

**Course Outline of Record**

1. Course Code: CIS-360A
2.
  - a. Long Course Title: Information Systems Security I
  - b. Short Course Title: SYSTEMS SECURITY I
3.
  - a. Catalog Course Description:
 

An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management.

CompTIA certifications help students build a solid foundation of essential knowledge and skills that will help students earn employment in technology-related careers. The CompTIA Security+ certification provides a global benchmark for best practices in IT network and operational security, one of the fastest-growing fields in IT. Completion of this course prepares students for part of the CompTIA Security+ certification exam.
  - b. Class Schedule Course Description:
 

An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management.

CompTIA certifications help students build a solid foundation of essential knowledge and skills that will help students earn employment in technology-related careers. The CompTIA Security+ certification provides a global benchmark for best practices in IT network and operational security, one of the fastest-growing fields in IT. Completion of this course prepares students for part of the CompTIA Security+ certification exam.
  - c. Semester Cycle (*if applicable*): N/A
  - d. Name of Approved Program(s):
    - SECURITY+ PREPARATORY Certificate of Completion
4. Total Units: 0      Total Semester Hrs: 27.00  
 Lecture Units: 0      Semester Lecture Hrs: 27.00  
 Lab Units: 0      Semester Lab Hrs: 0  
 Class Size Maximum: 32      Allow Audit: No  
 Repeatability Noncredit - Unlimited  
 Justification 0
5. Prerequisite or Corequisite Courses or Advisories:
 

*Course with requisite(s) and/or advisory is required to complete Content Review Matrix (CCForm1-A)*

 Prerequisite: CIS 053 with a minimum grade of C or  
 Prerequisite: CIS 353B
6. Textbooks, Required Reading or Software: (*List in APA or MLA format.*)
  - a. Clampa, M. (2016). *Security+ Guide to Network Security Fundamentals* Cengage.  
 College Level: Yes  
 Flesch-Kincaid reading level: 12
  - b. Whitman, M. E.; Mattord, H. J. (2016). *Principles of Information Security* Cengage.  
 College Level: Yes  
 Flesch-Kincaid reading level: 12
7. Entrance Skills: *Before entering the course students must be able:*
  - a.  
 Demonstrate the principles of security system development methodology.
    - CIS 353B - Explain fundamental Ethernet concepts such as media, services, and operations.

# CIS 360A-Information Systems Security I

- CIS 053 - Explain fundamental Ethernet concepts such as media, services, and operations.

b.

Apply the fundamental concepts of information security to network management and technology security.

- CIS 353B - Experiment with common network utilities to verify small network operations and analyze data traffic.
- CIS 053 - Experiment with common network utilities to verify small network operations and analyze data traffic.

## 8. Course Content and Scope:

### Lecture:

1. Procedures and security maintenance.
2. Monitoring the external and internal security environment.
3. Major protocols used for secure communications and understand the nature and execution of the dominant method of attack.
  1. TCP/IP Transmission Control Protocol/Internet Protocol
  2. SMTP Simple Mail Transfer protocol
  3. POP3 Post Office Protocol
  4. HTTP Hypertext Transfer Protocol
4. Isolation of the virtual environment.
5. Setting up a home office security system.
  1. Using a wireless router for home office security.
  2. Wireless encryption WPA2. (Short for Wi-Fi Protected Access 2 - Pre-Shared Key)
6. Approaches to remote and VPN (Virtual Private Network) access protection.
7. Malware and social engineering attacks.
8. Application and network attacks.
9. Vulnerability Assessment and Mitigating Attacks.
10. Host, application, and data security.

Lab: *(if the "Lab Hours" is greater than zero this is required)*

## 9. Course Student Learning Outcomes:

1.  
Describe the fundamental principles of information systems security.
2.  
Inspect data inventory vulnerabilities.
3.  
Evaluate network exposure to cyberattacks.

## 10. Course Objectives: *Upon completion of this course, students will be able to:*

- a. Describe the fundamental principles of information systems security.
- b. Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
- c. Evaluate the need for the careful design of a secure organizational information infrastructure.
- d. Perform risk analysis and risk management.
- e. Determine both technical and administrative mitigation approaches.

## 11. Methods of Instruction: *(Integration: Elements should validate parallel course outline elements)*

- a. Activity
- b. Collaborative/Team
- c. Demonstration, Repetition/Practice
- d. Discussion
- e. Distance Education

- f. Experiential
- g. Lecture
- h. Observation
- i. Participation
- j. Role Playing
- k. Technology-based instruction

12. Assignments: *(List samples of specific activities/assignments students are expected to complete both in and outside of class.)*

In Class Hours: 27.00

Outside Class Hours: 54.00

a. In-class Assignments

- Implement security configuration parameters on network devices and other technologies
- Given a scenario, user secure network administration policies
- Explain network design elements and components
- Given a scenario, implement common protocols and services
- Given a scenario troubleshoot security issues related to wireless networking
- Explain the importance of risk related concepts
- Summarize the security implications of integrating systems and data with third parties
- Given a scenario, execute appropriate risk mitigation strategies
- Given a scenario, implement basic forensic procedures
- Summarize common incident response procedures
- Explain the importance of security related awareness and training
- Compare and contrast physical security and environmental controls
- Summarize risk management best practices
- Given a scenario, select the appropriate control to meet the goals of security
- Explain types of malware
- Summarize various types of attacks

b. Out-of-class Assignments

- Textbook reading and/or other resource reading that cover the functions and purposes of information security and telecommuting or virtual environments, and describe an ergonomic and efficient network security.
- Develop online/distance learning tasks/activities such as web quests, router setups, and online presentations to assess the categories of skills and work habits of a secure work environment. Develop online/distance learning tasks/activities such as web quests, website reviews, and discussion posting to show types of employment that lend themselves to security work and relate them to their areas of information security. Develop and assign online/distance learning tasks/activities such as web quests and online paper submissions to design an ergonomic and efficient network security.
- Online activities such as web quests in order to identify and list 5 strategies to organize and manage home/security and office/security duties.

13. Methods of Evaluating Student Progress: *The student will demonstrate proficiency by:*

- Written homework  
Written reports designed to assess the categories of skills and filtering technology needed for a secure environment.  
Written reports to show the ability to design an efficient information security policy.
- Guided/unguided journals  
Written/online journal or written online summaries designed to describe the functions and purposes of network security.
- Self-paced testing
- Laboratory projects  
Develop and assign lab activities that are directed toward professional certification, that need mastery of Access

Controls, Cryptography, Risk, and Security operations. Develop labs that deliver fundamental information security principles packed with real-world applications. Develop lab assignments and tasks/activities to test security needed for a virtual Private Networks.

- Computational/problem solving evaluations  
Individual security projects designed to find types of network security that lend themselves to application protocol verification and relate them to their areas of interest.
- Presentations/student demonstration observations  
Individual or class projects designed to test security technology and software security needed for network control.
- Group activity participation/observation  
Individual, small group, or paired presentations designed to find and apply effective communication tools and techniques.
- Product/project development evaluation  
Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.
- True/false/multiple choice examinations  
Develop and assign class exercises such as drills and practice quizzes to define terms that relate to information security.
- Mid-term and final evaluations  
Final written projects/exam report which summarizes, synthesizes, and evaluates learning experiences and reflects how the course might influence student’s master security plan.
- Oral and practical examination

14. Methods of Evaluating: Additional Assessment Information:

15. Need/Purpose/Rationale -- *All courses must meet one or more CCC missions.*

PO - Career and Technical Education

Fulfill the requirements for an entry- level position in their field.

Apply critical thinking skills to execute daily duties in their area of employment.

Apply critical thinking skills to research, evaluate, analyze, and synthesize information.

Display the skills and aptitude necessary to pass certification exams in their field.

Exhibit effective written, oral communication and interpersonal skills.

IO - Personal and Professional Development

Demonstrate an understanding of ethical issues to make sound judgments and decisions.

IO - Scientific Inquiry

Collect and analyze data. Skills of data collection include an understanding of the notion of hypothesis testing and specific methods of inquiry such as experimentation and systematic observation.

IO - Critical Thinking and Communication

Apply principles of logic to problem solve and reason with a fair and open mind.

IO - Global Citizenship - Scientific & Technological Literacy

Synthesize, interpret, and infer, utilizing information, data, and experience to solve problems, innovate, and explore solutions.

IO - Global Citizenship - Ethical Behavior

Apply ethical reasoning to contemporary issues and moral dilemmas.

16. Comparable Transfer Course

University System	Campus	Course Number	Course Title	Catalog Year
-------------------	--------	---------------	--------------	--------------

17. Special Materials and/or Equipment Required of Students:

---

18. Materials Fees:  Required Material?

**Material or Item**

**Cost Per Unit**

**Total Cost**

19. Provide Reasons for the Substantial Modifications or New Course:

This course, in combination with CIS-360B, prepares students for the IT security certification exam known as Security+. This certification will help them obtain employment in an IT-related field. The course is also oriented and the nontraditional student who does not desire to continue to a 4 year college but rather benefit from gainful IT-related employment.

- 20. a. Cross-Listed Course (*Enter Course Code*): N/A
- b. Replacement Course (*Enter original Course Code*): N/A

21. Grading Method (*choose one*): Pass/No Pass Only

22. MIS Course Data Elements

- a. Course Control Number [CB00]: CCC000580642
- b. T.O.P. Code [CB03]: 70100.00 - Information Technology, G
- c. Credit Status [CB04]: N - Noncredit
- d. Course Transfer Status [CB05]: C = Non-Transferable
- e. Basic Skills Status [CB08]: 2N = Not basic skills course
- f. Vocational Status [CB09]: Clearly Occupational
- g. Course Classification [CB11]: J - Workforce Preparation Enhanced Funding
- h. Special Class Status [CB13]: N - Not Special
- i. Course CAN Code [CB14]: N/A
- j. Course Prior to College Level [CB21]: Y = Not Applicable
- k. Course Noncredit Category [CB22]: J - Workforce Preparation
- l. Funding Agency Category [CB23]: Y = Not Applicable
- m. Program Status [CB24]: 1 = Program Applicable

Name of Approved Program (*if program-applicable*): SECURITY+ PREPARATORY

*Attach listings of Degree and/or Certificate Programs showing this course as a required or a restricted elective.)*

23. Enrollment - Estimate Enrollment

First Year: 12  
 Third Year: 32

24. Resources - Faculty - Discipline and Other Qualifications:

- a. Sufficient Faculty Resources: Yes
- b. If No, list number of FTE needed to offer this course: N/A

25. Additional Equipment and/or Supplies Needed and Source of Funding.

N/A

26. Additional Construction or Modification of Existing Classroom Space Needed. (*Explain:*)

N/A

27. FOR NEW OR SUBSTANTIALLY MODIFIED COURSES

Library and/or Learning Resources Present in the Collection are Sufficient to Meet the Need of the Students Enrolled in the Course: Yes

28. Originator Felix Marhuenda-Donate Origination Date 08/18/16