Fundamentals of Information Security Course Syllabus

WESTERN GOVERNORS UNIVERSITY

Fundamentals of Information Security

Hello, and welcome!

Data breaches, hacks, malware, and cyberattacks. We hear about these security disruptions all too often, and they can impact government agencies, colleges, hospitals, and companies of all sizes. Keeping information safe can seem like a monumental task! But there are effective strategies to employ. In this course, you will explore the terminology, principles, processes, and best practices of information security at local and global levels. You will gain an overview of basic security vulnerabilities that organizations face. And you will learn about countermeasures for protecting information assets through planning and administrative controls. With this knowledge, you will be better prepared to protect data, and you will have the foundation to pursue cybersecurity pathways.

We invite you to take a minute to learn about the course by reviewing the information that follows. This way, you will be better able to understand the expectations of the course as a whole. Then you can determine how to manage your time and efforts as you navigate through it.

You are in the right place. You belong here. You can do this!

Course Description and Competencies

WHAT TO EXPECT

This course is divided into 10 modules that focus on security principles, network protocols, network design, wireless security, application development, privacy, artificial intelligence, and other topics. The course materials include readings, practice quizzes, videos, and lab activities. These elements will help prepare you to demonstrate your achievement of three competencies.

There is no prerequisite for this course, and there is no specific technical knowledge needed.

This course covers the following competencies:

1. The learner identifies the threats, principles, standards, and industry best practices related to data security.
2. The learner identifies the threats, principles, standards, and industry best practices related to software and component security.
3. The learner identifies the threats, principles, standards, and industry best practices related to connection and system security.
4. The learner explains how human, organizational, and societal factors impact cybersecurity.

Assessment

The assessment provides an opportunity to demonstrate your mastery of the competencies in this course. You may attempt the assessment two times before additional support is necessary. If you require further attempts, please contact your Course Instructor or Student Experience Specialist.

- **1** final exam
- **3** competency units

Course Outline

Module	Upon completion of this module, you will be able to:
Career Pathways	A. Describe the purpose of the NICE Cybersecurity Workforce Framework and its major categories. B. Differentiate between the red, blue, and yellow roles in the cybersecurity "color wheel." C. Identify cybersecurity jobs that fall outside the NICE framework and the skills they require. D. Explain challenges and common skill demands across different cybersecurity career paths. E. Explore potential cybersecurity roles by participating in interactive TryCyber challenges.
Introduction to Security	A. Define core security principles, including confidentiality, integrity, and availability (CIA). B. Recognize different types of vulnerabilities, threat actors, and attack vectors. C. Explain the purpose of access control and identity management in securing systems. D. Identify common social engineering techniques (physical, technical, and social-based). E. Describe common forms of malware and explain how they spread, hide, and mislead. F. Summarize the OWASP Top 10 security risks and their impact on application security.
Network Attacks and Secure Network Protocols	A. Identify different types of network-based attacks, including DDoS, DNS poisoning, and domain hijacking. B. Explain ARP poisoning, MAC flooding, and MAC cloning, and their impact on network security. C. Describe on-path attacks such as man-in-the-middle and man-in-the-browser. D. Explain how cyber threat intelligence contributes to preventing and mitigating network attacks.

Secure Network Design	A. Explain how network segmentation, VLANs, and zero-trust models enhance secure. B. Differentiate between firewall types, deployment models, and applications. C. Describe the role of intrusion detection and prevention systems (NIDS/NIPS). D. Explain the use of VPNs for secure communication across networks. E. Apply system hardening practices, including patch management and endpoint protection.
Wireless, Mobile, and IoT Security	A. Identify unique security risks related to embedded systems, mobile devices, and IoT. B. Explain mobile device management approaches and deployment models. C. Describe how AI and machine learning are used in cybersecurity. D. Recognize the importance of physical and operational security in securing devices.
Secure Application Development	A. Explain database basics and identify methods for securing databases. B. Describe secure coding practices and the role of provisioning, version control, and software diversity. C. Apply application security techniques such as input validation, fuzzing, and automation. D. Explain the significance of OWASP in guiding secure application development. E. Evaluate the CIA triad as it applies to software and component security.
Cloud Security	A. Describe software-defined networking and its implications for cloud environments. B. Explain challenges of securing cloud-based networks and infrastructure. C. Recognize the role of virtualization in cloud security.

Security Standards and Policies	A. Identify major cybersecurity laws, regulations, and standards. B. Explain how security frameworks (e.g., NIST CSF) guide organizational security. C. Describe the role of configuration guides, documentation, and asset management. D. Explain how change management, training, and awareness programs support security compliance. E. Demonstrate the application of security policies and governance practices through lab scenarios.
Risk Management and Privacy	A. Identify types of privacy breaches and describe methods of data classification. B. Explain privacy technologies and data protection practices. C. Describe the process of risk identification, assessment, and management. D. Analyze cybersecurity risks in emerging areas such as generative AI. E. Apply risk management principles in conducting a cybersecurity risk assessment.
Artificial Intelligence	A. Summarize the history and basic principles of artificial intelligence. B. Explain the role of generative AI and large language models in modern cybersecurity. C. Discuss ethical considerations and societal impacts of AI adoption. D. Evaluate how AI and machine learning can both strengthen and weaken cybersecurity. E. Apply practical AI skills in security contexts through labs and activities.

Technology Requirements

We want you to have the tools to succeed! Since this course includes at least one proctored test, please be sure to have a working microphone, speakers, and an external webcam. Unfortunately, an internal webcam (built into many laptops) is not acceptable. (Note: The external webcam is required only for exams that have proctors. You do not need one for practice tests and other non-proctored assessments.)

If you haven't already, be sure to download the *Meazure Learning Guardian* browser, which you will need for the proctoring system.

For other details about the technology you'll need, review the Computer System and Technology Requirements. If you have questions about your setup, contact support@academy.wgu.edu.

You will need Adobe Acrobat Reader DC. If you haven't already, download this free software. You may encounter an interactive form that contains fields that you can select or fill in. Review how to fill in a PDF form.

Key Contacts

Resource Hub	Check out the Course Lobby to take advantage of course resources, including videos and tips from our educators. There, you can ask and answer questions, provide feedback on your progress, and connect with fellow students. You will find this platform in the Student Resources section of the course. Log on and do some exploring!
Technical Support	If you encounter technical issues, be sure to contact the Help Desk. Just submit a Support Request for assistance.
Program Support	Do you have questions about your account? Student Support has answers. They can help with billing, switching courses, and other requests. You can contact them at (888) 320-0540 or support@academy.wgu.edu.

Accommodations

WGU provides compliant and accessible learning experiences. If you require accommodation, please contact us at the start of the course. You can email support@academy.wgu.edu or call (888) 320-0540. We are committed to ensuring that all students with disabilities have equal access to WGU's services and materials. We strive to use best practices for accessibility. Our goal is to conform to existing U.S. laws. These include the Americans with Disabilities Act and Section 504 and Section 508 of the Rehabilitation Act. Our learning management system (LMS) platform is Open edX. Open edX's commitment to accessible content is published on their Website Accessibility Policy.