**DESCRIPTOR: ITIS 160**

|  |  |  |  |
| --- | --- | --- | --- |
| Discipline: Information Technology and Information Systems | Proposed Sub-discipline (if applicable): | | |
| General Course Title:  **Introduction to Information Systems Security** | | | Min. Units 3 |
| General 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. Preparation for the CompTIA Security+ certification exams. | | | |
| Proposed Number: ITIS 160 | Proposed Suffix: | | |
| Required Prerequisites[[1]](#footnote-1): None | | | |
| Required Co-Requisites: None | | | |
| Advisories/Recommended Preparation[[2]](#footnote-2):  ITIS 150 Computer Network Fundamentals  The use of case examples for discussion and reflection in this course is highly recommended. | | | |
| Course Content:     1. Introduction to Information Systems Security 2. Malware and Social Engineering Attacks 3. Application and Network Attacks 4. Vulnerability Assessment and Mitigating Attacks 5. Host, Application, and Data Security 6. Network Security 7. Administering a Secure Network 8. Wireless Network Security 9. Access Control Fundamentals 10. Authentication and Account Management 11. Basic Cryptography 12. Advanced Cryptography 13. Business Continuity 14. Risk Mitigation | | | |
| Course Objectives: *At the conclusion of this course, the student should be able to:*   1. Describe the fundamental principles of information systems security. 2. Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related. 3. Evaluate the need for the careful design of a secure organizational information infrastructure. 4. Perform risk analysis and risk management. 5. Determine both technical and administrative mitigation approaches. 6. Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO). 7. Create and maintain a comprehensive security model. 8. Apply security technologies. 9. Define basic cryptography, its implementation considerations, and key management. 10. Design and guide the development of an organization’s security policy 11. Determine appropriate strategies to assure confidentiality, integrity, and availability of information. 12. Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls. | | | |
| Methods of Evaluation:  Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments. | | | |
| Sample Textbooks, Manuals, or Other Support Materials (do not include editions or publication dates): Ciampa, M. - Security+ Guide to Network Security Fundamentals, CengageWhitman, M. E. & Mattord, H. J. - Principles of Information Security, Cengage | | | |
| FDRG Lead Signature: Markus Geissler, PhD Date: 20Jan2021 | | | |
| [For Office Use Only] | | **Internal Tracking Number** | |
|  | | | |
|  | | | |

1. Prerequisite or co-requisite course need to be validated at the CCC level in accordance with Title 5 regulations; co-requisites for CCCs are the linked courses that must be taken at the same time as the primary or target course. [↑](#footnote-ref-1)
2. Advisories or recommended preparation will not require validation but are recommendations to be considered by the student prior to enrolling. [↑](#footnote-ref-2)