ISO 17799 Information

Code of Practice for Information Security Management

Overview information

ISO 17799 is a security standard written for a non-technical/senior management audience. Sometimes the name of the standard is written out more completely as: ISO/IEC 17799:2000. The sponsoring body is the International Organization for Standardization, which has this home page: www.iso.org

The publication of the ISO 17799 standard carries a date of September, 2001. Unlike several other more detailed IT security codes/standards/regulations reviewed by Unbeaten Path, this standards document is not available for the price of a google.com search. The 71 page document is available for sale from a variety of suppliers who also sell advice or implementation help. It's also sold directly from the ISO web site: **take-a-look.** *(The document is not for sale from Unbeaten Path.)*

Outline of contents

ISO 17799 is organized into these ten major sections.

1. Business continuity planning to manage business interruptions
2. System access control to prevent unauthorized access to information systems
3. System development and maintenance to maintain the security, authenticity, confidentiality and integrity of application system software and associated data
4. Physical and environmental security to prevent compromise or theft of information gained by unauthorized access to business premises
5. Compliance with obligations (e.g. statues, regulations, and contracts)
6. Employee training to sensitize staff to information security issues.
7. Advice to senior executives about how to manage information security
8. Computer and operations management to protect the integrity of and sustain the availability of information
9. Classification and control of corporate physical and information assets
10. Security policy making

Before you get out your credit card to buy ISO 17799, be advised that even the "details" provide no detailed or specific guidance on how to achieve the stated objectives.

Return to IT Security Assurance page