



SECURITY PROGRAM AND POLICIES

PRINCIPLES AND PRACTICES

SARI STERN GREENE

Security Program and Policies: Principles and Practices

Second Edition

Sari Stern Greene

PEARSON
IT CERTIFICATION

800 East 96th Street, Indianapolis, Indiana 46240 USA

Security Program and Policies: Principles and Practices

Table of Contents

Table of Contents

Chapter 1: Understanding Policy

Looking at Policy Through the Ages

The Bible as Ancient Policy

The United States Constitution as a Policy Revolution

Policy Today

Information Security Policy

Successful Policy Characteristics

The Role of Government

Information Security Policy Lifecycle

Policy Development

Policy Publication

Policy Adoption

Policy Review

Test Your Skills

Chapter 2: Policy Elements and Style

Policy Hierarchy

Standards

Baselines

Guidelines

Procedures

Plans and Programs

Policy Format

Table of Contents

Policy Audience

Policy Format Types

Policy Components

Writing Style and Technique

Using Plain Language

The Plain Language Movement

Plain Language Techniques for Policy Writing

Test Your Skills

Chapter 3: Information Security Framework

CIA

What Is Confidentiality?

What Is Integrity?

What Is Availability?

Who Is Responsible for CIA?

Information Security Framework

What Is NISTs Function?

What Does the ISO Do?

Can the ISO Standards and NIST Publications Be Used to Build a Framework?

Test Your Skills

Chapter 4: Governance and Risk Management

Understanding Information Security Policies

What Is Meant by Strategic Alignment?

Regulatory Requirements

User Versions of Information Security Policies

Vendor Versions of Information Security Policies

Client Synopsis of Information Security Policies

Who Authorizes Information Security Policy?

Revising Information Security Policies: Change Drivers

Table of Contents

Evaluating Information Security Policies

Information Security Governance

What Is a Distributed Governance Model?

Regulatory Requirements

Information Security Risk

Is Risk Bad?

Risk Appetite and Tolerance

What Is a Risk Assessment?

Risk Assessment Methodologies

What Is Risk Management?

Test Your Skills

Chapter 5: Asset Management

Information Assets and Systems

Who Is Responsible for Information Assets?

Information Classification

How Does the Federal Government Classify Data?

Why Is National Security Information Classified Differently?

Who Decides How National Security Data Is Classified?

How Does the Private Sector Classify Data?

Can Information Be Reclassified or Even Declassified?

Labeling and Handling Standards

Why Label?

Why Handling Standards?

Information Systems Inventory

What Should Be Inventoried?

Test Your Skills

Chapter 6: Human Resources Security

The Employee Lifecycle

Table of Contents

What Does Recruitment Have to Do with Security?

What Happens in the Onboarding Phase?

What Is User Provisioning?

What Should an Employee Learn During Orientation?

Why Is Termination Considered the Most Dangerous Phase?

The Importance of Employee Agreements

What Are Confidentiality or Non-disclosure Agreements?

What Is an Acceptable Use Agreement?

The Importance of Security Education and Training

What Is the SETA Model?

Test Your Skills

Chapter 7: Physical and Environmental Security

Understanding the Secure Facility Layered Defense Model

How Do We Secure the Site?

How Is Physical Access Controlled?

Protecting Equipment

No Power, No Processing?

How Dangerous Is Fire?

What About Disposal?

Stop, Thief!

Test Your Skills

Chapter 8: Communications and Operations Security

Standard Operating Procedures (SOPs)

Why Document SOPs?

Developing SOPs

Operational Change Control

Why Manage Change?

Why Is Patching Handled Differently?

Table of Contents

Malware Protection

Are There Different Types of Malware?

How Is Malware Controlled?

What Is Antivirus Software?

Data Replication

Is There a Recommended Backup or Replication Strategy?

Secure Messaging

What Makes Email a Security Risk?

Are Email Servers at Risk?

Activity Monitoring and Log Analysis

What Is Log Management?

Service Provider Oversight

What Is Due Diligence?

What Should Be Included in Service Provider Contracts?

Test Your Skills

Chapter 9: Access Control Management

Access Control Fundamentals

What Is a Security Posture?

How Is Identity Verified?

What Is Authorization?

Infrastructure Access Controls

Why Segment a Network?

What Is Layered Border Security?

Remote Access Security

User Access Controls

Why Manage User Access?

What Types of Access Should Be Monitored?

Test Your Skills

Table of Contents

Chapter 10: Information Systems Acquisition, Development, and Maintenance

System Security Requirements

Secure Code

Cryptography

Test Your Skills

Chapter 11: Information Security Incident Management

Organizational Incident Response

What Is an Incident?

How Are Incidents Reported?

What Is an Incident Response Program?

What Happened? Investigation and Evidence Handling

Data Breach Notification Requirements

Is There a Federal Breach Notification Law?

Does Notification Work?

Test Your Skills

Chapter 12: Business Continuity Management

Emergency Preparedness

What Is a Resilient Organization?

Business Continuity Risk Management

What Is a Business Continuity Threat Assessment?

What Is a Business Continuity Risk Assessment?

What Is a Business Impact Assessment?

The Business Continuity Plan

Roles and Responsibilities

Disaster Response Plans

Operational Contingency Plans

The Disaster Recovery Phase

Table of Contents

The Resumption Phase

Plan Testing and Maintenance

Why Is Testing Important?

Plan Maintenance

Test Your Skills

Chapter 13: Regulatory Compliance for Financial Institutions

The Gramm-Leach-Bliley Act (GLBA)

What Is a Financial Institution?

What Are the Interagency Guidelines?

What Is a Regulatory Examination?

Personal and Corporate Identity Theft

What Is Required by the Interagency Guidelines Supplement A?

What Is Required by the Supplement to the Authentication in an
Internet Banking Environment Guidance?

Test Your Skills

Chapter 14: Regulatory Compliance for the Healthcare Sector

The HIPAA Security Rule

What Is the Objective of the HIPAA Security Rule?

Enforcement and Compliance

How Is the HIPAA Security Rule Organized?

What Are the Physical Safeguards?

What Are the Technical Safeguards?

What Are the Organizational Requirements?

What Are the Policies and Procedures Standards?

The HITECH Act and the Omnibus Rule

What Changed for Business Associates?

What Are the Breach Notification Requirements?

Test Your Skills

Table of Contents

Chapter 15: PCI Compliance for Merchants

Protecting Cardholder Data

What Is the PCI DDS Framework?

Business-as-Usual Approach

What Are the PCI Requirements?

PCI Compliance

Who Is Required to Comply with PCI DSS?

What Is a Data Security Compliance Assessment?

What Is the SAQ?

Are There Penalties for Noncompliance?

Test Your Skills

Appendix A: Information Security Program Resources

National Institute of Standards and Technology (NIST) Special
Publications

Federal Financial Institutions Examination Council (FFIEC) IT
Handbooks

Department of Health and Human Services HIPAA Security Series

Payment Security Standards Council Documents Library

Information Security Professional Development and Certification
Organizations

Appendix B: Sample Information Security Policy

Appendix C: Information Systems Acceptable Use Agreement and Policy

Index