

Overview of *ISO-17799* Code of Practice for Information Security Management ¹

ISO 17799 is an emerging international standard for managing information security. With roots in Australian information security standards and British Standard 7799, ISO 17799 is the first acknowledged world-wide standard to identify a “Code of Practice” for the management of information Security.

ISO 17799 defines *Information Security* as encompassing the following three objectives:

- Confidentiality—Ensuring that information is accessible only to those authorized to have access
- Integrity—Safeguarding the accuracy and completeness of information and processing methods
- Availability—Ensuring that authorized users have access to information and associated assets when required

ISO 17799 identifies 10 specific vital *Information Security Management Practices*. An organization’s information is secure only to the extent that these 10 practices are being *systematically* managed. Weaknesses in any single practice can often negate the combined strength in the other nine.

The 10 *Information Security Management Practices* are:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

¹ *Information Technology—Code of Practice for Information Security Management*, International Standards Organization, ISO-17799, 2000

Brief descriptions of these practices follows:

Security Policy (17799, Section 3)

Objective: To provide management direction and support for information security.

Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Organizational Security (17799, Section 4)

Objective: To manage information security within the organization.

A management framework should be established to initiate and control the implementation of information security within the organization.

Suitable management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management.

Asset Classification and Control (17799, Section 5)

Objective: To maintain appropriate protection of organizational assets.

All major information assets should be accounted for and have a nominated owner.

Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

Personnel Security (17799, Section 6)

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.

Potential recruits should be adequately screened, especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) agreement.

Physical and Environmental Security (17799, Section 7)

Objective: To prevent unauthorized access, damage and interference to business premises and information.

Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

Communications and Operations Management (17799, Section 8)

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures.

Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

Access Control (17799, Section 9)

Objective: To control access to information.

Access to information, and business processes should be controlled on the basis of business and security requirements.

This should take account of policies for information dissemination and authorization.

Systems Development and Maintenance (17799, Section 10)

Objective: To ensure that security is built into information systems.

This will include infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems.

All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

Business Continuity Management (17799, Section 11)

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls..

The consequences of disasters, security failures and loss of service should be analyzed.

Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and practiced to become an integral part of all other management processes.

Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

Compliance (17799, Section 12)

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory or Contractual obligations and of any security requirements.

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.

Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (i.e. trans-border data flow).



Citadel Information Group ... Securing the Critical Information Assets of Middle Market Businesses, Mid-Sized Government Agencies, and the Not-for-Profit Community

To schedule a free no-obligation *Information Security Executive Briefing* or for additional information, please contact:

Stan Stahl, Ph.D.
Kimberly Pease

323.876.1441
323.397.5752

sstahl@citadel-information.com
kpease@citadel-information.com