
Information technology — Code of practice for information security management

*Technologies de l'information — Code de pratique pour la gestion de
sécurité d'information*

Reference number
ISO/IEC 17799:2000(E)



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2000

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

FOREWORD	VII
INTRODUCTION.....	VIII
WHAT IS INFORMATION SECURITY?.....	VIII
WHY INFORMATION SECURITY IS NEEDED.....	VIII
HOW TO ESTABLISH SECURITY REQUIREMENTS.....	IX
ASSESSING SECURITY RISKS	IX
SELECTING CONTROLS.....	X
INFORMATION SECURITY STARTING POINT	X
CRITICAL SUCCESS FACTORS.....	X
DEVELOPING YOUR OWN GUIDELINES.....	XI
1 SCOPE.....	1
2 TERMS AND DEFINITIONS.....	1
3 SECURITY POLICY	1
3.1 INFORMATION SECURITY POLICY.....	1
3.1.1 Information security policy document	1
3.1.2 Review and evaluation.....	2
4 ORGANIZATIONAL SECURITY.....	2
4.1 INFORMATION SECURITY INFRASTRUCTURE	2
4.1.1 Management information security forum.....	3
4.1.2 Information security co-ordination.....	3
4.1.3 Allocation of information security responsibilities.....	3
4.1.4 Authorization process for information processing facilities.....	4
4.1.5 Specialist information security advice.....	4
4.1.6 Co-operation between organizations.....	5
4.1.7 Independent review of information security	5
4.2 SECURITY OF THIRD PARTY ACCESS	5
4.2.1 Identification of risks from third party access	5
4.2.2 Security requirements in third party contracts	6
4.3 OUTSOURCING.....	7
4.3.1 Security requirements in outsourcing contracts	7
5 ASSET CLASSIFICATION AND CONTROL.....	8
5.1 ACCOUNTABILITY FOR ASSETS.....	8
5.1.1 Inventory of assets.....	8
5.2 INFORMATION CLASSIFICATION.....	9
5.2.1 Classification guidelines.....	9
5.2.2 Information labelling and handling.....	9
6 PERSONNEL SECURITY	10
6.1 SECURITY IN JOB DEFINITION AND RESOURCING.....	10
6.1.1 Including security in job responsibilities.....	10
6.1.2 Personnel screening and policy.....	10
6.1.3 Confidentiality agreements.....	11
6.1.4 Terms and conditions of employment	11
6.2 USER TRAINING.....	11
6.2.1 Information security education and training.....	11
6.3 RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS.....	12
6.3.1 Reporting security incidents.....	12
6.3.2 Reporting security weaknesses	12
6.3.3 Reporting software malfunctions.....	12
6.3.4 Learning from incidents.....	13

6.3.5	Disciplinary process.....	13
7	PHYSICAL AND ENVIRONMENTAL SECURITY	13
7.1	SECURE AREAS.....	13
7.1.1	Physical security perimeter.....	13
7.1.2	Physical entry controls.....	14
7.1.3	Securing offices, rooms and facilities.....	14
7.1.4	Working in secure areas.....	15
7.1.5	Isolated delivery and loading areas.....	15
7.2	EQUIPMENT SECURITY.....	16
7.2.1	Equipment siting and protection.....	16
7.2.2	Power supplies.....	17
7.2.3	Cabling security.....	17
7.2.4	Equipment maintenance.....	17
7.2.5	Security of equipment off-premises	18
7.2.6	Secure disposal or re-use of equipment	18
7.3	GENERAL CONTROLS.....	18
7.3.1	Clear desk and clear screen policy.....	19
7.3.2	Removal of property	19
8	COMMUNICATIONS AND OPERATIONS MANAGEMENT	19
8.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES.....	19
8.1.1	Documented operating procedures.....	19
8.1.2	Operational change control.....	20
8.1.3	Incident management procedures	20
8.1.4	Segregation of duties.....	21
8.1.5	Separation of development and operational facilities.....	22
8.1.6	External facilities management.....	22
8.2	SYSTEM PLANNING AND ACCEPTANCE.....	23
8.2.1	Capacity planning.....	23
8.2.2	System acceptance.....	23
8.3	PROTECTION AGAINST MALICIOUS SOFTWARE.....	24
8.3.1	Controls against malicious software	24
8.4	HOUSEKEEPING.....	25
8.4.1	Information back-up	25
8.4.2	Operator logs.....	25
8.4.3	Fault logging.....	25
8.5	NETWORK MANAGEMENT	26
8.5.1	Network controls.....	26
8.6	MEDIA HANDLING AND SECURITY.....	26
8.6.1	Management of removable computer media.....	26
8.6.2	Disposal of media.....	27
8.6.3	Information handling procedures.....	27
8.6.4	Security of system documentation	28
8.7	EXCHANGES OF INFORMATION AND SOFTWARE.....	28
8.7.1	Information and software exchange agreements.....	28
8.7.2	Security of media in transit.....	29
8.7.3	Electronic commerce security.....	29
8.7.4	Security of electronic mail.....	30
8.7.5	Security of electronic office systems	31
8.7.6	Publicly available systems.....	31
8.7.7	Other forms of information exchange.....	32
9	ACCESS CONTROL.....	33
9.1	BUSINESS REQUIREMENT FOR ACCESS CONTROL	33
9.1.1	Access control policy.....	33
9.2	USER ACCESS MANAGEMENT	34
9.2.1	User registration.....	34
9.2.2	Privilege management.....	34
9.2.3	User password management	35

9.2.4	Review of user access rights.....	35
9.3	USER RESPONSIBILITIES.....	36
9.3.1	Password use	36
9.3.2	Unattended user equipment.....	36
9.4	NETWORK ACCESS CONTROL.....	37
9.4.1	Policy on use of network services.....	37
9.4.2	Enforced path.....	37
9.4.3	User authentication for external connections.....	38
9.4.4	Node authentication.....	38
9.4.5	Remote diagnostic port protection.....	38
9.4.6	Segregation in networks.....	39
9.4.7	Network connection control.....	39
9.4.8	Network routing control.....	39
9.4.9	Security of network services.....	40
9.5	OPERATING SYSTEM ACCESS CONTROL	40
9.5.1	Automatic terminal identification.....	40
9.5.2	Terminal log-on procedures.....	40
9.5.3	User identification and authentication	41
9.5.4	Password management system.....	41
9.5.5	Use of system utilities.....	42
9.5.6	Duress alarm to safeguard users.....	42
9.5.7	Terminal time-out.....	42
9.5.8	Limitation of connection time.....	42
9.6	APPLICATION ACCESS CONTROL.....	43
9.6.1	Information access restriction.....	43
9.6.2	Sensitive system isolation.....	43
9.7	MONITORING SYSTEM ACCESS AND USE.....	44
9.7.1	Event logging	44
9.7.2	Monitoring system use.....	44
9.7.3	Clock synchronization.....	45
9.8	MOBILE COMPUTING AND TELEWORKING.....	46
9.8.1	Mobile computing.....	46
9.8.2	Teleworking.....	46
10	SYSTEMS DEVELOPMENT AND MAINTENANCE.....	47
10.1	SECURITY REQUIREMENTS OF SYSTEMS	47
10.1.1	Security requirements analysis and specification.....	48
10.2	SECURITY IN APPLICATION SYSTEMS	48
10.2.1	Input data validation.....	48
10.2.2	Control of internal processing.....	49
10.2.3	Message authentication.....	49
10.2.4	Output data validation.....	50
10.3	CRYPTOGRAPHIC CONTROLS.....	50
10.3.1	Policy on the use of cryptographic controls.....	50
10.3.2	Encryption	50
10.3.3	Digital signatures.....	51
10.3.4	Non-repudiation services.....	51
10.3.5	Key management.....	52
10.4	SECURITY OF SYSTEM FILES	53
10.4.1	Control of operational software.....	53
10.4.2	Protection of system test data	53
10.4.3	Access control to program source library.....	54
10.5	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES.....	54
10.5.1	Change control procedures.....	54
10.5.2	Technical review of operating system changes.....	55
10.5.3	Restrictions on changes to software packages.....	55
10.5.4	Covert channels and Trojan code	56
10.5.5	Outsourced software development.....	56
11	BUSINESS CONTINUITY MANAGEMENT	56

11.1	ASPECTS OF BUSINESS CONTINUITY MANAGEMENT.....	56
11.1.1	<i>Business continuity management process.....</i>	57
11.1.2	<i>Business continuity and impact analysis.....</i>	57
11.1.3	<i>Writing and implementing continuity plans.....</i>	57
11.1.4	<i>Business continuity planning framework.....</i>	58
11.1.5	<i>Testing, maintaining and re-assessing business continuity plans.....</i>	59
12	COMPLIANCE	60
12.1	COMPLIANCE WITH LEGAL REQUIREMENTS.....	60
12.1.1	<i>Identification of applicable legislation.....</i>	60
12.1.2	<i>Intellectual property rights (IPR).....</i>	60
12.1.3	<i>Safeguarding of organizational records.....</i>	61
12.1.4	<i>Data protection and privacy of personal information.....</i>	62
12.1.5	<i>Prevention of misuse of information processing facilities.....</i>	62
12.1.6	<i>Regulation of cryptographic controls.....</i>	62
12.1.7	<i>Collection of evidence.....</i>	63
12.2	REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE	63
12.2.1	<i>Compliance with security policy.....</i>	63
12.2.2	<i>Technical compliance checking.....</i>	64
12.3	SYSTEM AUDIT CONSIDERATIONS.....	64
12.3.1	<i>System audit controls.....</i>	64
12.3.2	<i>Protection of system audit tools.....</i>	65

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 17799 was prepared by the British Standards Institution (as BS 7799) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

What is information security?

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

- a) confidentiality: ensuring that information is accessible only to those authorized to have access;
- b) integrity: safeguarding the accuracy and completeness of information and processing methods;
- c) availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Why information security is needed

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image.

Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

Information security controls are considerably cheaper and more effective if incorporated at the requirements specification and design stage.

How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources.

The first source is derived from assessing risks to the organization. Through risk assessment threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

The second source is the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy.

The third source is the particular set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful.

Risk assessment is systematic consideration of:

- a) the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;
- b) the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The results of this assessment will help guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

It is important to carry out periodic reviews of security risks and implemented controls to:

- a) take account of changes to business requirements and priorities;
- b) consider new threats and vulnerabilities;
- c) confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

Selecting controls

Once security requirements have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this document or from other control sets, or new controls can be designed to meet specific needs as appropriate. There are many different ways of managing risks and this document provides examples of common approaches. However, it is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all organizations. As an example, 8.1.4 describes how duties may be segregated to prevent fraud and error. It may not be possible for smaller organizations to segregate all duties and other ways of achieving the same control objective may be necessary. As another example, 9.7 and 12.1 describe how system use can be monitored and evidence collected. The described controls e.g. event logging might conflict with applicable legislation, such as privacy protection for customers or in the workplace.

Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.

Some of the controls in this document can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading “Information security starting point”.

Information security starting point

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security.

Controls considered to be essential to an organization from a legislative point of view include:

- a) data protection and privacy of personal information (see 12.1.4).
- b) safeguarding of organizational records (see 12.1.3);
- c) intellectual property rights (see 12.1.2);

Controls considered to be common best practice for information security include:

- a) information security policy document (see 3.1);
- b) allocation of information security responsibilities (see 4.1.3);
- c) information security education and training (see 6.2.1);
- d) reporting security incidents (see 6.3.1);
- e) business continuity management (see 11.1).

These controls apply to most organizations and in most environments. It should be noted that although all controls in this document are important, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- a) security policy, objectives and activities that reflect business objectives;
- b) an approach to implementing security that is consistent with the organizational culture;
- c) visible support and commitment from management;
- d) a good understanding of the security requirements, risk assessment and risk management;
- e) effective marketing of security to all managers and employees;
- f) distribution of guidance on information security policy and standards to all employees and contractors;
- g) providing appropriate training and education;
- h) a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidance. Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required. When this happens it may be useful to retain cross-references which will facilitate compliance checking by auditors and business partners.

Information technology — Code of practice for information security management

1 Scope

This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.

2 Terms and definitions

For the purposes of this document, the following definitions apply.

2.1 Information security

Preservation of confidentiality, integrity and availability of information.

- **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.

2.2 Risk assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

2.3 Risk management

Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.

3 Security policy

3.1 Information security policy

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.

3.1.1 Information security policy document

A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. As a minimum, the following guidance should be included:

- a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);
- b) a statement of management intent, supporting the goals and principles of information security;
- c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:
 - 1) compliance with legislative and contractual requirements;
 - 2) security education requirements;
 - 3) prevention and detection of viruses and other malicious software;
 - 4) business continuity management;
 - 5) consequences of security policy violations;
- d) a definition of general and specific responsibilities for information security management, including reporting security incidents;
- e) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

3.1.2 Review and evaluation

The policy should have an owner who is responsible for its maintenance and review according to a defined review process. That process should ensure that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure. There should also be scheduled, periodic reviews of the following:

- a) the policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents;
- b) cost and impact of controls on business efficiency;
- c) effects of changes to technology.

4 Organizational security

4.1 Information security infrastructure

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 fora with 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.

4.1.1 Management information security forum

Information security is a business responsibility shared by all members of the management team. A management forum to ensure that there is clear direction and visible management support for security initiatives should therefore be considered. That forum should promote security within the organization through appropriate commitment and adequate resourcing. The forum may be part of an existing management body. Typically, such a forum undertakes the following:

- a) reviewing and approving information security policy and overall responsibilities;
- b) monitoring significant changes in the exposure of information assets to major threats;
- c) reviewing and monitoring information security incidents;
- d) approving major initiatives to enhance information security.

One manager should be responsible for all security related activities.

4.1.2 Information security co-ordination

In a large organization a cross-functional forum of management representatives from relevant parts of the organization may be necessary to co-ordinate the implementation of information security controls. Typically, such a forum:

- a) agrees specific roles and responsibilities for information security across the organization;
- b) agrees specific methodologies and processes for information security, e.g. risk assessment, security classification system;
- c) agrees and supports organization-wide information security initiatives, e.g. security awareness programme;
- d) ensures that security is part of the information planning process;
- e) assesses the adequacy and co-ordinates the implementation of specific information security controls for new systems or services;
- f) reviews information security incidents;
- g) promotes the visibility of business support for information security throughout the organization.

4.1.3 Allocation of information security responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined.

The information security policy (see clause 3) should provide general guidance on the allocation of security roles and responsibilities in the organization. This should be supplemented, where necessary, with more detailed guidance for specific sites, systems or services. Local responsibilities for individual physical and information assets and security processes, such as business continuity planning, should be clearly defined.

In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each information asset who then becomes responsible for its day-to-day security.

Owners of information assets may delegate their security responsibilities to individual managers or service providers. Nevertheless the owner remains ultimately responsible for the security of the asset and should be able to determine that any delegated responsibility has been discharged correctly.

It is essential that the areas for which each manager is responsible are clearly stated; in particular the following should take place.

- a) The various assets and security processes associated with each individual system should be identified and clearly defined.
- b) The manager responsible for each asset or security process should be agreed and the details of this responsibility should be documented.
- c) Authorization levels should be clearly defined and documented.

4.1.4 Authorization process for information processing facilities

A management authorization process for new information processing facilities should be established.

The following controls should be considered.

- a) New facilities should have appropriate user management approval, authorizing their purpose and use. Approval should also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met.
- b) Where necessary, hardware and software should be checked to ensure that they are compatible with other system components.

NOTE Type approval may be required for certain connections.

- c) The use of personal information processing facilities for processing business information and any necessary controls should be authorized.
- d) The use of personal information processing facilities in the workplace may cause new vulnerabilities and should therefore be assessed and authorized.

These controls are especially important in a networked environment.

4.1.5 Specialist information security advice

Specialist security advice is likely to be required by many organizations. Ideally, an experienced in-house information security adviser should provide this. Not all organizations may wish to employ a specialist adviser. In such cases, it is recommended that a specific individual is identified to co-ordinate in-house knowledge and experiences to ensure consistency, and provide help in security decision making. They should also have access to suitable external advisers to provide specialist advice outside their own experience.

Information security advisers or equivalent points of contact should be tasked with providing advice on all aspects of information security, using either their own or external advice. The quality of their assessment of security threats and advice on controls will determine the effectiveness of the organization's information security. For maximum effectiveness and impact they should be allowed direct access to management throughout the organization.

The information security adviser or equivalent point of contact should be consulted at the earliest possible stage following a suspected security incident or breach to provide a source of expert guidance or investigative resources. Although most internal security investigations will

normally be carried out under management control, the information security adviser may be called on to advise, lead or conduct the investigation.

4.1.6 Co-operation between organizations

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators should be maintained to ensure that appropriate action can be quickly taken, and advice obtained, in the event of a security incident. Similarly, membership of security groups and industry forums should be considered.

Exchanges of security information should be restricted to ensure that confidential information of the organization is not passed to unauthorized persons.

4.1.7 Independent review of information security

The information security policy document (see 3.1) sets out the policy and responsibilities for information security. Its implementation should be reviewed independently to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective (see 12.2).

Such a review may be carried out by the internal audit function, an independent manager or a third party organization specialising in such reviews, where these candidates have the appropriate skills and experience.

4.2 Security of third party access

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

Access to the organization's information processing facilities by third parties should be controlled.

Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party.

Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access.

This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

4.2.1 Identification of risks from third party access

4.2.1.1 Types of access

The type of access given to a third party is of special importance. For example, the risks of access across a network connection are different from risks resulting from physical access. Types of access that should be considered are:

- a) physical access, e.g. to offices, computer rooms, filing cabinets;
- b) logical access, e.g. to an organization's databases, information systems.

4.2.1.2 Reasons for access

Third parties may be granted access for a number of reasons. For example, there are third parties that provide services to an organization and are not located on-site but may be given physical and logical access, such as:

- a) hardware and software support staff, who need access to system level or low level application functionality;
- b) trading partners or joint ventures, who may exchange information, access information systems or share databases.

Information might be put at risk by access from third parties with inadequate security management. Where there is a business need to connect to a third party location a risk assessment should be carried out to identify any requirements for specific controls. It should take into account the type of access required, the value of the information, the controls employed by the third party and the implications of this access to the security of the organization's information.

4.2.1.3 On-site contractors

Third parties that are located on-site for a period of time as defined in their contract may also give rise to security weaknesses. Examples of on-site third party include:

- a) hardware and software maintenance and support staff;
- b) cleaning, catering, security guards and other outsourced support services;
- c) student placement and other casual short term appointments;
- d) consultants.

It is essential to understand what controls are needed to administer third party access to information processing facilities. Generally, all security requirements resulting from third party access or internal controls should be reflected by the third party contract (see also 4.2.2). For example, if there is a special need for confidentiality of the information, non-disclosure agreements might be used (see 6.1.3).

Access to information and information processing facilities by third parties should not be provided until the appropriate controls have been implemented and a contract has been signed defining the terms for the connection or access.

4.2.2 Security requirements in third party contracts

Arrangements involving third party access to organizational information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of their supplier. The following terms should be considered for inclusion in the contract:

- a) the general policy on information security;
- b) asset protection, including:
 - 1) procedures to protect organizational assets, including information and software;
 - 2) procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;
 - 3) controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
 - 4) integrity and availability;
 - 5) restrictions on copying and disclosing information;
- c) a description of each service to be made available;
- d) the target level of service and unacceptable levels of service;

- e) provision for the transfer of staff where appropriate;
- f) the respective liabilities of the parties to the agreement;
- g) responsibilities with respect to legal matters, e.g. data protection legislation, especially taking into account different national legal systems if the contract involves co-operation with organizations in other countries (see also 12.1);
- h) intellectual property rights (IPRs) and copyright assignment (see 12.1.2) and protection of any collaborative work (see also 6.1.3);
- i) access control agreements, covering:
 - 1) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
 - 2) an authorization process for user access and privileges;
 - 3) a requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use;
- j) the definition of verifiable performance criteria, their monitoring and reporting;
- k) the right to monitor, and revoke, user activity;
- l) the right to audit contractual responsibilities or to have those audits carried out by a third party;
- m) the establishment of an escalation process for problem resolution; contingency arrangements should also be considered where appropriate;
- n) responsibilities regarding hardware and software installation and maintenance;
- o) a clear reporting structure and agreed reporting formats;
- p) a clear and specified process of change management;
- q) any required physical protection controls and mechanisms to ensure those controls are followed;
- r) user and administrator training in methods, procedures and security;
- s) controls to ensure protection against malicious software (see 8.3);
- t) arrangements for reporting, notification and investigation of security incidents and security breaches;
- u) involvement of the third party with subcontractors.

4.3 Outsourcing

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Outsourcing arrangements should address the risks, security controls and procedures for information systems, networks and/or desk top environments in the contract between the parties.

4.3.1 Security requirements in outsourcing contracts

The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desk top environments should be addressed in a contract agreed between the parties.

For example, the contract should address:

- a) how the legal requirements are to be met, e.g. data protection legislation;

- b) what arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities;
- c) how the integrity and confidentiality of the organization's business assets are to be maintained and tested;
- d) what physical and logical controls will be used to restrict and limit the access to the organization's sensitive business information to authorized users;
- e) how the availability of services is to be maintained in the event of a disaster;
- f) what levels of physical security are to be provided for outsourced equipment;
- g) the right of audit.

The terms given in the list in 4.2.2 should also be considered as part of this contract. The contract should allow the security requirements and procedures to be expanded in a security management plan to be agreed between the two parties.

Although outsourcing contracts can pose some complex security questions, the controls included in this code of practice could serve as a starting point for agreeing the structure and content of the security management plan.

5 Asset classification and control

5.1 Accountability for assets

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.

5.1.1 Inventory of assets

Inventories of assets help ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important aspect of risk management. An organization needs to be able to identify its assets and the relative value and importance of these assets. Based on this information an organization can then provide levels of protection commensurate with the value and importance of the assets. An inventory should be drawn up and maintained of the important assets associated with each information system. Each asset should be clearly identified and its ownership and security classification (see 5.2) agreed and documented, together with its current location (important when attempting to recover from loss or damage). Examples of assets associated with information systems are:

- a) information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
- b) software assets: application software, system software, development tools and utilities;
- c) physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines),

- magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
- d) services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

5.2 Information classification

Objective: To ensure that information assets receive an appropriate level of protection.

Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

5.2.1 Classification guidelines

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorized access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected.

Information and outputs from systems handling classified data should be labelled in terms of its value and sensitivity to the organization. It may also be appropriate to label information in terms of how critical it is to the organization, e.g. in terms of its integrity and availability.

Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to an unnecessary additional business expense. Classification guidelines should anticipate and allow for the fact that the classification of any given item of information is not necessarily fixed for all time, and may change in accordance with some predetermined policy (see 9.1).

Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations which may have different definitions for the same or similarly named labels.

The responsibility for defining the classification of an item of information, e.g. for a document, data record, data file or diskette, and for periodically reviewing that classification, should remain with the originator or nominated owner of the information.

5.2.2 Information labelling and handling

It is important that an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by the organization. These procedures need to cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity:

- a) copying;
- b) storage;
- c) transmission by post, fax, and electronic mail;

- d) transmission by spoken word, including mobile phone, voicemail, answering machines;
- e) destruction.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label (in the output). The labelling should reflect the classification according to the rules established in 5.2.1. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CDs, cassettes), electronic messages and file transfers.

Physical labels are generally the most appropriate forms of labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling need to be used.

6 Personnel security

6.1 Security in job definition and resourcing

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 (see 6.1.2), especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) agreement.

6.1.1 Including security in job responsibilities

Security roles and responsibilities, as laid down in the organization's information security policy (see 3.1) should be documented where appropriate. They should include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

6.1.2 Personnel screening and policy

Verification checks on permanent staff should be carried out at the time of job applications. This should include the following controls:

- a) availability of satisfactory character references, e.g. one business and one personal;
- b) a check (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity check (passport or similar document).

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the organization should also carry out a credit check. For staff holding positions of considerable authority this check should be repeated periodically.

A similar screening process should be carried out for contractors and temporary staff. Where these staff are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern.

Management should evaluate the supervision required for new and inexperienced staff with authorization for access to sensitive systems. The work of all staff should be subject to periodic review and approval procedures by a more senior member of staff.

Managers should be aware that personal circumstances of their staff may affect their work. Personal or financial problems, changes in their behaviour or lifestyle, recurring absences and evidence of stress or depression might lead to fraud, theft, error or other security implications. This information should be handled in accordance with any appropriate legislation existing in the relevant jurisdiction.

6.1.3 Confidentiality agreements

Confidentiality or non-disclosure agreements are used to give notice that information is confidential or secret. Employees should normally sign such an agreement as part of their initial terms and conditions of employment.

Casual staff and third party users not already covered by an existing contract (containing the confidentiality agreement) should be required to sign a confidentiality agreement prior to being given access to information processing facilities.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

6.1.4 Terms and conditions of employment

The terms and conditions of employment should state the employee's responsibility for information security. Where appropriate, these responsibilities should continue for a defined period after the end of the employment. The action to be taken if the employee disregards security requirements should be included.

The employee's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation, should be clarified and included within the terms and conditions of employment. Responsibility for the classification and management of the employer's data should also be included. Whenever appropriate, terms and conditions of employment should state that these responsibilities are extended outside the organization's premises and outside normal working hours, e.g. in the case of home-working (see also 7.2.5 and 9.8.1).

6.2 User training

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

6.2.1 Information security education and training

All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages, before access to information or services is granted.

6.3 Responding to security incidents and malfunctions

Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Incidents affecting security should be reported through appropriate management channels as quickly as possible.

All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organization should establish a formal disciplinary process for dealing with employees who commit security breaches. To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (see 12.1.7).

6.3.1 Reporting security incidents

Security incidents should be reported through appropriate management channels as quickly as possible.

A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. All employees and contractors should be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible. Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training (see 6.2) as examples of what could happen, how to respond to such incidents, and how to avoid them in the future (see also 12.1.7).

6.3.2 Reporting security weaknesses

Users of information services should be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their management or directly to their service provider as quickly as possible. Users should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

6.3.3 Reporting software malfunctions

Procedures should be established for reporting software malfunctions. The following actions should be considered.

- a) The symptoms of the problem and any messages appearing on the screen should be noted.
- b) The computer should be isolated, if possible, and use of it should be stopped. The appropriate contact should be alerted immediately. If equipment is to be examined, it should be disconnected from any organizational networks before being re-powered. Diskettes should not be transferred to other computers.
- c) The matter should be reported immediately to the information security manager.

Users should not attempt to remove the suspected software unless authorized to do so. Appropriately trained and experienced staff should carry out recovery.

6.3.4 *Learning from incidents*

There should be mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process (see 3.1.2).

6.3.5 *Disciplinary process*

There should be a formal disciplinary process for employees who have violated organizational security policies and procedures (see 6.1.4 and, for retention of evidence, see 12.1.7). Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. Additionally, it should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.

7 **Physical and environmental security**

7.1 **Secure areas**

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.

7.1.1 *Physical security perimeter*

Physical protection can be achieved by creating several physical barriers around the business premises and information processing facilities. Each barrier establishes a security perimeter, each increasing the total protection provided. Organizations should use security perimeters to protect areas which contain information processing facilities (see 7.1.3). A security perimeter is something which builds a barrier, e.g. a wall, a card controlled entry gate or a manned reception desk. The siting and strength of each barrier depends on the results of a risk assessment.

The following guidelines and controls should be considered and implemented where appropriate.

- a) The security perimeter should be clearly defined.
- b) The perimeter of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.
- c) A manned reception area or other means to control physical access to the site or building should be in place. Access to sites and buildings should be restricted to authorized personnel only.

- d) Physical barriers should, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding.
- e) All fire doors on a security perimeter should be alarmed and should slam shut.

7.1.2 *Physical entry controls*

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls should be considered.

- a) Visitors to secure areas should be supervised or cleared and their date and time of entry and departure recorded. They should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.
- b) Access to sensitive information, and information processing facilities, should be controlled and restricted to authorized persons only. Authentication controls, e.g. swipe card plus PIN, should be used to authorize and validate all access. An audit trail of all access should be securely maintained.
- c) All personnel should be required to wear some form of visible identification and should be encouraged to challenge unescorted strangers and anyone not wearing visible identification.
- d) Access rights to secure areas should be regularly reviewed and updated.

7.1.3 *Securing offices, rooms and facilities*

A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of a secure area should take account of the possibility of damage from fire, flood, explosion, civil unrest, and other forms of natural or man-made disaster. Account should also be taken of relevant health and safety regulations and standards. Consideration should be given also to any security threats presented by neighbouring premises, e.g. leakage of water from other areas.

The following controls should be considered.

- a) Key facilities should be sited to avoid access by the public.
- b) Buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities.
- c) Support functions and equipment, e.g. photocopiers, fax machines, should be sited appropriately within the secure area to avoid demands for access, which could compromise information.
- d) Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.
- e) Suitable intruder detection systems installed to professional standards and regularly tested should be in place to cover all external doors and accessible windows. Unoccupied areas should be alarmed at all times. Cover should also be provided for other areas, e.g. computer room or communications rooms.
- f) Information processing facilities managed by the organization should be physically separated from those managed by third parties.