University of Arkansas – Fort Smith
5210 Grand Avenue
P.O. Box 3649
Fort Smith, AR 72913
479-788-7000

General Syllabus

CS 3503 IT Security

Credit Hours: 3 Lecture Hours: 3 Laboratory Hours: 0

Prerequisite: CS 1033 Foundations of Operating Systems I and CS 1063 Foundations of Operating Systems II

Effective Catalog: 2018-2019

I. Course Information

A. Catalog Description

Begins with examining the business continuity mandate for securing IT assets, moves through physical versus logical security, how to categorize and analyze threats using organizational security policies; integrating multi-disciplinary skills to analyze risks, and implement security measures. These security measures include authentication, authorization, cryptography, perimeter security, as well as methods for securing applications and various functional servers.

II. Student Learning Outcomes

A. Subject Matter

Upon successful completion of this course, the student will be able to:

1. Discover, categorize and rank the risks to organizational technology assets.
2. Research, analyze and implement appropriate measures to ensure the safeguarding of organizational technology assets.
3. Detect and evaluate security incidents.
4. Analyze policies and procedures related to handling a security incident and conduct the investigation according to industry standards and ethics.

B. University Learning Outcomes

This course enhances student abilities in the following areas:

Analytical Skills

Critical Thinking Skills: Students will research and evaluate security risks and evaluate possible appropriate responses to those risks. Students will synthesize knowledge of risks with knowledge of risk responses to prepare, assess and justify appropriate policies and technological procedures in support of those policies.

Ethical Decision Making

Students will identify ethical dilemmas and affected parties while preparing security policies. They will apply ethical frameworks to resolve ethical dilemmas while assessing and justifying security policies.

III. Major Course Topics

A. Fundamental aspects
B. Defensible Architectures
C. Networking & Protocols
D. Security mechanisms (countermeasures)
E. Updates and patches
F. Defense in depth
G. Critical Controls
H. Operational issues
I. Disaster Recovery
J. Business Continuity
K. Risk Management
L. Security Policy
M. Strategic Policy
N. Tactical Procedures
O. External and Internal Attacks
P. Security domains
Q. Cyber
R. Physical
S. People
T. Forensics
U. Electronic Evidence
V. Admissibility of E-Evidence
W. Forensic examination of electronics
X. Information states
Y. Security services
Z. Confidentiality
AA. Integrity
BB. Availability
CC. Threat analysis model
DD. Reconnaissance
EE. Scanning
FF. Gaining Access

GG. Maintaining Access
HH. Covering Tracks
II. Vulnerabilities