CPCS-463 Syllabus

Catalog Description

CPCS-463 Computing Systems Security
Credit: 3 (Theory: 3, Lab: 0, Practical: 0)
Prerequisite: CPCS-361 , CPCS-371
Classification: Elective

The objective of this course is to introduce the fundamentals of Computer Security Systems and the potential risks and vulnerabilities in these therein. Topics include security management practices, access control systems and methodology, networks and Internet security, enterprise security architecture, operations security law, investigation, and ethics.

Class Schedule

Meet 50 minutes 3 times/week or 80 minutes 2 times/week

Lab/Tutorial 90 minutes 1 times/week

Textbook

Charles P. Pfleeger, Shari Lawrence Pfleeger, , "Security in Computing", Prentice Hall; 4 edition (2007)

ISBN-13 9780132390774 **ISBN-10** 0132390779

Grade Distribution

Week	Assessment	Grade %

Topics Coverage Durations

Topics	Weeks
Security Management Practices	2
Access Control Systems and Methodology	2
Networks and Internet Security	3
Enterprise Security Architecture	3
Operations Security	2
Law, Investigation, and Ethics	2

Last Articulated

Relationship to Student Outcomes

a	b	c	d	e	f	g	h	i	j	k
x	x							x		

Course Learning Outcomes (CLO)

By completion of the course the students should be able to

1. To be familiar with computing systems security and their significance. ()
2. To be familiar with the division of computer systems in terms of security requirements. ()
3. To know the digital systems interference methods. ()
4. To be able to measure computer systems performance and making sure that they have not been breached. ()
5. To be familiar with military and navigational systems, ()
6. To be able to protect software and information against potential threats. ()
7. To be able to determine the requirements of computer systems. ()

Coordinator(s)