



KIoT

Department of Information Technology

Course Guide Book	
Program	Regular
Course Information	
Module Name	Information Technology and Society
Module code	ITec-M3141
Course Title	Information Assurance and Security
Course Code	ITec4143
ECTS	5 (2hrs Lecture, 3hrs Laboratory)
Prerequisite	None
Academic Year	2012
Semester	II
Target Group	4 th Year Information Technology Students
Instructor Name	Tadesse M.
Instructor Address	E-mail: tadimulehu@gmail.com
Course Description	
<p>This course covers theory and practice of Information system security. Students will learn the principles of information security, security architectures and models, aspects and methods of information security such as physical security control, operations security, access control, security threats, risks, vulnerabilities, Data security Policies/Admin, Security Procedural Control, Designing secure systems, Cryptography-symmetric and asymmetric. Students will also learn how to plan and manage security, security policies, business continuity plans, disaster recovery plans, and social and legal issues of information security.</p>	

Course Contents and Schedule

Week	Topics or Subtopics or Chapters	Learning Outcomes of Each Chapters
1,2	Chapter-1 – Computer security and privacy <ul style="list-style-type: none"> ✓ Course Introduction ✓ Communications and Information ✓ Security Goals ✓ Enterprise Security ✓ Enterprise Security within an Enterprise Architecture Context 	<p>After completing this chapter, the students are expected to:</p> <ol style="list-style-type: none"> 1. Understand about the basic concepts of computer security and how to maintain security of an enterprise
3,4,5	Chapter-2 – Web services security <ul style="list-style-type: none"> ✓ Web Services Security – Introduction ✓ Brief Overview of Commercial Issues ✓ Convergence 	<p>After completing this chapter, the students are expected to:</p> <ol style="list-style-type: none"> 1. Understand how to provide

	<ul style="list-style-type: none"> ✓ Internet Security Architecture ✓ Internet security: IPV 4/6 Security Considerations 	information security on the web
6,7,8	Chapter-3 – Network security <ul style="list-style-type: none"> ✓ Network Firewall Security (Firewall Rules) ✓ Host Security (authentication and authorization techniques) ✓ Cyber defense ✓ Introduction to the TCP/IP Stack ✓ Network Security (ports and protocols) ✓ Intrusion Detection System/Prevention (IDS/IPS): overview 	<p>At the end of this chapter the students are expected to:</p> <ol style="list-style-type: none"> 1. Understand ways that provide secure communication on the network 2. Understand different user authentication and authorization techniques 3. Understand how to set firewall rules to filter inbound and outbound traffic
9,10,11	Chapter-4 - Cryptography <ul style="list-style-type: none"> ✓ Terminology ✓ Review of Shared Key Cryptography and Hash Functions ✓ Basic Public Key Cryptography (DH, RSA, CAs) ✓ Wired/Wireless PKI (Public Key Infrastructure) 	<p>At the end of this chapter the students are expected to:</p> <ol style="list-style-type: none"> 1. Understand various cryptographic techniques used to provide information security
12,13,14	Chapter 5: Application security <ul style="list-style-type: none"> ✓ Application Security (vulnerabilities of programming/scripting languages) ✓ Malicious Code (virus, worms, malware) ✓ Securing Services (shells, e-mail, web servers) ✓ Identifying Vulnerabilities (tools and techniques) 	<p>After completing this chapter, the students are expected to</p> <ol style="list-style-type: none"> 1. Know how to "build security in" rather than consider it as an afterthought, 2. have a plethora of skills, applicable at each phase of SDLC that can be used to strengthen the security of software systems.

Course Assessment Methods

Continuous Assessment Method	Expected Assessment date	Expected Feedback date	Weight
Tests	05/08/2012	15/08/2012	15%
Lab exam	25/08/2012	30/08/2012	20%
Mid exam	15/09/2012	22/09/2012	25%
Final Examination	Final exam schedule	As per the University's Schedule	40%

Reference:

- 1, Defensive Security Handbook: Best Practices for Securing Infrastructure
- 2, Hacker Techniques, Tools, and Incident Handling: information systems security and assurance series, Jones and Bartlett learning books
- 3, CRYPTOGRAPHY - QUICK GUIDE:
http://www.tutorialspoint.com/cryptography/cryptography_quick_guide.htm

Prepared by

Name: Tigist S.

Signature: _____

Date: _____

Approved by

QA Focal person

Department Head

Name: Tadesse M.

Name: Kedir A.

Signature: _____

Signature: _____

Date: _____

Date: _____