Security Policy Guidelines

CSH6 Chapter 44

"Security Policy Guidelines"

M. E. Kabay & Bridgett Robertson

Selected Topics in CSH6 Ch 44

- Terminology
- Resources for Policy Writers
- Writing the Policies
- Organizing the Policies
- Presenting the Policies
- Maintaining the Policies

Terminology

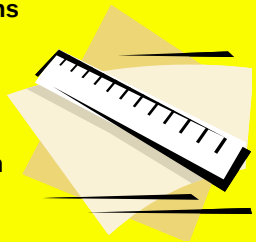
- Policy
- Controls
- Standards
- Procedures

Terminology (1)

- Policy
  - Rules and regulations set by the organization
  - Laid down by management
  - Mandatory, require compliance
  - Failure to follow policy results in disciplinary action
  - Policies focus on desired results, not on means for achieving them
- Controls – measures used to protect systems against specific threats

Terminology (2)

- Standards
  - Accepted specification for hardware, software, or human actions
  - *De facto* or *de jure*
  - Technical choices for implementing particular policies
  - Change more rapidly than policies
- Procedures
  - Prescribe how people are to behave in implementation policies



Resources for Policy Writers

- ISO/IEC 27000
- COBIT
- Informal Security Standards
  - CERT-CC® Documentation
  - NSA Security Guidelines
  - US Federal Best Security Practices
  - RFC 2196
  - German Federal IT Baseline Protection Manual
- Commercially Available Policy Guides

ISO 27000 (1)

- History
  - BS7799:
    - ✓UK Dept. of Trade and Industry Feb 1995
    - ✓Proprietary and expensive
  - BS7799 v2: May 1999
- ISO 17799 built on BS7799 – published 1999
- ISO 17799:2005 revised & published 2005 (duhhh)
- ISO/IEC 27000 replaced 17799:2005 in 2009
  - Popular worldwide
  - Costs of individual components ~100CHF (~€82, U$109)
  - Overview 27000 available free < http://tinyurl.com/ye3rwro >

ISO 27000 (2)

Control objectives & controls for information security management

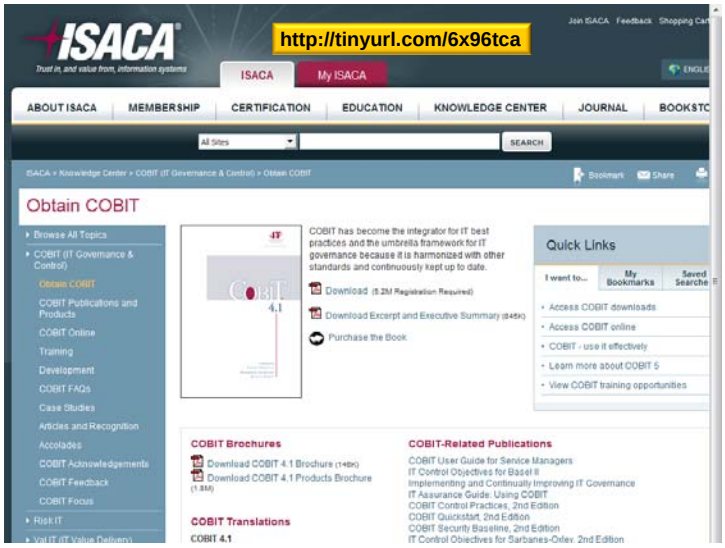
- ISO/IEC 27000 — Overview and Vocabulary
- ISO/IEC 27001 — Requirements
- ISO/IEC 27002 — Code of Practice
- ISO/IEC 27003 — Implementation Guidance
- ISO/IEC 27004 — Measurement
- ISO/IEC 27005 — Risk Management
- ISO/IEC 27006 — Certification Body Requirements
- ISO/IEC 27007 — Audit Guidelines
- ISO/IEC 27011 — Telecommunications Organizations
- ISO 27799 — Health Organizations

COBIT (1)

- Control Objectives for Information and Related Technology (ISACA)
- Business-oriented set of standards for guiding management in sound use of IT
- COBIT Overview
  - Executive summary
  - Framework
    - ✓IT objectives
    - ✓Control functions in IT
  - Business requirements for information

COBIT (2)

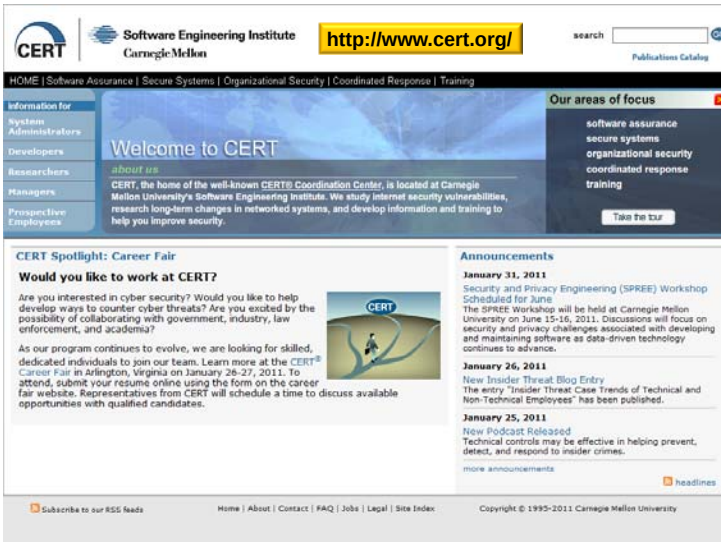
- Control objectives
  - Planning and organization
  - Acquisition and implementation
  - Delivery and support
  - Monitoring
- Audit guidelines
- Implementation tool set
  - Executive overview
  - Guide to implementation
  - Case studies describing COBIT implementation
  - FAQs
  - Slide presentations for implementing/selling COBIT
- Management guidelines



CERT/CC® Documentation

Computer Emergency Response Team Coordination Center® of the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, PA

- Security for IT
- Service contracts
- Securing desktop workstations
- Responding to intrusions
- Securing network servers
- Deploying firewalls
- Securing public Web servers
- Detecting signs of intrusion



US Government Documents

- NIST Special Publications
  - http://csrc.nist.gov/publications/PubsSPs.html
  - Or http://tinyurl.com/23jst6
- NSA *Security Guidelines Handbook*
  - http://www.tscm.com/NSAsecmanual1.html
  - Or http://tinyurl.com/6g3g2ch
  - Initial security responsibilities
  - General responsibilities
  - Helpful information
- Federal Information Processing Standards (FIPS)
  - http://www.itl.nist.gov/fipspubs/index.htm
  - Or http://tinyurl.com/agmwvl

US Federal Best Security Practices (1)

- Federal Chief Information Security Officers (CISO) Council
  - Best Practices Committee (BPC)
  - Sharing best ideas/practical experiences
- Many useful PDF documents available free; e.g.,
  - Best Practices
  - Enterprise Architecture
  - IT Security/Privacy
  - GAO (Government Accountability Office) Reports
  - IT Related Laws & Regulations

US Federal Best Security Practices (2)

http://www.cio.gov/

RFC 2196 – from IETF (1)

- Classic document (1997)
  - Replaced RFC 1244 (1991)
  - Still useful!
  - *IETF: Internet Engineering Task Force*
- Introduction
- Security Policies
- Architecture
- Security services and procedures
  - Security incident handling
  - Ongoing activities
  - Tools and locations
  - Mailing lists and other resources
  - References

http://www.ietf.org/rfc.html

[RFC Index | Usenet FAQs | Web FAQs | Documents | Cities]

Alternate Formats: rfc2196.txt.pdf

Comment on RFC 2196

RFC 2196 - Site Security Handbook

Search the Archives | **Display RFC by number**

Search RFCs | Display RFC By Number

RFC2196 - Site Security Handbook

http://datatracker.ietf.org/doc/rfc2196/

```
Network Working Group                                        B. Fraser
Request for Comments: 2196                                      Editor
FYI: 8                                                        SEI/CMU
Obsoletes: 1244                                          September 1997
Category: Informational

                        Site Security Handbook
```

RFC 2196 (3)


```
                        Site Security Handbook
```


http://www.faqs.org/rfcs/rfc2196.html
Also avail in PDF & plain text

```
Status of this Memo

   This memo provides information for the Internet community.  It does
   not specify an Internet standard of any kind.  Distribution of this
   memo is unlimited.

Abstract

   This handbook is a guide to developing computer security policies and
   procedures for sites that have systems on the Internet.  The purpose
   of this handbook is to provide practical guidance to administrators
   trying to secure their information and services.  The subjects
   covered include policy content and formation, a broad range of
   technical system and network security topics, and security incident
   response.
```

IT Baseline Protection Manual (1)

German Information Security Agency

English version updated 2005

- **Stand-alone systems**
- **Networked systems**
- **Communications**
- **Infrastructure**
- **Methodologies**

Bundesamt für Sicherheit in der Informationstechnik

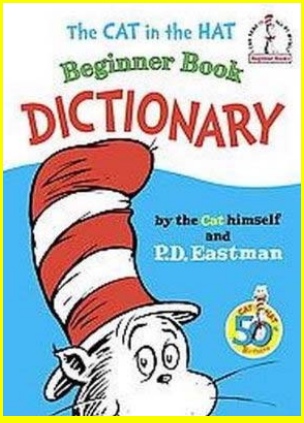
Federal Office for Information Security

IT Baseline Protection Manual (2)

http://tinyurl.com/6kyorl5

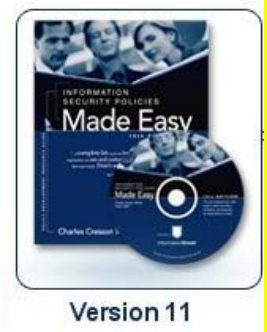
Commercially Available Policy Guides

- **ISPME**
- **Tom Peltier's Text**
- **SANS Resources**



ISPME (Charles Cresson Wood)

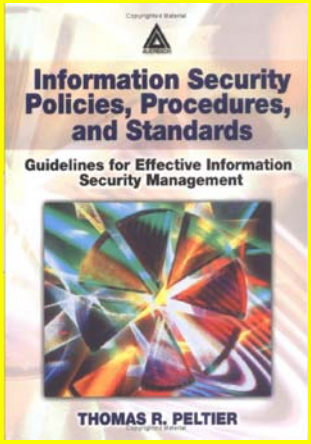
- http://www.informationshield.com/ispmemain.htm
- **Best in the field**
- **$800 and worth every penny**
- **Given to every graduating MSIA student in 2004* at Norwich University as graduation gift!**



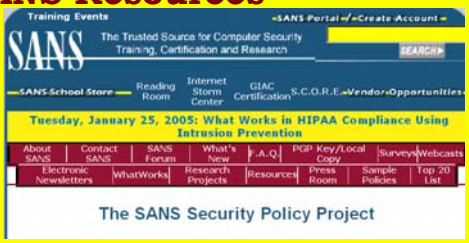
* First year that MSIA students graduated

Tom Peltier's Text

- Useful
- Inexpensive
- Well-respected industry expert
- Professor in NU MSIA



SANS Resources



- http://www.sans.org
- Security Essentials courses
- Step-by-step guides
- SANS Security Policy Project (free)
  - http://www.sans.org/resources/policies/
  - Collaborative compilation of policies

Policy Style

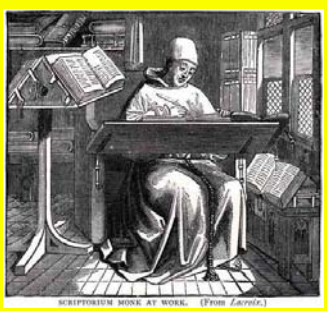
- Why Does Style Matter?
- Writing the Policies
- Organizing the Policies
- Presenting the Policies
- Maintaining the Policies

Why Does Style Matter?

CLASS DISCUSSION

Writing the Policies

- Orientation: *prescriptive* and *proscriptive*
  - Clear, definite, unambiguous
- Writing style
  - Short, simple declarative sentences
- Reasons
  - Explain why policies make sense
  - Optional explanations
- Indexing
  - Many different ways of locating specific policies



Organizing the Policies

- Topical organization
  - Sequence corresponding to model of perception of security; e.g., outside-in
- Organizational
  - Create special-purpose documents aimed at particular groups
- Hierarchical
  - Learn from military standards
  - Increasing detail at lower levels

Presenting the Policies

- Printed text
  - Huge loose-leaf binders; or
  - Short paper documents; or
  - Reference cards, summary sheets, stickers, posters
  - Updating a headache
- Electronic one-dimensional text
  - E-mail updated versions periodically
- Hypertext
  - HTML and XML
  - RTF and word processor files
  - PDF, help files

Maintaining the Policies

- Review process
  - Employees suggest improvement
  - Committees update policy
- Announcing changes
  - Circulate drafts for input – sense of policy ownership for employees
  - Major changes announced by high-level staff with explanations
  - Distribute changes automatically through electronic access

Review Questions

1. Distinguish among *policies*, *controls*, *standards*, *procedures* and give an example of each.
2. What are the advantages and disadvantages of using *industry-standard guidelines* such as CobiT or RFCs in creating policies?
3. Why is the *writing-style* of policies important for effectiveness?
4. Why can it be useful to give *reasons* for policies?
5. What are the benefits and costs of providing *different views* of policy for different sectors of the organization?
6. What are the pros and cons of *electronic* vs *paper* distribution of policies?
7. *Who* should be involved in *reviewing* and *modifying* policies and policy documents? *Why?*

Now go and study