

**DEPARTMENT OF INDUSTRIAL ENGINEERING
COURSE SYLLABUS**

<i>COURSE TITLE</i>	<i>ENGLISH CODE/NO</i>	<i>ARABIC CODE/N O.</i>	<i>CREDITS</i>			
			<i>Th.</i>	<i>Pr.</i>	<i>Tr.</i>	<i>Total</i>
Industrial Information Security	IE 425	حص ٤٢٥	3	1	-	3
<i>Pre-requisites:</i>	IE 321					
<i>Course Role in Curriculum</i>	<i>Required or Elective:</i>		Elective			
<i>Catalogue Description:</i> Introduction to information security. Assessment of threats, vulnerabilities and risk exposure. Models for estimating risks and optimizing return on information security investment. Computer forensics, electronic evidence, frauds, cyber terrorism and computer criminal laws.						

Textbooks:

PRINCIPLES AND PRACTICE OF INFORMATION SECURITY, Linda Volonino, Stephen R. Robinson, Prentice Hall, ISBN-10: 0131840274, ISBN-13: 9780131840270

References:

APPLIED INFORMATION SECURITY, Randy Boyle, ISBN-10: 0136122035, ISBN-13: 9780136122036

Supplemental Materials:

Course Learning Outcomes:

By the completion of the course the student should be able to:

1. Understand basic terminology associated with information security.
2. Learn common information security threats including viruses, worms, Trojan horses etc.
3. Identify and rank organization's information assets.
4. Recognize vulnerabilities and security threats in organization's information network and prioritize them for remediation.
5. Determine methods used to verify the identity and authenticity of an individual.
6. Learn basic essentials of security in transmission and security in infrastructure.
7. Learn the concept and importance of information security audit.
8. Learn operational /organizational security.
9. Understand how policies and procedures play important role in addressing the security needs of an organization.
10. Know the laws and standards that govern information security.
11. Implement an appropriate information protection scheme to meets organization's requirement.
12. Investigate and analyze the computer system for compliance with organizational policies.

<u>Topics to be Covered:</u>		<u>Duration in Weeks</u>
1	Importance of information security management , definitions and terms associated with information security	1.5
2	Information security basics, access controls and authentication.	2
3	Vulnerability, threats and risk exposure including hacking, viruses, worms, Trojan horses etc.	2.5
4	An overview of security in transmission and security in infrastructure	2
5	Information security auditing	2
6	Information security standards, policies and procedures.	2
7	Computer forensic, electronic evidence and computer crime laws.	2

Student Outcomes addressed by the course: (Put a \checkmark sign)

(a)	an ability to apply knowledge of mathematics, science, and engineering	
(b)	an ability to design and conduct experiments, as well as to analyze and interpret data	
(c)	an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability	\checkmark
(d)	an ability to function on multidisciplinary teams	
(e)	an ability to identify, formulate, and solve engineering problems	
(f)	an understanding of professional and ethical responsibility	
(g)	an ability to communicate effectively	\checkmark
(h)	the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context	
(i)	a recognition of the need for, and an ability to engage in life-long learning	
(j)	a knowledge of contemporary issues	
(k)	an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.	\checkmark

Key Student Outcomes assessed in the course: () and ()

Instructor or course coordinator: Dr. Manzoor Hussain Sheikh

Last updated: Jan. 2014