MARICOPA
COMMUNITY COLLEGES

## Information Security Fundamentals

| | |
|---|---|
| Course: **ITS110** | Lec + Lab **3.0** Credit(s) **4.0** Period(s) **4.0** Load |
| | Course Type: **Occupational** |
| First Term: **2020 Fall** | Load Formula: **T - Lab Load** |
| Final Term: **Current** | |

**Description:** Fundamental concepts of information technology security. Topics include authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies and securing infrastructures and topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of Transmission Control Protocol/Internet Protocol (TCP/IP) and security concepts and Microsoft (MS) Windows and Linux Administration.

**Requisites:** Prerequisites: A grade of C or better in CIS126DL, or CIS126RH, or permission of Program Director. Corequisites: BPC270 or MST150++.

### MCCCD Official Course Competencies

1. Explain the need for authentication methods and available solutions. (I)
2. Implement appropriate access control methods and demonstrate techniques for monitoring access to network resources. (II)
3. Apply cryptographic methods to ensure data integrity and privacy. (III)
4. Explain the elements of Public Key Infrastructure and how to plan for implementation. (IV)
5. Identify the types of threats to networks and the steps to take to reduce these threats. (V)
6. Identify vulnerabilities in operating system software and network devices, and implement measures to mitigate these vulnerabilities. (VI)
7. Demonstrate methods to secure remote access to network resources. (VII)
8. Identify weaknesses in wireless technology and implement measures to secure wireless environments. (VIII)
9. Explain the methods used to design and maintain a secure network infrastructure. (IX)
10. Explain the techniques used to assess risk, detect network intrusions and ensure the continuity of network resources. (X)
11. Describe the elements of effective security policies in a business environment. (XI)

### MCCCD Official Course Outline

I. Authentication methods
  A. Security terms
  B. Central Intelligence Agency and non-repudiation
  C. Security standards

D. Kerberos
E. Certificates
F. Token-based authentication
G. Challenge Handshake Authentication Protocol (CHAP)
H. Smart Cards
I. Biometrics
J. Extensible Authentication Protocol (EAP)

II. Access control
A. Access control terminology and concepts
B. Auditing and logging
C. Isolating the auditing system
D. Filtering logs
E. Audit trails and the collection of evidence
F. Access Control Methods Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC)
G. Balancing responsibilities of security

III. Cryptography
A. Cryptography and encryption
B. Common cryptography terms
C. Types of encryption algorithms
D. Services provided by encryption
E. Hash encryption
F. Symmetric-key encryption
G. Asymmetric-key encryption
H. Applied encryption

IV. Public Key Infrastructure (PKI)
A. PKI terms
B. Types of certificates
C. PKI standards and protocols
D. Public-Key Infrastructure X.509 (PKIX)
E. Certificate policies
F. Certificate Practice Statement (CPS)
G. Certificate revocation
H. Online Certificate Status Protocol (OCSP)
I. Trust models
J. Centralized and decentralized key management
K. Key management and certificate life cycles
L. Certificate and key storage
M. Planning for PKI

V. Network attacks and vulnerabilities
A. File Transfer Protocol/Internet Protocol (FTP/IP) protocol suite overview
B. Spoofing attacks
C. Scanning attacks
D. Denial-of-Service (DOS) attacks
E. Distributed Denial-of-Service (DDOS) attacks
F. Mitigating vulnerability and risk
G. Man-in-the-Middle attacks
H. Packet sniffing

I. TCP/IP Connection hijacking
J. Domain Name System (DNS) and Address Resolution Protocol (ARP) cache poisoning
K. Password-guessing attacks
L. Software exploitation
M. Back door
N. Weak keys
O. Birthday attack
P. Mathematical attacks
Q. Social Engineering
R. Hoaxes
S. Malicious code
T. Viruses
U. Worms
V. Illicit servers
W. Trojan horses and root kits
X. Logic bombs
Y. Managing malware
Z. Auditing, logging and system scanning
VI. Operating system and application hardening
A. Security baselines
B. Client security issues
C. Encryption: Secure Socket Layer (SSL) and Transport Layer Security (TLS)
D. Isolating services and jails
E. Mail servers and Simple Mail Transport Protocol (SMTP) relay
F. File sharing
G. File transfer vulnerabilities
H. Server Message Block (SMB) encryption
I. File Transfer Protocol (FTP)
J. Securing web servers
K. DNS servers
L. Data repositories
M. Operating system hardening
VII. Securing remote access
A. Concepts, terminologies and methods
B. Virtual Private Networks (VPNs)
C. Terminal Access Controller Access Control System (TACACS and TACACS+)
D. Remote Authentication Dial-In User Service (RADIUS)
E. Internet Protocol Security (IPSec)
F. 802.1x
G. Remote administration methods
H. Secure Shell (SSH)
VIII. Wireless network security
A. Wireless technologies
B. Wireless networking modes
C. Wireless cells
D. Wireless Application Protocol (WAP)
E. Wireless Transport Layer Security (WTLS)
F. Wireless Vulnerabilities and Wired Equivalent Privacy (WEP)

G. Solutions for wireless network vulnerabilities
H. Site surveys and war driving
IX. Securing topologies and infrastructure
A. Firewall overview
B. Security topologies
C. Security zones
D. Virtual Local Area Network (LAN) (VLAN)
E. Network Address Translation (NAT)
F. Traffic control methods
G. Configuring firewalls
H. Configuring an Access Control List (ACL)
I. Network device hardening
J. Physical security
K. Cabling and network security
X. Risk analysis, intrusion detection and business continuity
A. Risk identification
B. Intrusion detection systems
C. Honey pots
D. Incident response policy
E. Forensics
F. Disaster recovery plan
G. Business continuity
XI. Security policy management
A. Security policy
B. Human resource policies
C. Documentation

MCCCD Governing Board Approval Date: **February 25, 2020**

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.