

Master Course Record Form

Course Prefix and Number: IT 275
Course Title: Security Fundamentals
Recommended Transcript Title: Security Fundamentals
Date Approved/Revised
Credit Hours: 3 Contact hours per week (Based on 15 week term): Lecture: 3 Lab:
Prerequisite: CIS 114 or permission of instructor Corequisite: Pre/Corequisite:
Grading Mode: Letter grade
Catalog Description: This course introduces concept of information security. It provides students with the understanding of the need for an organizational policy on security and the various services related to the policy such as integrity, authentication, confidentiality, nonrepudiation and access control. It also, provides instruction on physical security, network security and computer security. It broadens the students' awareness of network security to include accidental damage, of denial of service attacks and malicious software and proactive measure to create defenses against these risks.
Course Outcomes: <ul style="list-style-type: none"> A. Define information security (IS) and information assurance (IA), and explain their relevance to information systems and information technology. B. Describe security services needed for modern information systems. C. Describe common threats to and attacks against information systems. D. Explain the need for an organization to define an information security policy describing the services required to secure the organization's information assets, and for information security technologies adopted by the organization to be consistent with the policy requirements. E. Explain and describe Security Layers, Operating System Security, Network Security, and Security Software. <p style="text-align: center;">○</p>
Implementation Cycle: Spring
Role in College Curriculum: Role in College Curriculum: (Check all that apply) <input type="checkbox"/> General Education Core (Specify category) <input checked="" type="checkbox"/> Technical Core (Specify Program) (CAS in IT) <input checked="" type="checkbox"/> Restricted Elective: (AAS in IT)

Course Number & Title: IT 275- Security Fundamentals

Date Prepared: April 6, 2015

Submitted to LOT:

Date Course Approved by LOT: April 20, 2015

Master Course Record Form

<input checked="" type="checkbox"/> General Elective <input type="checkbox"/> Workforce Education <input type="checkbox"/> Other (Please specify)
Course Fee: Yes
Instructor's Qualifications: Bachelor's degree in information technology with two years of related work experience in IT field or master's degree with 18 graduate hours in IT.
Expanded Course Description: It provides the student with the skills and knowledge necessary to take the Microsoft Technology Exam in Security Fundamentals (98-367). Expanded outcomes: <ul style="list-style-type: none">F. Define information security (IS) and information assurance (IA), and explain their relevance to information systems and information technology.G. Describe security services needed for modern information systems.H. Describe common threats to and attacks against information systems.I. Explain the need for an organization to define an information security policy describing the services required to secure the organization's information assets, and for information security technologies adopted by the organization to be consistent with the policy requirements.J. Understand Security Layers:<ul style="list-style-type: none">• Understand core security principles<ul style="list-style-type: none">○ Confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface• Understand physical security<ul style="list-style-type: none">○ Site security; computer security; removable devices and drives; access control; mobile device security; disable Log On Locally; keyloggers• Understand Internet security<ul style="list-style-type: none">○ Browser settings; zones; secure websites• Understand wireless security<ul style="list-style-type: none">○ Advantages and disadvantages of specific security types; keys; service set identifiers (SSIDs); MAC filtersK. Understand Operating System Security<ul style="list-style-type: none">• Understand user authentication<ul style="list-style-type: none">○ Multifactor; smart cards; Remote Authentication Dial-In User Service (RADIUS); Public Key Infrastructure (PKI); understand the certificate chain; biometrics; Kerberos and time skew; use Run As to perform administrative tasks; password reset procedures• Understand permissions<ul style="list-style-type: none">○ File; share; registry; Active Directory; NT file system (NTFS) versus

Course Number & Title: IT 275- Security Fundamentals

Date Prepared: April 6, 2015

Submitted to LOT:

Date Course Approved by LOT: April 20, 2015

Master Course Record Form

- file allocation table (FAT); enable or disable inheritance; behavior when moving or copying files within the same disk or on another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; delegation
- Understand password policies
 - Password complexity; account lockout; password length; password history; time between password changes; enforce by using Group Policies; common attack methods
- Understand audit policies
 - Types of auditing; what can be audited; enable auditing; what to audit for specific purposes; where to save audit information; how to secure audit information
- Understand encryption
 - Encrypting file system (EFS); how EFS-encrypted folders impact moving/copying files; BitLocker (To Go); TPM; software-based encryption; MAIL encryption and signing and other uses; virtual private network (VPN); public key/private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; token devices
- Understand malware
 - Buffer overflow; worms; Trojans; spyware
- L. Understand Network Security
 - Understand dedicated firewalls
 - Types of hardware firewalls and their characteristics; why to use a hardware firewall instead of a software firewall; SCMs and UTMs; stateful versus stateless inspection
 - Understand Network Access Protection (NAP)
 - Purpose of NAP; requirements for NAP
 - Understand network isolation
 - Virtual local area networks (VLANs); routing; honeypot; perimeter networks; network address translation (NAT); VPN; IPsec; server and domain isolation
 - Understand protocol security
 - Protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; common attack methods
- M. Understand Security Software
 - Understand client protection
 - Antivirus; User Account Control (UAC); keep client operating system and software updated; encrypt offline folders, software restriction policies

Course Number & Title: IT 275- Security Fundamentals

Date Prepared: April 6, 2015

Submitted to LOT:

Date Course Approved by LOT: April 20, 2015

Master Course Record Form

- Understand email protection
 - Antispam, antivirus, spoofing, phishing, and pharming; client versus server protection; Sender Policy Framework (SPF) records; PTR records
- Understand server protection
 - Separation of services; hardening; keep server updated; secure dynamic Domain Name System (DNS) updates; disable unsecure authentication protocols; Read-Only Domain Controllers (RODC); separate management VLAN; Microsoft Baseline Security Analyzer (MBSA)

Prepared by: Vincenza Cumbo

April 6, 2015

Signature, Title

Date

Approved by:

Dean, Academic & Student Services

Date

Course Number & Title: IT 275- Security Fundamentals

Date Prepared: April 6, 2015

Submitted to LOT:

Date Course Approved by LOT: April 20, 2015