CHAPTER 1: ORGANIZATIONAL POLICY

LEARNING OBJECTIVES
- Identify requirements of the organizational security policies.
- Recognize the three levels of security.
- Recognize proper security safeguards.

TOPICS COVERED
- Organizational Policy
- Security Administration
- Establishing a Security Policy
- The Security Administrator
- Final Consideration

CHAPTER 2: PHYSICAL SECURITY AND DATA PRESERVATION

LEARNING OBJECTIVES
- After completing this section, you should be able to:
- Recognize the different lines of defense for a computer system.
- Identify environmental considerations as they apply to computer security.
- Recognize the components of a maintenance log.
- Identify computer access controls for software and data files.

TOPICS COVERED
- Computer Facilities
- Environmental Considerations
- Protecting Information
- Controlling Access
- Hardware Security
- Software and Devices for Physical Security

CHAPTER 3: HARDWARE SECURITY

LEARNING OBJECTIVES
- Identify some of the most common hardware problems.
- Identify how data integrity may be threatened.
- Recognize some hardware security devices used to protect the computer system.

TOPICS COVERED
- Physical Security
- Data Integrity
- Deploying a Security System
- VPN Solution
- Smart Cards
- eToken
- Biometrics
- Intrusion Prevention Systems (IPS)
- Laptop Security

CHAPTER 4: SOFTWARE SECURITY

LEARNING OBJECTIVES
- Identify top security related products in use.
- Recognize different types of viruses and security threats.
- Recognize the uses of firewall security systems.

TOPICS COVERED
- Security Breaches
- What is a Virus?
- Illegal Access and Use - Hacking
- Ransomware
- What is a Firewall?
- What is Authentication?
- What is Encryption?
- Public/Private Key Technology in Online Trading
- What is Digital Signature?
- What is a Public Key Infrastructure (PKI)?
- What is Kerberos?
- What is Pretty Good Privacy?
- What was the Orange Book?
- Internet Security Market
- Security Protocols
- What is VPN?
- Doing Business over the Internet
- E-mail Security
- Hacked Email 66

CHAPTER 5: PERSONNEL SECURITY

LEARNING OBJECTIVES
- Identify prerequisites for sensitive personnel positions.

- Recognize the value of an employee performance evaluation system and components of a training system.
- Identify security issues posed by terminated employees.

TOPICS COVERED
- Screening
- Legal Agreements
- Training New Employees
- Performance Appraisal
- Exit Procedures

CHAPTER 6: NETWORK SECURITY

LEARNING OBJECTIVES
- Recognize network tools used to implement security plans.
- Identify the tools and techniques used by saboteurs.

Topics Covered
- Passwords
- Saboteur's Tools
- Considerations in Designing Networks
- Secure Sockets Layer
- Firewalls
- Pretty Good Privacy (PGP)
- Vulnerability Testing Using Automated Tools
- Protecting Your Networks from Ransomware

CHAPTER 7: SECURITY POLICY

LEARNING OBJECTIVES
- Identify questions that policy makers should answer when designing a security system.
- Recognize activities conducted as part of the risk analysis and management.
- Recognize human factor threats for security.

TOPICS COVERED
- Managing Computer Security
- Creating the Policy and the Plan
- Risk Analysis and Management
- The Security Administrator
- The Human Factor
- Account Administration

CHAPTER 8: CONTINGENCY PLANNING

Learning Objectives
- Recognize the types of disruptions in computer processing.
- Recognize components of a contingency plan.
- Identify fire safety preventive plans.

Topics Covered
- The Role of Senior Management
- Mobile Device Security and Contingency Planning
- The Contingency Planning Committee
- Areas to Cover
- Fire Safety
- Insurance

CHAPTER 9: AUDITING AND LEGAL ISSUES

LEARNING OBJECTIVES
- Identify the scope of internal and external security auditing.
- Recognize the audit trail to identify unusual activities.
- Recognize control techniques.
- Identify EDI security risks.

TOPICS COVERED
- Security Auditing
- Audit Trail
- EDI and Electronic Contracting
- Auditing Contingency Plans
- Controls
- Audit Software
- Legal Liability in Security Management

CHAPTER 10: COMPUTER CRIME, CYBERFRAUD, AND RECENT TRENDS

LEARNING OBJECTIVES
- Recognize penalties of the US Computer Fraud and Abuse Act.
- Identify major issues regarding computer crimes and privacy issues.
- Identify new certificate programs in computer security.

TOPICS COVERED
- Computer Crime
- Privacy Issues
- Tools of Security Management
- Other Security Measures
- Cloud Computing
- FTC - Computer Security