

# **INFORMATION SECURITY POLICIES AND PROCEDURES: A PRACTITIONER'S REFERENCE, SECOND EDITION**

## **INFORMATION SECURITY POLICIES AND PROCEDURES**

Introduction  
Corporate Policies  
Organizationwide (Tier 1) Policies  
Organizationwide Policy Document  
Legal Requirements  
Duty of Loyalty  
Duty of Care  
Other Laws and Regulations  
Business Requirements  
Where to Begin?  
Summary

### **Why Manage This Process as a Project?**

Introduction  
First Things First: Identify the Sponsor  
Defining the Scope of Work  
Time Management  
Cost Management  
Planning for Quality  
Managing Human Resources  
Creating a Communications Plan  
Summary

### **Planning and Preparation**

Introduction  
Objectives of Policies, Standards, and Procedures  
Employee Benefits  
Preparation Activities  
Core and Support Teams  
Focus Groups  
What to Look for in a Good Writer and Editor  
Development Responsibilities  
Other Considerations  
Key Factors in Establishing the Development Cost  
Reference Works  
Milestones  
Responsibilities  
Development Checklist  
Summary

### **Developing Policies**

Policy Is the Cornerstone  
Why Implement Information Security Policy?  
Some Major Points for Establishing Policies  
What Is a Policy?  
Definitions

**BUY ONLINE FROM:** <http://www.27001.com/products/77>

Policy Key Elements  
Policy Format  
Additional Hints  
Pitfalls to Avoid  
Summary

### **Asset Classification Policy**

Introduction  
Overview  
Why Classify Information?  
What Is Information Classification?  
Where to Begin?  
Resist the Urge to Add Categories  
What Constitutes Confidential Information?  
Employee Responsibilities  
Classification Examples  
Declassification or Reclassification of Information  
Records Management Policy  
Information Handling Standards Matrix  
Information Classification Methodology  
Authorization for Access  
Summary

### **Developing Standards**

Introduction  
Overview  
Where Do Standards Belong?  
What Does a Standard Look Like?  
Where Do I Get the Standards?  
Sample Information Security Manual  
Summary

### **Developing Procedures**

Introduction  
Overview  
Important Procedure Requirements  
Key Elements in Procedure Writing  
Procedure Checklist  
Getting Started  
Procedure Styles  
Procedure Development Review  
Observations  
Summary

## **Creating a Table of**

Introduction  
Document Layout  
Document Framework  
Preparing a Draft Table of  
Sections to Consider  
Summary

## **Understanding How to Sell Policies, Standards, and Procedures**

Introduction  
Believe in What You Are Doing  
Return on Investment for Security Functions  
Effective Communication  
Keeping Management Interested in Security  
Why Policies, Standards, and Procedures Are Needed  
The Need for Controls  
Where to Begin?  
Summary

## **Appendix 1A Typical Tier 1 Policies**

Introduction  
Tier 1 Policies  
Employee Standards of Conduct  
Conflict of Interest  
Employment Practices  
Records Management  
Corporate Communications  
Electronic Communications  
Internet Security  
Internet Usage and Responsibility Statement  
Employee Discipline  
General Security  
Business Continuity Planning  
Information Protection  
Information Classification

## **Appendix 1B Typical Tier 2 Policies**

Introduction  
Electronic Communications  
Internet Security  
Internet Usage and Responsibility Statement  
Computer and Network Management  
Anti-Virus Policy  
Computer and Network Management  
Personnel Security  
Systems Development and Maintenance Policy  
Application Access Control Policy  
Data and Software Exchange Policy  
Network Access Control

Network Management Policy  
Information Systems' Operations Policy  
Physical and Environmental Security  
User Access Policy  
Employment Agreement

### **Appendix 1C Sample Standards Manual**

Introduction  
The Company Information Security Standards Manual  
Table of  
Preface  
Corporate Information Security Policy  
Responsibilities  
Standards

### **Appendix 1D Sample Information Security Manual**

The Company Information Security Policy Manual  
General  
What Are We Protecting?  
User Responsibilities  
Access Control Policy  
Penalty for Security Violation  
Security Incident Handling Procedures  
Virus and Worm Incidents  
Malicious Hacker Incidents

### **INFORMATION SECURITY REFERENCE GUIDE**

Introduction to Information Security  
Definition of Information  
What is Information Security?  
Why Do We Need To Protect Information?  
What Information Should Be Protected?

### **Fundamentals of Information Security**

Introduction  
Information Availability (Business Continuity)  
Information Integrity  
Information Confidentiality

### **Employee Responsibilities**

Introduction  
Owner  
Custodian  
User

## **Information Classification**

Introduction  
Classification Process  
Reclassification

## **Information Handling**

Introduction  
Information Labeling  
Information Use and Duplication  
Information Storage  
Information Disposal

## **Tools of Information Security**

Introduction  
Access Authorization  
Access Control  
Backup and Recovery  
Awareness

## **Information Processing**

General  
Right to Review  
Desktop Processing  
Training  
Physical Security  
Proprietary Software - Controls and Security  
Software Code of Ethics  
Computer Virus Security  
Office Automation

## **Information Security Program Administration**

Introduction  
Corporate Information Systems Steering Committee  
Corporate Information Security Program  
Organization Information Security Program

## **Baseline Organization Information Security Program**

Introduction  
Pre-Program Development  
Program Development Phase  
Program Implementation Phase  
Program Maintenance Phase

## **Appendix 2A**

Information Handling Procedures Matrix

Glossary

Information Identification Worksheet

Information Risk Assessment Worksheet

Summary and Controls Worksheet

Risk Assessment: Self-assessment Questionnaire