

INFORMATION SECURITY FUNDAMENTALS

Table of Contents

OVERVIEW

Elements of Information Protection
More Than Just Computer Security
Employee Mind-Set toward Controls
Roles and Responsibilities
Director, Design and Strategy
Common Threats
Policies and Procedures
Risk Management
Typical Information Protection Program
Summary

THREATS TO INFORMATION SECURITY

What Is Information Security?
Common Threats
Errors and Omissions
Fraud and Theft
Malicious Hackers
Malicious Code
Denial-of Service-Attacks
Social Engineering
Common Types of Social Engineering
Summary

THE STRUCTURE OF AN INFORMATION SECURITY PROGRAM

Overview
Enterprisewide Security Program
Business Unit Responsibilities
Creation and Implementation of Policies and Standards
Compliance with Policies and Standards
Information Security Awareness Program
Frequency
Media
Information Security Program Infrastructure
Information Security Steering Committee
Assignment of Information Security Responsibilities
Senior Management
Information Security Management
Business Unit Managers
First Line Supervisors
Employees
Third Parties
Summary

BUY ONLINE FROM: <http://www.27001.com/products/76>

INFORMATION SECURITY POLICIES

Policy Is the Cornerstone
Why Implement an Information Security Policy
Corporate Policies
Organizationwide (Tier 1) Policies
Employment
Standards of Conduct
Conflict of Interest
Performance Management
Employee Discipline
Information Security
Corporate Communications
Workplace Security
Business Continuity Plans (BCPs)
Procurement and Contracts
Records Management
Asset Classification
Organizationwide Policy Document
Legal Requirements
Duty of Loyalty
Duty of Care
Federal Sentencing Guidelines for Criminal Convictions
The Economic Espionage Act of 1996
The Foreign Corrupt Practices Act (FCPA)
Sarbanes-Oxley (SOX) Act
Health Insurance Portability and Accountability
Act (HIPAA)
Gramm-Leach-Bliley Act (GLBA)
Business Requirements
Definitions
Policy
Standards
Procedures
Guidelines
Policy Key Elements
Policy Format
Global (Tier 1) Policy
Topic
Scope
Responsibilities
Compliance or Consequences
Sample Information Security Global Policies
Topic-Specific (Tier 2) Policy
Thesis Statement
Relevance
Responsibilities
Compliance
Supplementary Information
Application-Specific (Tier 3) Policy
Summary

BUY ONLINE FROM: <http://www.27001.com/products/76>

ASSET CLASSIFICATION

- Introduction
- Overview
- Why Classify Information?
- What Is Information Classification?
- Where to Begin?
- Information Classification Category Examples
- Example 1
- Example 2
- Example 3
- Example 4
- Resist the Urge to Add Categories
- What Constitutes Confidential Information
- Copyright
- Employee Responsibilities
- Owner
- Information Owner
- Custodian
- User
- Classification Examples
- Classification: Example 1
- Classification: Example 2
- Classification: Example 3
- Classification: Example 4
- Declassification or Reclassification of Information
- Records Management Policy
- Sample Records Management Policy
- Information Handling Standards Matrix
- Printed Material
- Electronically Stored Information
- Electronically Transmitted Information
- Record Management Retention Schedule
- Information Classification Methodology
- Authorization for Access
- Owner
- Custodian
- User
- Summary

ACCESS CONTROL

- Business Requirements for Access Control
- Access Control Policy
- User Access Management
- Account Authorization
- Access Privilege Management
- Account Authentication Management
- System and Network Access Control
- Network Access and Security Components
- System Standards

BUY ONLINE FROM: <http://www.27001.com/products/76>

- Remote Access
- Operating System Access Controls
- Operating Systems Standards
- Change Control Management
- Monitoring System Access
- Event Logging
- Monitoring Standards
- Intrusion Detection Systems
- Cryptography
- Definitions
- Public Key and Private Key
- Block Mode, Cipher Block, and Stream Ciphers
- Cryptanalysis
- Sample Access Control Policy
- Summary

PHYSICAL SECURITY

- Data Center Requirements
- Physical Access Controls
- Assets to be Protected
- Potential Threats
- Attitude toward Risk
- Sample Controls
- Fire Prevention and Detection
- Fire Prevention
- Fire Detection
- Fire Fighting
- Verified Disposal of Documents
- Collection of Documents
- Document Destruction Options
- Choosing Services
- Agreements
- Duress Alarms
- Intrusion Detection Systems
- Purpose
- Planning
- Elements
- Procedures
- Sample Physical Security Policy
- Summary

RISK ANALYSIS AND RISK MANAGEMENT

- Introduction
- Frequently Asked Questions on Risk Analysis
- Why Conduct a Risk Analysis?
- When to Conduct a Risk Analysis?
- Who Should Conduct the Risk Analysis?
- How Long Should A Risk Analysis Take?
- What a Risk Analysis Analyzes

BUY ONLINE FROM: <http://www.27001.com/products/76>

What Can the Results of a Risk Analysis Tell an Organization?
Who Should Review the Results of a Risk Analysis?
How Is the Success of the Risk Analysis Measured?
Information Security Life Cycle
Risk Analysis Process
Asset Definition
Threat Identification
Determine Probability of Occurrence
Determine the Impact of the Threat
Controls Recommended
Documentation
Risk Mitigation
Control Categories
Cost/Benefit Analysis
Summary

BUSINESS CONTINUITY PLANNING

Overview
Business Continuity Planning Policy
Policy Statement
Scope
Responsibilities
Compliance
Conducting a Business Impact Analysis (BIA)
Identify Sponsor(s)
Scope
Information Meeting
Information Gathering
Questionnaire Design
Scheduling the Interviews
Conducting Interviews
Tabulating the Information
Presenting the Results
Preventive Controls
Recovery Strategies
Hot Site, Cold Site, Warm Site, Mobile Site
Key Considerations
People
Communications
Computing Equipment
Facilities
Plan Construction, Testing, And Maintenance
Plan Construction
Crisis Management Plan
Plan Distribution
Plan Testing
Line Testing
Walk-Through Testing
Single Process Testing
Full Testing
Plan Testing Summary

BUY ONLINE FROM: <http://www.27001.com/products/76>

Plan Maintenance
Sample Business Continuity Plan Policy
Summary

Glossary

Bibliography

Index

BUY ONLINE FROM: <http://www.27001.com/products/76>