

7. Writing Information Security Policies and Procedures

7.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information security management principles. Participants should have a good command of English language and grammar. There are no other prerequisites.

7.2 Course Objectives

You will learn:

- Information Security management concepts and terminology
- How to plan and organize an Information Security documentation program in your organization
- How to determine your organization's policy needs
- How to develop and implement effective information security policies and procedures according to your organization's specific needs
- Understand the role that policies, procedures, standards and guidelines play in an organization's information security strategy
- How to manage the information security policy and procedure process as a project
- How to develop and implement a documentation review process

7.3 Course Description

This course addresses one of the key aspects of information security: policy. The purpose of information protection is to protect an organization's resources. The cornerstone of any information security strategy is a robust set of policies, procedures, standards and guidelines. Participants will learn the importance of developing an information security documentation program in their organizations and how to go about developing and implementing effective policies and procedures. Participants will understand that providing information protection requires a comprehensive approach that considers areas within and outside the area of information technology. Effective information security often involves sustained process improvement. Participants will focus on the following areas: Information Protection Fundamentals, Writing Mechanics and the Message, Policy Development, Mission Statement, Standards, Writing Procedures, Information Classification, and How to Manage the Process as a Project. Examples of various policies and procedures will be provided.

7.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

7.5 Course Topics

1. Overview of Information Protection Fundamentals
 - 1.1. Elements of Information Protection
 - 1.2. More than just computer security
 - 1.3. Roles and responsibilities
 - 1.4. Common Threats

- 1.5. Policies and Procedures
- 1.6. Risk Management
- 1.7. Typical Information Protection program
2. Writing Mechanics and the Message
 - 2.1. Attention spans
 - 2.2. Key concepts
 - 2.3. Topic sentence and thesis statement
 - 2.4. The message
3. Policy Development
 - 3.1. Policy definitions
 - 3.2. Frequently asked questions
 - 3.3. Policies are not enough: a preliminary look at standards, guidelines, and procedures
 - 3.4. Policy, standards, guidelines, and procedures: definitions and examples
 - 3.5. Policy key elements
 - 3.6. Policy format and basic policy components
 - 3.7. Policy content considerations
 - 3.8. Program policy examples
 - 3.9. Topic specific policy examples
 - 3.10. Topic specific policy subjects to consider
 - 3.11. An approach for success
4. Mission Statement
 - 4.1. Background on your position
 - 4.2. Business goals versus security goals
 - 4.3. Computer security objectives
 - 4.4. Mission statement format
 - 4.5. Allocation of information security responsibilities (ISO 17799)
 - 4.6. Mission statement examples
 - 4.7. Support for the mission statement
 - 4.8. Key roles in organizations
 - 4.9. Business objectives
5. Standards
 - 5.1. Where does a standard go?
 - 5.2. What is a standard?
 - 5.3. International standards
6. Writing Procedures
 - 6.1. Definitions
 - 6.2. Writing commandments
 - 6.3. Key elements in procedure writing

- 6.4. Procedure checklist
- 6.5. Getting started
- 6.6. Procedure styles
- 6.7. Creating a procedure
- 7. Information Classification
 - 7.1. Why classify information?
 - 7.2. What is information classification?
 - 7.3. Establish a team
 - 7.4. Developing the policy
 - 7.5. Resist the urge to add categories
 - 7.6. What constitutes confidential information?
 - 7.7. Classification examples
 - 7.8. Declassification or reclassification of information
 - 7.9. Information classification methodology
 - 7.10. Authorization of access
- 8. Security Awareness Program
 - 8.1. Key goals of an information security program
 - 8.2. Key elements of a security program
 - 8.3. Security awareness program goals
 - 8.4. Identify current training needs
 - 8.5. Security awareness program development
 - 8.6. Methods used to convey the awareness message
 - 8.7. Presentation key elements
 - 8.8. Typical presentation format
 - 8.9. When to do awareness
 - 8.10. The information security message
 - 8.11. Information security self-assessment
- 9. Why Manage This Process as a Project?
 - 9.1. First things first – identify the sponsor
 - 9.2. Defining the scope of work
 - 9.3. Time management
 - 9.4. Cost management
 - 9.5. Planning for quality
 - 9.6. Managing human resources
 - 9.7. Creating a communications plan
- 10. Information Technology: Code of Practice for Information Security Management
 - 10.1. Terms and definitions
 - 10.2. Information security policy

- 10.3. Organization security
- 10.4. Asset classification and control
- 10.5. Personnel security
- 10.6. Physical and environmental security
- 10.7. Communications and operations management
- 10.8. Access control policy
- 10.9. Systems development and maintenance
- 10.10. Business continuity planning
- 10.11. Compliance
- 11. Determining Your Policy Needs
 - 11.1. Identify what is to be protected
 - 11.2. Identify from whom it is being protected
 - 11.3. Data security considerations
 - 11.4. Backups, archival storage, and disposal of data
 - 11.5. Intellectual property rights and policies
 - 11.6. Incident response and forensics
- 12. Writing the Security Policies
 - 12.1. Physical Security
 - 12.2. Authentication and Network Security
 - 12.3. Internet Security Policies
 - 12.4. Email Security Policies
 - 12.5. Viruses, Worms, and Trojan Horses
 - 12.6. Encryption
 - 12.7. Software Development Policies
- 13. Maintaining the Policies
 - 13.1. Acceptable Use Policies
 - 13.2. Compliance and Enforcement
 - 13.3. The Policy Review Process