Center for Curriculum and Transfer Articulation

Information Security Principles

Course: **CIS272DB** Lec + Lab **3** Credit(s) **4** Period(s) **3.7** Load
Course Type: **Occupational**
First Term: **2014 Fall** Load Formula: **S- Standard**
Final Term: **Current**

Description: Covers threats to the IT infrastructure and how they can impact operations. Demonstrates strategies to mitigate risk impacts as they relate to the IT infrastructure. Provides technical knowledge required to execute on the essentials of information security. Provides partial preparation for certification in one or all of the following: Comptia Security + exam, International Information Systems Security Certification Consortium ((ISC)2), Systems Security Certified Practitioner (SSCP) exam, the Committee on National Security Systems (CNSS) 4011 certification, or GIAC Security Essentials Certificate (GSEC).

Requisites: Prerequisites: CIS271DB.

MCCCD Official Course Competencies

1. Describe threats, attacks and vulnerabilities that impact the IT infrastructure (I, VI).
2. Demonstrate security tools and techniques that mitigate risk (I, VI).
3. Explain the fundamentals of encryption and cryptography (II).
4. Explain how security is managed from an operational perspective including access control, security operations, administration and day-to-day security activities (V, VI).
5. Describe audit, testing and monitoring strategies, which are designed to support security verification (IV)
6. Describe tactical security risks that threaten the stability of the IT enterprise including malicious code activity (III).
7. Describe information technology protection mechanisms (VI).

MCCCD Official Course Outline

I. Attacks, Threats and Vulnerabilities
A. Malicious Activity
B. Asset Protection
1. Information
2. IT Infrastructure
3. Intellectual Property
4. Finances and Financial Data
5. Availability and Reliability
6. Reputation
C. Attack Tools
1. Vulnerability Scanners
2. Port Scanners

2. Port Scanners
3. Sniffers
4. Wardialers
5. Keyloggers

D. Breach Types

1. Denial of Service
2. Drive By
3. Virus Infection
4. Code Exploitation
5. Wiretapping
6. Backdoor
7. Data Modifications

E. Malicious Attacks

1. Brute-Force Attacks
2. Dictionary Attacks
3. Address Spoofing
4. Hijacking
5. Replay Attacks
6. Man-in-the-Middle Attacks
7. Masquerading
8. Eavesdropping
9. Social Engineering
10. Phreaking
11. Phishing
12. Pharming

F. Malicious Software

1. Viruses
2. Worms
3. Trojan Horses
4. Rootkits
5. Spyware

G. Countermeasures

1. System Countermeasures
2. Network Countermeasures
3. Human Countermeasures
4. Application Countermeasures

II. Cryptography

A. Cryptographic Principles

1. Cryptography Basics
2. History of Cryptography
3. Cryptography?s Role in Information Security

B. Business and Security Requirements for Cryptography

1. Internal Security
2. Security Between Business
3. Security Measures that Benefit everyone

C. Cryptographic Applications and Uses in Information System Security

1. Cryptanalysis and Public Versus Private Keys
2. Cryptographic Functions and Ciphers
3. Types of Ciphers

3. Types of Ciphers
4. Symmetric and Asymmetric Key Cryptography
5. Keys, Key space, and Key Management
6. Digital Signatures and Hash Functions
7. Symmetric Key Standards
8. Asymmetric Solutions
9. Hash Function and Integrity
10. Digital Signatures and Nonrepudiation
11. Principles of Certificate and Key Management
12. Modern Key-Management Techniques

D. Encryption

1. Encryption mechanisms
2. Data in motion
3. Data at rest

III. Malicious Code and Activity

A. Characteristics, Architecture and Operations of Malicious Software

B. Malware Types

1. Virus
2. Spam
3. Worms
4. Trojan Horses
5. Logic Bombs
6. Activity Content Vulnerabilities
7. Botnets
8. Denial of Service Attacks
9. Spyware
10. Adware
11. Phishing
12. Keystroke Loggers
13. Hoaxes and Myths
14. Home-Page Hijacking
15. Web-Page Defacements

C. History of Malicious Code Threats

1. 1970s and Early 1980s: Academic Research and UNIX
2. 1980?s: Early PC Viruses
3. 1990s: Early LAN Viruses
4. Mid-1990s: Smart Applications and the Internet
5. 2000 to Present: Mobile Device threats

D. Business Threats

1. Types of Threats
2. Internal Threats
3. External Threats

E. Ports and Protocols

F. Anatomy of an Attack

1. Attack Motivators
2. Attack Purposes
3. Types of Attacks
4. Phases of an Attack

G. Attack Prevention Tools and Techniques

G. Attack Prevention Tools and Techniques
1. Application Defenses
2. Operating System Defenses
3. Network Defenses
4. Safe Recovery Techniques and Practices
5. Implementing Effective Software Best Practices
H. Incident Detection Tools and Techniques
1. Antivirus Scanning Software
2. Network Monitors and Analyzers
3. Content/Context Filtering and Logging Software
4. Honeypots and Honeynets
IV. Auditing, Testing and Monitoring
A. Security Auditing and Analysis
1. Security Controls Address Risk
2. Acceptable Levels
3. Permission Levels
4. Areas of Security Audits
5. Purpose of Audits
6. Customer Confidence
7. Defining an Audit Plan
B. Post Audit Activities
1. Exit Interview
2. Data Analysis
3. Generation of Audit Report
4. Presentation of Findings
C. Security Monitoring
1. Security Monitoring for Computer Systems
2. Monitoring Issues
3. Logging Anomalies
4. Log Management
5. Types of Logs
D. Security Control Verification
1. Intrusion Detection/Prevention Systems
2. Analysis Methods
3. Host Intrusion Detection System
4. Layered Defense
5. Control Checks
6. Host Isolation
7. System Hardening
8. Wireless and Wire line Network Hardening
9. Antivirus
V. Security Operations and Administration
A. Security Administration
1. Controlling Access
2. Documentation, Procedures and Guidelines
3. Disaster Assessment and Recovery
4. Security Outsourcing
B. Compliance
1. Security Event Logs

1. Security Event Logs

2. Compliance Liaison

3. Remediation

C. Professional Ethics

1. Common Fallacies About Ethics

2. Code of Ethics

3. Personnel Security Principles

D. IT Security Policy Infrastructure

1. Policies

2. Standards

3. Procedures

4. Baselines

5. Guidelines

E. Data Classification Standards

1. Information Classification Objectives

2. Examples of Classification

3. Classification Procedures

4. Assurance

F. Configuration and Change Management

1. Inventory and Configuration

2. Change Controls Management

3. Change Control Committees

4. Change Control Procedures

5. Change Control Issues

G. System Development Lifecycle

1. Testing and Developing Systems

2. Software Development and Security

3. Software Development Methods

VI. Security Protection Tools and Techniques

A. Intrusion Detection and Prevention

1. Identifying Threats

2. Identifying Vulnerabilities

3. Identifying Countermeasures

4. Preventing Security Breaches

B. Firewalls and Access Control

1. Protecting Externally Facing Systems

2. Protecting Critical Information

3. Network Segmentation

4. Application Segmentation

5. System Segmentation

C. Security Event Management

1. Risk Correlation

2. Threat Analysis

3. Vulnerability Analysis

D. Security Assessments

1. Vulnerability Assessment

2. Penetration Test

3. Breach Indicators

4. IT Security Assessment

4. IT Security Assessment

5. Security Program Assessment

E. Policies, Processes, Standards and Procedures

1. Policies

2. Processes

3. Standards

4. Procedures

Last MCCCD Governing Board Approval Date: **June 24, 2014**

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.