students to complete a subset of courses in a specific sequence. Students and program mentors work together to plan the appropriate prerequisites for advanced courses and adhere to the standard path as required.

The BSAISEC program requires that the following courses be taken as prerequisites to the next set of courses. Some courses may have additional prerequisites, refer to the course pages for more details. Course numbering does not imply the correct sequencing in every case; some courses in the standard path do not adhere to the course number sequence. The placement of these courses aids students with pacing and completion.

Group 1: Foundations

Complete all three tracks before moving to Group 2. The tracks can be taken in parallel.

Programming (take in order):

1. Foundations of Programming (Python)
2. Version Control
3. Mathematics for Programmers
4. Object Oriented Programming in Python
5. Python for IT Automation

Mathematics and Data Structures (take in order):

1. Applied Probability and Statistics
2. Applied Algebra
3. Applied Discrete Mathematics
4. Data Structures and Algorithms I

Networks, Security, and Data

Take these courses in order:

1. Networks
2. Fundamentals of Information Security
3. Network and Security - Applications

Then take these courses in any order:

- Data Management - Foundations
- Software Security and Testing
- Linux Foundations

Group 2: AI Security Foundations

Take this set of courses in order before moving to Group 3:

1. Data Foundations for AI Security
2. Mathematics for AI Security
3. Foundations of Artificial Intelligence
4. AI Governance, Risk, and Ethics

Group 3: Applied AI and Machine Learning Security

Take this set of courses before moving to Group 4:

- Cloud AI Systems and Security
- Machine Learning for Security Practitioners
- Secure Software Lifecycle Management
- Deep Learning for Security

Group 4: AI Defense and Deployment

Take this set of courses before moving to Group 5:

- AI Systems Threat and Defense
- AI Integration and Deployment
- ML DevSecOps

Group 5: Advanced AI Security

Take this set of courses before moving to the capstone:

- Adversarial Learning
- Model Selection, Evaluation, and Specification
- Enterprise AI Security

Capstone

Capstone: AI System Deployment and Security Validation

Certifications

Certain courses are aligned to industry certifications:

- The course Networks has alignment with the CompTIA Network+.
- The course Network and Security - Applications has alignment with the CompTIA Security+.
- The course Linux Foundations has alignment with the LPI Linux Essentials.
- The course Cloud AI Systems and Security has alignment with the AWS Certified AI Practitioner.
- The course Secure Software Lifecycle Management has alignment with the ISC2 Certified Secure Software Lifecycle Professional (CSSLP).
- The course Enterprise AI Security has alignment with the CompTIA SecAI+.

AI Security and Ethics

When considering a major in AI security, students must understand the importance of ethics and principles such as integrity, responsibility, and respect for privacy. Ethical behavior helps prevent misuse of critical data and AI systems and fosters trust with clients, employers, and the public. This trust is essential for effective collaboration and security measures. Ethical behavior also guides professionals in making decisions that comply with laws and regulations, preventing breaches, legal issues, or damage to an organization’s reputation. Maintaining high ethical standards is key to building secure and reliable AI-enabled systems and digital environments.

While there are no WGU-specific criteria related to an applicant’s background for program participation, some professional organizations like ISC2 require you to disclose any criminal history, association with criminal computer activity, or loss of license or certification during their application process. This may impact your ability to obtain specific certifications that align with WGU’s standards of competency. Maintaining a clean legal record is important as it can affect your opportunities for certification and future employment opportunities in the field.

Cybersecurity and AI security are not regulated professions; however, employers often require thorough background checks to ensure candidates have a history of integrity and reliability. Depending on the job, you might also need a security clearance, especially if you'll be working with sensitive government data. Obtaining a clearance involves a detailed review of your personal, financial, and criminal history. Any criminal records can impact your chances of getting these clearances.

Changes to Curriculum

WGU publishes an Institutional Catalog, which describes the academic requirements of each degree program. Although students are required to complete the program version current at the time of their enrollment, WGU may modify requirements and course offerings within that version of the program to maintain the currency and relevance of WGU's competencies and programs. When program requirements are updated, students readmitting after withdrawal from the university will be expected to re-enter into the most current catalog version of the program.

Areas of Study for **Bachelor of Science, AI Security**

The following section includes the areas of study in the program, with their associated courses. Your specific learning resources and level of instructional support will vary based on the individual competencies you bring to the program and your confidence in developing the knowledge, skills, and abilities required in each area of the degree.

General Education

Health, Fitness, and Wellness

Health, Fitness, and Wellness focuses on the importance and foundations of good health and physical fitness, particularly for children and adolescents. This course addresses health, nutrition, and fitness, and substance use and abuse.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The graduate identifies factors that influence mental, emotional, and social wellness.*
- *The graduate identifies the application of the core competencies of social and emotional learning.*
- *The graduate identifies the influence of disease, fitness, and lifestyle on the body.*
- *The graduate identifies the principles of nutrition and the components of a healthy diet.*

Composition: Successful Self-Expression

Welcome to Composition: Successful Self-Expression! In this course, you will focus on four main topics: professional writing for a cross-cultural audience, narrowing research topics and questions, researching for content to support a topic, and referencing research sources. Each section includes learning opportunities through readings, videos, audio, and other relevant resources. Assessment activities with feedback also provide opportunities to check your learning, practice, and show how well you understand course content. Because the course is self-paced, you may move through the material as quickly or as slowly as you need to gain proficiency in the seven competencies that will be covered in the final assessment. If you have no prior knowledge or experience, you can expect to spend 30-40 hours on the course content. You will demonstrate competency through a performance assessment. There is no prerequisite for this course and there is no specific technical knowledge needed.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner composes a written message with language appropriate for cross-cultural communication.*
- *The learner incorporates research to support a position or idea.*
- *The learner incorporates self-expression in written communication.*
- *The learner researches valid and reliable sources.*
- *The learner writes a message using an effective communication approach for a given situation.*
- *The learner writes a reference list.*
- *The learner writes in a professional manner for a given scenario.*

Applied Probability and Statistics

Applied Probability and Statistics is designed to help students develop competence in the fundamental concepts of basic statistics including: introductory algebra and graphing; descriptive statistics; regression and correlation; and probability. Statistical data and probability are often used in everyday life, science, business, information technology, and educational settings to make informed decisions about the validity of studies and the effect of data on decisions. This course discusses what constitutes sound research design and how to appropriately model phenomena using statistical data. Additionally, the content covers simple probability calculations, based on events that occur in the business and IT industries. No prerequisites are required for this course.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The graduate applies principles and methods of probability-based mathematics to explain and solve problems.*
- *The graduate applies the operations, processes, and procedures of basic algebra to evaluate quantitative expressions, and to solve equations and inequalities.*
- *The graduate applies the operations, processes, and procedures of fractions, decimals, and percentages to evaluate quantitative expressions.*
- *The graduate evaluates categorical and quantitative data pertaining to a single variable using appropriate graphical displays and numerical measures.*
- *The graduate evaluates the relationship between two quantitative variables through correlation and regression.*
- *The graduate evaluates the relationship between two variables through interpretation of visual displays and numerical measures.*

Ethics in Technology

Ethics in Technology examines the ethical considerations of technology use in the 21st century and introduces students to a decision-making process informed by ethical frameworks. Students will study specific cases related to important topics such as surveillance, social media, hacking, data manipulation, plagiarism and piracy, artificial intelligence, responsible innovation, and the digital divide. This course has no prerequisites.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner describes ethical issues regarding data privacy, accuracy, access, and security.*
- *The learner explains professional ethical codes and their role in guiding professional behavior.*
- *The learner identifies interventions for personal bias and related legal concerns.*
- *The learner implements ethical decision-making frameworks in the information age.*

Applied Algebra

Applied Algebra is designed to help you develop competence in working with functions, the algebra of functions, and using some applied properties of functions. You will start learning about how we can apply different kinds of functions to relevant, real-life examples. From there, the algebra of several families of functions will be explored, including linear, polynomial, exponential, and logistic functions. You will also learn about relevant, applicable mathematical properties of each family of functions, including rate of change, concavity, maximizing/minimizing, and asymptotes. These properties will be used to solve problems related to your major and make sense of everyday living problems. Students should complete Applied Probability and Statistics or its equivalent prior to engaging in Applied Algebra.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner analyzes graphical depictions of real-world situations using functional properties.*
- *The learner applies exponential functions and their properties to real-world problems.*
- *The learner applies linear functions and their properties to real-world problems.*
- *The learner applies logistic functions and their properties to real-world problems.*
- *The learner applies polynomial functions and their properties to real-world problems.*
- *The learner interprets the real-world meaning of various functions based on notation, graphical representations, and data representations.*
- *The learner verifies the validity of a given model.*

Critical Thinking: Reason and Evidence

In this course you will learn key critical thinking concepts and how to apply them in the analysis and evaluation of reasons and evidence. The course examines the basic components of an argument, the credibility of evidence sources, the impact of bias, and how to construct an argument that provides good support for a claim. The course consists of an introduction and four major sections. Each section includes learning opportunities through readings, videos, audio, and other relevant resources. Assessment activities with feedback also provide opportunities to check your learning, practice, and show how well you understand course content. Because the course is self-paced, you may move through the material as quickly or as slowly as you need to gain proficiency in the four competencies that will be covered in the final assessment. If you have no prior knowledge or experience, you can expect to spend 30-40 hours on the course content.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner evaluates bias and its impact.*
- *The learner evaluates evidence based on source credibility.*
- *The learner evaluates the quality of an argument.*
- *The learner makes claims based on evidence.*

American Politics and the US Constitution

American Politics and the U.S. Constitution examines the evolution of representative government in the United States and the changing interpretations of the civil rights and civil liberties protected by the Constitution. This course will give candidates an understanding of the powers of the branches of the federal government, the continual tensions inherent in a federal system, the shifting relationship between state and federal governments, and the interactions between elected officials and the ever-changing electorate. This course will focus on such topics as the role of a free press in a democracy, the impact of changing demographics on American politics, and the debates over and expansion of civil rights. Upon completion of the course, candidates should be able to explain the basic functions of the federal government, describe the forces that shape American policy and politics, and be better prepared to participate in America's civic institutions. This course has no prerequisite.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The graduate describes the influence of competing political ideologies on the development of the United States government.*
- *The graduate examines the influence of political parties, citizens, and non-governmental organizations on elections and other political processes inside a participatory democracy.*
- *The graduate examines the influence of the media, public opinion, and political discourse on American democracy.*
- *The graduate examines the struggle to balance individual liberty, public order, and state's rights.*
- *The graduate explains how the structure and powers of the United States government interact to form public policy.*

Introduction to Communication: Connecting with Others

Welcome to Introduction to Communication: Connecting with Others! It may seem like common knowledge that communication skills are important, and that communicating with others is inescapable in our everyday lives. While this may appear simplistic, the study of communication is actually complex, dynamic, and multifaceted. Strong communication skills are invaluable to strengthening a multitude of aspects of life. Specifically, this course will focus on communication in the professional setting, and present material from multiple vantage points, including communicating with others in a variety of contexts, across situations, and with diverse populations. Upon completion, you will have a deeper understanding of both your own and others' communication behaviors, and a toolbox of effective behaviors to enhance your experience in the workplace.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner implements appropriate communication styles based on audience and setting.*
- *The learner uses communication strategies for managing conflict.*
- *The learner uses communication strategies to influence others.*

Natural Science Lab

This course provides students an introduction to using the scientific method and engaging in scientific research to reach conclusions about the natural world. Students will design and carry out an experiment in the natural sciences to investigate a hypothesis by gathering quantitative data. They will also research a specific topic in the natural sciences using academic sources and draw conclusions from their findings.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The graduate accurately executes the process of scientific inquiry through experimentation in the natural world.*
- *The graduate draws conclusions based on academic research and scientific inquiry.*
- *The graduate evaluates academic sources for their credibility and relevance to a chosen research topic on a natural world phenomenon.*

Computer Science

Introduction to Computer Science

Introduction to Computer Science introduces learners to the field of computer science and its essential concepts. In this course students will explore, among other topics, programming basics through language-agnostic pseudocode, computational thinking and problem-solving, algorithms, hardware, and social and ethical considerations in the field. This course is designed for beginners to gain a solid understanding of computer science principles and their applications and prepare students for further study in the field. There are no prerequisites for this course.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies computer science principles to real-world scenarios, using scientific inquiry and higher-order critical thinking skills to solve problems.*
- *The learner explains pseudocode and the mathematics representation of simple algorithms to provide a comprehensive understanding of the computational processes involved.*
- *The learner identifies common programming constructs, variables, data types, functions, and operators.*
- *The learner identifies the components of different operating systems.*
- *The learner identifies the computer architectures and components encompassing a broad range of devices beyond traditional PCs.*

Practical Applications of Prompt

The Practical Applications of Prompt course introduces learners to generative artificial intelligence (AI). This course aims to allow learners to gain skills for writing effective prompts and develop more effective conversations with artificial intelligence. Practical Applications of Prompt will lead learners to explore why prompt engineering is necessary. The course also aims to help learners, regardless of background, increase prompt fluency, which is fluency in using prompt effectively. The course teaches learners how to create effective prompts to elicit information with consideration of scope, specificity, and context; additionally, it teaches learners to evaluate the medium of the prompt and adjust prompts to output relevant results. The last section of the course focuses on ways to evaluate the efficacy of prompts and improve the depth and quality of analytical investigations. This approach

prepares students to navigate the complexities of working with generative AI and use these skills effectively throughout their careers.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *Learners create effective prompts with the consideration of scope, specificity, and context to elicit targeted information.*
- *Learners evaluate the efficacy of writing different prompts on research outcomes and improve the depth and quality of their analytical investigations.*
- *Learners evaluate the images, texts, and sound of the prompt and adjust prompts to output relevant results.*
- *Learners explain why prompt engineering is necessary.*

Data Structures and Algorithms I

Data Structures and Algorithms I covers the fundamentals of dynamic data structures, such as bags, lists, stacks, queues, trees, and hash tables with their associated algorithms. This course discusses object-oriented design and abstract data types as design paradigms. The course emphasizes problem-solving and techniques for designing efficient, maintainable software applications. Students will implement simple applications using the techniques learned.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies algorithms that address a desired outcome based on space and time complexity in big-O notation.*
- *The learner determines how data structure types impact operations within application, service, or data stores.*
- *The learner explains the use, logic, and structure of algorithms.*

IT Fundamentals

Foundations of Programming (Python)

Foundations of Programming (Python) introduces students to the fundamental principles of programming using Python. This course is designed to equip students with the essential skills needed to write, troubleshoot, and debug simple Python programs. Students will explore the syntax and structure of Python, develop an understanding of variables, loops, and conditional statements, and learn to work within different development environments, including integrated development environments (IDEs) and text editors. By the end of the course, students will be able to create functional Python programs, manipulate data structures, and apply debugging techniques across various platforms. There are no prerequisites for this course.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner creates functional programs by writing and debugging code.*
- *The learner executes Python code in different development environments.*
- *The learner identifies basic Python programming constructs to create simple functions.*
- *The learner manipulates data structures to effectively store, retrieve, and process data.*

Networks

Networks

Networks introduces skills in configuring networking components and a network infrastructure. Learners will gain skills in optimizing network operations for availability, performance, and security, and in troubleshooting network issues. The course prepares learners for the CompTIA Network+ certification exam. Network and Security - Foundations is a prerequisite for this course.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner configures a network infrastructure.*
- *The learner configures networking components.*
- *The learner implements network security techniques.*
- *The learner optimizes network operations for availability, performance, and security.*
- *The learner troubleshoots network issues.*

Secure Systems Analysis & Design

Fundamentals of Information Security

Fundamentals of Information Security lays the foundation for understanding terminology, principles, processes, and best practices of information security at local and global levels. It further provides an overview of basic security vulnerabilities and countermeasures for protecting information assets through planning and administrative controls within an organization.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner explains how human, organizational, and societal factors impact cybersecurity.*
- *The learner identifies the threats, principles, standards, and industry best practices related to connection and system security.*
- *The learner identifies the threats, principles, standards, and industry best practices related to data security.*
- *The learner identifies the threats, principles, standards, and industry best practices related to software and component security.*

Secure Software Lifecycle Management

Secure Software Lifecycle Management examines the practices, processes, and controls required to integrate security throughout the software development lifecycle. The course develops skills in defining security requirements, evaluating software architectures, conducting threat modeling, identifying and remediating implementation vulnerabilities, and assessing deployment and software supply chain risks. The course provides a foundation for secure software assurance and software security engineering.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies secure software concepts and lifecycle management practices.*
- *The learner defines secure software requirements.*
- *The learner designs a threat model for a software architecture.*
- *The learner evaluates a deployment configuration package.*
- *The learner remediates security defects in code.*

Full Stack Engineering

Version Control

Version control is critical to maintaining software and enabling scalability solutions. A best practice for any programming project that requires multiple files uses version control. Version control enables teams to have collaborative workflows and enhances the software development lifecycle. This course introduces students to the basics of publishing, retrieving, branching, and cloning. There are no prerequisites for this course.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner implements version control processes and solutions that maintains source code.*

Mathematics Content

Mathematics for Programmers

This course bridges mathematics and programming by using Python to develop mathematical reasoning skills. Students create and evaluate functions to model relationships, analyze and graph algebraic and trigonometric functions, and solve problems that build readiness for calculus and object-oriented programming while using computational tools to explore patterns, precision, and real-world applications.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies algebraic and functional models using Python to analyze, graph, and solve calculus-preparatory problems.*
- *The learner develops Python functions to represent, evaluate, test, and explain mathematical relationships.*
- *The learner models trigonometric, geometric, and change-based relationships using Python to solve programming and calculus-preparatory problems.*

Applied Discrete Mathematics

Applied Discrete Mathematics introduces the foundational mathematical structures that underpin modern technology. Topics include logic, Boolean algebra, sets, functions, relations, graphs, combinatorics, and modular arithmetic, with emphasis on their applications to technology concepts such as Boolean algebra and structures, password complexity, access control models, network topologies, and cryptography. Students will not focus on abstract proofs but will instead learn how discrete mathematics informs real-world technology structures and practices. By the end of the course, students will be able to apply mathematical reasoning to technology scenarios, analyze system vulnerabilities through discrete models, and explain the mathematical principles behind technological architectures and protocols.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner analyzes real-world systems, including representations or models of mathematical structures.*
- *The learner applies logic and Boolean algebra principles to interpret and analyze real-world systems.*
- *The learner applies modular arithmetic and number theory concepts to describe aspects of real-world technological systems.*
- *The learner creates problem-solving models of real-world problems using combinatorics, probability, and graph theory.*

Programming

Object Oriented Programming in Python

This course bridges foundational programming skills to advanced object-oriented concepts, empowering learners to design and implement robust, scalable applications. It emphasizes the core pillars of object-oriented programming such as inheritance, composition, encapsulation, abstraction, and polymorphism while introducing data structure fundamentals. Learners will define and extend class hierarchies, apply method overriding, work with polymorphic collections, and traverse data structures using iterative and recursive techniques. Through practical problem-solving, the course reinforces code reusability and equips learners to apply object-oriented principles for efficient, maintainable solutions.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies inheritance, encapsulation, and abstraction to programming problems with object-oriented code.*
- *The learner applies polymorphism and recursion to programming problems with object-oriented code.*
- *The learner develops code using inheritance in object-oriented programming.*

Agile for Software Engineering

This course introduces the application of Agile methodology in software engineering, focusing on Scrum, Kanban, and collaborative team practices. Learners apply agile leadership frameworks, communication strategies, and agile processes to contribute effectively to software engineering projects and foster an agile team culture. Successful completion of this course may support learners in pursuing Agile or Scrum-related certifications offered by the Scrum Alliance.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies a leadership framework to software engineering within an agile environment.*
- *The learner applies agile methodology to contribute to software engineering projects.*
- *The learner evaluates how agile leadership and processes improve the results and efficiency of software engineering processes.*
- *The learner implements effective collaboration and communication practices within agile software engineering teams.*
- *The learner strategizes how to foster an agile culture in software engineering contexts.*

Artificial Intelligence

Introduction to AI Coding Assistants

Introduction to AI Coding Assistants explores the effective use of artificial intelligence as a collaborative tool in software and infrastructure work. The course examines techniques for communicating with AI systems, evaluating AI-generated solutions, and applying professional judgment to ensure accuracy, quality, and responsible decision-making in technical environments.

This course covers the following competencies:

- *• The learner applies AI-assisted prompt engineering techniques to generate code.*
- *• The learner explains the human-in-the-loop posture.*
- *• The learner reviews AI-generated code for quality and corrections.*
- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*

Mathematics for AI Security

Mathematics for AI Security provides the mathematical foundation required to understand, evaluate, and reason about AI-enabled systems in cybersecurity contexts. The course integrates linear

algebra, optimization, Bayesian reasoning, and information theory to examine how machine learning systems represent data, learn from information, and make decisions under uncertainty. Through Python-based analysis of security-relevant datasets, students apply mathematical concepts to evaluate model behavior, assess risk, and interpret system performance. The course prepares students for advanced study in machine learning, deep learning, and AI security.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies Bayes' theorem and Bayesian updating to assess classifier performance.*
- *The learner applies information-theoretic calculations in Python that analyze security-relevant distributions.*
- *The learner applies matrix operations in Python to multidimensional security datasets.*
- *The learner explains the role of loss functions and gradient-based optimization in Python.*

Foundations of Artificial Intelligence

Foundations of Artificial Intelligence introduces the concepts, techniques, and applications that underpin modern AI systems. The course examines core AI approaches, including machine learning, neural networks, intelligent agents, reasoning systems, and generative AI, while exploring how AI is applied across industries and security-relevant domains. Emphasis is placed on evaluating AI tools, assessing the quality and limitations of AI-generated outputs, and analyzing ethical, societal, safety, and security considerations. The course provides a foundation for responsible AI use and prepares students for advanced study in AI governance, security, and applied AI disciplines.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies AI tools to solve problems using appropriate techniques.*
- *The learner evaluates the ethical and societal implications of AI.*
- *The learner evaluates the safety and security properties of AI systems.*
- *The learner explains how classical AI techniques and reasoning approaches are used to solve structured problems.*
- *The learner explains how core artificial intelligence concepts, terminology, and applications function in different AI systems across industries.*

Machine Learning for Security Practitioners

Machine Learning for Security Practitioners applies machine learning techniques to cybersecurity detection, analysis, and decision-making. The course develops skills in preparing security datasets, implementing and comparing supervised and unsupervised machine learning approaches, evaluating model performance, and assessing model robustness in operational environments. The course prepares students to evaluate machine learning solutions used in cybersecurity operations and security analytics.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner evaluates an appropriate ML approach for a security problem.*
- *The learner evaluates model performance and robustness.*
- *The learner evaluates supervised classification algorithms.*
- *The learner implements unsupervised anomaly detection methods.*
- *The learner prepares real-world security datasets for machine learning.*

Deep Learning for Security

Deep Learning for Security examines the neural network and transformer architectures that underpin modern AI-enabled cybersecurity systems. The course develops skills in evaluating deep learning models, analyzing model behavior, assessing robustness, applying explainability

techniques, and identifying security-relevant failure modes. The course prepares students to assess, communicate, and manage security risks associated with deep learning technologies used in enterprise and cybersecurity environments.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner analyzes gradient values in a trained PyTorch network.*
- *The learner analyzes the attack surfaces of a pre-trained language model.*
- *The learner deploys a feedforward neural network in PyTorch.*
- *The learner interprets feature attribution results from trained deep learning models.*
- *The learner refines a pre-trained deep learning model on a security classification task.*

AI Systems Threat and Defense

AI Systems Threat and Defense applies AI security principles to the assessment, analysis, and defense of deployed AI applications. The course develops skills in identifying and evaluating vulnerabilities in AI Systems with emphasis on threat modeling, vulnerability validation, mitigation analysis, and professional security reporting using industry-recognized frameworks.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner constructs threat models for RAG pipelines and agentic AI systems.*
- *The learner designs detection logic for AI-specific threats in production environments.*
- *The learner evaluates deployed LLM applications for vulnerabilities across the OWASP LLM Top 10 and implements validated mitigations.*
- *The learner produces a professional AI security findings report documenting red team assessment results.*

AI Integration and Deployment

AI Integration and Deployment Security examines the security challenges that arise when AI systems are integrated into applications and deployed in production environments. The course develops skills in applying security controls, assessing architectural and deployment risks, validating defensive measures, and supporting secure and resilient AI implementations in enterprise environments.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner evaluates agentic AI system architectures and MCP server implementations.*
- *The learner implements AI security standards to deployment infrastructure.*
- *The learner secures REST API endpoints that serve ML models.*
- *The learner validates LLM API integrations.*

ML DevSecOps

ML DevSecOps explores the principles and practices used to secure machine learning systems throughout the development and operational lifecycle. The course examines risk management, system security, incident response, and secure development practices for machine learning environments, providing a foundation for protecting AI solutions while supporting reliability, trust, and organizational objectives.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner assesses an ML system for security using established frameworks.*
- *The learner communicates security findings and risk assessments to organizational stakeholders.*
- *The learner mitigates security risks in ML systems.*
- *The learner responds to active security events in ML systems.*

Adversarial Learning

Adversarial Learning examines how machine learning systems can be attacked, evaluated, and defended in real-world environments. The course develops skills in adversarial threat modeling, implementing and analyzing attacks against machine learning models, evaluating model robustness, and assessing privacy risks associated with AI systems.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner communicates the privacy implications of adversarial attacks.*
- *The learner evaluates adversarial defenses against threat models.*
- *The learner implements adversarial attacks against ML classifiers.*

Model Selection, Evaluation, and Specification

Model Selection, Evaluation, and Specification examines how AI systems are assessed for suitability, risk, and effectiveness in security-relevant deployment contexts. The course develops skills in defining model requirements, evaluating model performance and tradeoffs, analyzing failure modes and deployment risks, and assessing third-party AI systems under limited visibility. The course prepares students to make and defend AI deployment decisions that align with organizational objectives, risk tolerance, and governance requirements.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies a structured evaluation toolkit to AI security models.*
- *The learner evaluates trade-offs in deploying AI models for security-relevant applications.*
- *The learner evaluates vendor and third-party AI systems under black-box constraints.*

Enterprise AI Security

Enterprise AI Security examines the security, risk, governance, and compliance challenges associated with AI-enabled enterprise systems. The course develops skills in analyzing AI threats and attack surfaces, evaluating and recommending security controls, applying AI security frameworks, and assessing governance and regulatory requirements. Students explore the use of AI-enabled tools in cybersecurity operations and evaluate organizational approaches to responsible AI adoption. Emphasis is placed on securing AI systems across the AI lifecycle and applying risk-based decision-making within enterprise environments.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner compares and contrasts core AI concepts and techniques used in cybersecurity.*
- *The learner evaluates AI governance structures and compliance frameworks.*
- *The learner recommends security controls for AI systems.*
- *The learner uses AI-enabled tools to facilitate and automate security tasks.*

Networking

Python for IT Automation

Python for IT Automation covers the fundamentals of the Python language and its features to control program flow, inform decisions, and automate IT tasks and processes. The course emphasizes a systematic approach to solving problems and the application of programming logic to administer secure, scalable, and resilient IT networks and systems.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies Python principles and syntax to manage variables, data structures, and operators and to perform IT tasks.*
- *The learner creates Python scripts using control structures to automate system tasks.*
- *The learner integrates Python scripts, modules, packages, and libraries to automate networking tasks and processes.*

Network and Security

Network and Security - Applications

Network and Security - Applications prepares learners for the CompTIA Security+ certification exam. The course introduces learners to skills in identifying threats, attacks, and vulnerabilities to organizational security. The learner will also gain skills in designing security solutions for enterprise infrastructures and architectures, as well as in implementing security solutions across hardware, applications, and network services. Learners will be able to execute operations and incident response with tools, policies, forensics, and mitigation techniques, and to analyze information security controls, governance, risk, and compliance.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner analyzes information security controls, governance, risk, and compliance.*
- *The learner designs security solutions for enterprise infrastructures and architectures.*
- *The learner executes operations and incident response with tools, policies, forensics, and mitigation techniques.*
- *The learner identifies threats, attacks, and vulnerabilities to organizational security.*
- *The learner implements security solutions across hardware, applications, and network services.*

Operating Systems

Linux Foundations

Linux Foundations prepares learners for the LPI Linux Essentials certification and is an introduction to Linux as an operating system as well as an introduction to open-source concepts and the basics of the Linux command line. Learners will gain skills in identifying the fundamentals of open-source software and to develop resources for data access and security.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner develops resources for data access and security.*
- *The learner identifies the fundamentals of open-source software.*

Data Management

Data Management - Foundations

Data Management Foundations offers an introduction in creating conceptual, logical and physical data models. Students gain skills in creating databases and tables in SQL-enabled database management systems, as well as skills in normalizing databases. No prerequisites are required for this course.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner defines primary and foreign keys in data normalization.*
- *The learner determines how to run queries for creation and manipulation of data in relational databases.*
- *The learner explains attributes of databases, database tables, and structured and associated query language (SQL) commands.*

Software

Software Security and Testing

This course prepares you to recognize security vulnerabilities in software, to plan interventions to address security vulnerabilities where they exist, and to develop and test these interventions. The course covers topics in Web security, permissions, and identity security; debugging; log file analysis; API security; and encryption and cryptography concepts.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner configures security authentication for representational state transfer (REST) and application programming interfaces (APIs).*
- *The learner develops mitigation solutions for security vulnerabilities.*
- *The learner evaluates application and network logs for performance, availability, and security vulnerabilities.*

Data Manipulation

Data Foundations for AI Security

Data Foundations for AI Security establishes data handling, governance, and data trust as foundational cybersecurity competencies. The course develops practical skills for preparing, managing, evaluating, and analyzing security-relevant data. Learners work with datasets such as network logs, authentication records, and security event data to assess quality and integrity, identify meaningful patterns, and support security decision-making. Emphasis is placed on governance, lifecycle management, and trustworthy data practices that support cybersecurity operations.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner applies appropriate data cleaning and transformation practices to structured and semi-structured security data.*
- *The learner applies data governance principles to security-relevant data flows.*
- *The learner applies data techniques to security datasets.*
- *The learner communicates security dataset analyses.*
- *The learner evaluates datasets for practical security outcomes.*

Security Policies and Standards

AI Governance, Risk, and Ethics

AI Governance, Risk, and Ethics examines the legal, regulatory, ethical, and organizational considerations that shape the responsible design, deployment, and oversight of artificial intelligence systems. The course develops skills in applying AI governance frameworks, analyzing regulatory requirements, evaluating fairness and accountability concerns, and assessing AI-specific risks across the system lifecycle. The course prepares students to evaluate AI governance practices and support responsible AI implementation in enterprise environments.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner analyzes applicable AI legal and regulatory frameworks.*
- *The learner applies the NIST AI RMF to analyze organizational AI governance structures and recommend oversight mechanisms appropriate to AI deployment contexts.*
- *The learner audits AI systems for ethical compliance, using structured analytical tools.*
- *The learner prioritizes AI-specific risks across the AI lifecycle, using structured risk assessment methodology.*

Web and Cloud Security

Cloud AI Systems and Security

Cloud AI Systems and Security examines how artificial intelligence systems are built, deployed, governed, and secured in cloud environments. The course explores machine learning lifecycle concepts, generative AI architectures, foundation model applications, prompt engineering, and responsible AI practices within a cloud environment. The course prepares students to assess AI-enabled cloud deployments and supports readiness for cloud-based AI security.

This course covers the following competencies:

- *Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.*
- *The learner assesses the security and governance posture of a cloud-hosted AI deployment.*
- *The learner describes the architecture of generative AI systems in cloud environments.*
- *The learner evaluates an AI system against responsible AI principles.*
- *The learner explains the cloud managed services for each phase of the ML development lifecycle.*

Capstone

Capstone: AI System Deployment and Security Validation

The AI Security Capstone serves as the culminating experience of the AI Security program by integrating the technical, analytical, governance, and communication skills developed throughout the curriculum. The course prepares students to perform end-to-end AI security assessments and communicate actionable risk-based recommendations in professional practice.

This course covers the following competencies:

- *The learner produces a complete AI Security Assessment Package.*
- *The student executes a structured technical security assessment against a realistic AI system.*
- *The student produces a professional threat model for a realistic AI system.*

Accessibility and Accommodations

Western Governors University (WGU) is committed to providing equal access to its academic programs to all qualified students. WGU's Student Disability Services department supports this mission by providing support, resources, advocacy, collaboration, and academic accommodations in accordance with federal and state statutes and regulations to WGU students and prospective students. Potential and current students needing to request accommodation(s) are encouraged to contact Student Disability Services to initiate the request. To initiate the accommodation process, all potential and current WGU students must complete the secure online Accommodation Request Form located at' https://www.wgu.edu/wgu/ada_form. Potential and current students can reach the Student Disability Services team Monday through Friday 8:00 a.m. to 5:00 p.m. MT at 1-877- 435-7948 x5922 or at sds@wgu.edu. Additional information on accommodations can be found in the student handbook Accommodations for Students with Disabilities policy.

Need More Information? WGU Student Services

Student Support Services team members also assist with unresolved concerns to find equitable resolutions. To contact the Student Support Services team, please feel free to call 877-435-7948 or email studentservices@wgu.edu. We are available Monday through Friday from 6:00 a.m. to 10:00 p.m., and Saturday and Sunday, 10:00 a.m. to 7:00 p.m, mountain standard time.