The information created, used, stored and transmitted by your organisation forms one of its most important assets. This document shows how you can use good practice to protect this information from being maliciously or unintentionally changed (integrity); make it available when and where needed (availability); and ensure that only those with a legitimate right can access it (confidentiality).

This document should be regarded as a starting point for developing organisation-specific controls and guidance for the classification and protection of information assets. Not all the guidance provided in this document may be applicable to an organisation's specific needs. It is therefore important to understand the organisation's business requirements and to apply this guidance appropriately. The document provides general guidance only and, if fully implemented, can only reduce, not eliminate, your vulnerability.

Organisations which regularly handle UK government protectively-marked information must continue to follow the procedures agreed with the appropriate UK security authorities. However, this guidance has been developed in conjunction with them, and similar security procedures can therefore be applied to commercial and protectively-marked information.

Who this document is for: those responsible for initiating, implementing or maintaining information security in their organisation as well as those who use and process their organisation's information.

What it covers: the issues surrounding your potential vulnerability to the loss and/or damage of your business information.

## 1 EXECUTIVE SUMMARY

This document indicates how you can identify your information assets, and who should have responsibility for them. It also suggests how you can assess the best methods of protecting your identified assets; by considering the threats to them, their vulnerability and the impact that compromise of their confidentiality, integrity or availability might have.

The document goes on to consider the 'classification' of information assets to ensure that appropriate levels of protection are given to them. It considers examples of five levels of confidentiality, from 'publicly available' to 'strictly confidential' and suggests what type of assets might fall into each category. Three categories of integrity classification are considered, with examples. Four levels of classification for availability are suggested, with indications as to the timeframes that might be appropriate to each level (for example 12-48 hours for 'basic' and 2-3 hours for 'high availability').

The practical use of these classifications is considered, particularly in relation to information sharing with partner organisations.

The major part of the document shows how the advice and guidance contained in the international code of practice for information security management (ISO/IEC 17799) can be applied to ensure that appropriate protection is given to the integrity, availability and confidentiality of your information. This section covers handling and storage of information (whether physically or electronically held); backup and disposal of information; sharing information with third parties (including outsourcing arrangements); exchanging information electronically or physically; planning for new systems or upgrades to old; using computer applications; and using mobile phones, laptops and other devices away from the workplace.

The final part of the document indicates how you can integrate information protection into your overall business. It looks at the importance of establishing security awareness and of having appropriate policies, standards and procedures operating within an information security management system, such as that specified within BS 7799-2:2002.

## 2 INTRODUCTION

### 2.1 Need for information protection

In recent years, the proliferation of interconnected information systems and networks has meant that no business can afford to neglect its information security. Organisations can't make assumptions about how their trading partners or a third party will protect their information. This has led international legislators and regulators to emphasise the importance of the development of a ‘culture of security’ within business.

All organisations acquire and generate information that is vital to their operation and growth. Examples include client and supplier records of various kinds and proprietary information relating to products, processes, business performance and planning.

Protection of an organisation's information resources is vital both for the continued health of the business and for compliance with legal, regulatory and contractual demands. For these reasons information is now recognised as a significant business asset that needs to be managed effectively. Therefore, of necessity, organisations require their information assets to be kept confidential where required, made available when needed and protected from damage and destruction, and loss of integrity.

Information assets can be in the form of paper records, electronic media or the intellectual property stored in people's heads. Whatever form an information asset takes a business must consider how best to protect its security.

### 2.2 Best practice

Following the guidance in this brochure should help you to:

- protect your organisation's sensitive and critical information in a consistent and appropriate manner,
- protect information entrusted to you by other organisations.

By doing this, you should:

- reduce the risk and damage to your organisation's reputation, profitability or business interests due to loss of, or harm to, sensitive or critical information,
- reduce the risk of embarrassment or loss of business arising from loss of, or damage to, another organisation's sensitive or critical information,
- increase confidence in trading partnerships and outsourcing arrangements.

The security controls outlined in this document provide best practice advice for information protection. Controls to provide this protection should be selected based on a risk assessment (see Section 4.2).

## 3 DEFINITIONS

For the purposes of this booklet the following definitions apply:

### 3.1 Information Security

Information security involves the preservation of confidentiality, integrity and availability of information (reference ISO/IEC 17799:2000). In general terms this means that information security deals with the maintenance and control of:

- Confidentiality: ensuring the information is accessible only to those authorised to have access,
- Integrity: protecting the accuracy and completeness of information,
- Availability: ensuring that access to information is available when and where required and is not denied to any authorised user.

### 3.2 Risk assessment

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

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (ISO Guide 73:2002).

### 3.3 Risk management

Risk management encompasses a range of activities within an organisation that are directed at the assessment and treatment of risk.

NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication (exchange or sharing of information about risk between the decision-maker and other stakeholders) (ISO Guide 73:2002).

### 3.4 Information security incident

An information security incident is one or more unwanted or unexpected events that have a significant probability of compromising business operations and threatening information security (ISO/IEC TR 18044:2004).

Examples of security incidents are:

- loss of service, equipment or facilities
- system malfunctions or overloads
- human errors
- fraud
- non-compliance with policies or guidelines
- breaches of physical security arrangements
- uncontrolled system changes
- malfunctions of software or hardware
- access violations.

### 3.5 Threat

A threat is a potential cause of an unwanted incident which may result in harm to a system or organisation.

### 3.6 Vulnerability

Vulnerability is a weakness of an asset or group of assets which can be exploited by a threat.

## 4 INFORMATION PROTECTION FRAMEWORK

### 4.1 Identification and ownership of information

All assets, including information assets, should be accounted for and have a nominated owner and/or custodian whose responsibility it is to ensure that appropriate protection is maintained. Business processes which might involve the copying, printing, emailing, placing on websites, publishing and destroying of valuable information assets should also have a nominated and accountable owner.

Owners should be responsible for ensuring that appropriate security controls are implemented and maintained throughout the lifetime of the asset. Responsibility for implementing controls may be delegated; however the accountability should remain with the nominated owner of the asset.

An inventory of all important assets should be produced and it should be updated on a regular basis. This should include information about the type of asset, its owner/custodian, relevant licence information, business value and location.

An asset inventory:

- helps effective asset protection to take place
- is important for business continuity purposes and in the recovery from a disaster or system failure
- may be required for various other business purposes such as health and safety, insurance, finance and for compliance with certain laws and regulations.

**Examples (information assets)**

These are examples of some of the information assets which require protection:

- organisational records (e.g. company accounts, tax and VAT statements)
- personal records (Data Protection Act 1998)
- customer details
- intellectual property (e.g. designs, specifications, research results)
- healthcare records

If the organisation maintains more than one inventory, it should make sure that the content of these is aligned so that all assets are fully recorded and can be tracked.

The inventory should have an assigned owner who is responsible for its accuracy and availability and a process should be in place for its maintenance.

### 4.2 Assessment of protection needs

The security controls an organisation deploys to protect its assets should be justifiable, practical and necessary. Assessment of the protection needs and the resources required to deploy suitable protection should be balanced against the risks to the assets the business faces. The process of compiling an inventory of assets is an important aspect of risk management.

Information security risk is assessed in the following terms:

**Information Assets**

What is the importance, usefulness or value of the information asset to the organisation?

**Threats**

What are the threats which might cause harm, damage or loss to the organisation's information? How real or likely is the threat? For example, threats might include:

- system failure
- disgruntled employee
- unauthorised access by competitor
- denial of service attack
- malicious software attack
- theft of laptop
- fraud and deception
- online theft and forgeries
- identity theft

**Examples (responsibilities)**

The Data Protection Act 1998 defines a number of responsibilities including the following:

- Data controller person who determines the purpose and manner in which personal data is processed.
- Data processor any person who processes the data on behalf of the data controller.

The Companies Act 1989 defines a number of responsibilities for company directors:

- Management has the responsibility to protect all organisational records from loss, destruction and falsification, in accordance

- with statutory, regulatory and contractual requirements and obligations.
- All employees, contractors and any other users should be made aware of their responsibility to report any information security incidents as quickly as possible.
- All employees should be aware of their legal responsibilities to protect intellectual property.

**Vulnerabilities**

How and where is your information asset most vulnerable? How can it be exploited and/or compromised by the threats? For example, vulnerabilities might include:

- lack of effective procedures and instructions for handling information
- lack of user training and awareness
- weak access control on IT systems
- no allocation of responsibilities
- no information backup

**Impacts**

What would be the impact on the integrity, availability and/or confidentiality of the asset if a threat were able to exploit a vulnerability?

The process of risk assessment is good business practice. It should be the basis of any information asset classification or grading and be used to determine classification levels. By assessing these aspects, you'll get an idea of the threats to your information and the business risk to the organisation.

## LEVELS OF AVAILABILITY

Levels of availability that are defined to reflect the accessibility of information assets and the impact if such assets are not available within a specified timeframe are as follows:

- BASIC AVAILABILITY (Routine)

Information and services required for business applications and processes to be available within 12-48 hours

- MEDIUM AVAILABILITY (Priority)

Information and services required for business applications and processes to be available within 12 hours

- HIGH AVAILABILITY (High Priority)

Information and services required for business applications and processes to be available within 2-3 hours

- VERY HIGH AVAILABILITY (Immediate)

Information and services required for business applications and processes to be immediately available at all times

**Levels of confidentiality**

Levels of confidentiality that are defined to reflect the sensitivity of information assets and the impact of their unauthorised disclosure are as follows:

**Publicly available information**

This refers to information that would cause no damage to the company if disclosed.

This could be information that appears on the organisation's web site, in marketing and sales materials, public presentations and product user manuals.

**"Internal use only" information**

This refers to information available to any employee in the organisation, but to which external access is granted only with authorisation. The disclosure or loss of such information would be inappropriate and inconvenient, and could have an appreciable impact on the organisation.

**"Confidential information"**

This refers to information which is commercially sensitive and whose disclosure or loss would have a significant impact on the organisation.

For example, the impact might be financial or it might affect profitability, competitive advantage or business opportunities or it might involve embarrassment or loss of reputation.

**Strictly confidential information**

This refers to information which is commercially sensitive and whose disclosure or loss would have a very significant impact on the organisation. Again, the impact might be on the company's finances or might affect its profits, competitive advantage or business opportunities, or involve embarrassment or loss of reputation but the loss or effect, whatever its nature, would be very serious.

Organisations may also have information which is sector specific and which may influence the levels of classification described above. One such type of information, held by many organisations, is:

**Personal data/information**

This covers information about employees, customers and other individuals that is protected by the Data Protection Act. Disclosure of such information could have serious legal consequences. Information falling into this category must be treated as 'CONFIDENTIAL' or 'STRICTLY CONFIDENTIAL'.

Information that might be considered in the "Confidential" or "Strictly Confidential" category includes:

- negotiating positions
- investment strategies
- marketing information
- competitor assessments
- personal information (see above)
- customer information
- details of major acquisitions, divestments, and mergers
- high-level business and competition strategy
- very sensitive competitor, partner or contractor assessments
- high-level business plans and potential options
- patent/copyright information

## 5 DOWNGRADING

Some information is only sensitive or critical for a specific period of time. In such cases, the marking should indicate a date or event after which the information can be declassified or downgraded to a lower level. This avoids unnecessary protection of information.

### 5.1 Disposal

When information is to be disposed of, appropriate precautions should be taken to ensure it is securely destroyed (see section 6 of this booklet for some good practice on this subject).

Before sharing information with another organisation, a mutually acceptable classification scheme should be agreed. If existing classifications are used, these should be clearly related to their equivalent in the partner organisation.

## 6 HANDLING AND STORAGE OF PAPERS AND OTHER PHYSICAL MATERIAL AND MEDIA:

OBJECTIVE: To prevent unauthorised physical access, damage and interference to papers and other media. The protection required should be commensurate with the risks the business faces and the classification level of the information (references ISO/IEC 17799:2000 clauses 7.1 to 7.3).

**Integrity and availability**

Typical controls include:

- regular maintenance and testing of physical storage media

- development and implementation of appropriate handling procedures for papers and media containing information classified as medium or high integrity and/or availability - storage of papers and other physical media in areas that are suitably protected from environmental risks

**Confidentiality**

Typical controls to protect against unauthorised access include:

- physical entry controls to protect buildings and offices
- securing of individual offices, rooms and other facilities
- use of lockable cabinets, drawers and safes to ensure material is securely stored away when not in use
- clear desk policy i.e. put papers and media away when unattended and at the end of the day
- clear screen policy to ensure material cannot be observed by unauthorised people
- physical separation of papers with different classifications to ensure that strictly confidential information is not accidentally left with less sensitive information
- ensuring the user has the appropriate rights and privileges for physical access to information (depending on the level of classification)

## 6.2 HANDLING AND STORAGE OF INFORMATION IN ICT SYSTEMS

OBJECTIVE: To control access to information stored and processed by ICT systems (reference ISO/IEC 17799:2000 clauses 8.3.1, 8.6.3, 9.1).

**Integrity**

Typical controls include:

- access controls (to control access to application system functions and user rights, such as read, write, delete and execute) should be in place in line with the business access control policy, to ensure that only authorised persons can modify information
- ensuring input data is correct and complete, that processing is properly completed and that output validation is applied
- applying controls against malicious software to protect the integrity of information

**Availability**

Typical controls include:

- access controls (to control access to application system functions and user rights, such as read, write, delete and execute) should be in place in line with the business access control policy, to allow access by authorised persons and to ensure that only authorised persons can delete information
- controls against malicious software should be applied to protect the availability of information
- controls for information back-up should be in place to ensure its continued availability (see also 6.3)

**Confidentiality**

Typical controls include:

- access controls (to control access to application system functions and user rights, such as read, write, delete and execute) should be in place in line with the business access control policy, to ensure that only authorised persons have access to the information - protection of outputs from application systems (e.g. print outs) in accordance with their classification level
- regular reviews of distribution lists to ensure they are up to date and regular maintenance of formal records of recipients of information

## 6.3 INFORMATION BACKUP

OBJECTIVE: To maintain the integrity and availability of information (reference ISO/IEC 17799:2000 clause 8.4.1).

**Integrity, availability and confidentiality**

Typical controls include:

- take regular back-up copies of sensitive and/or critical business information
- give back-up information an appropriate level of protection against unauthorised access and physical and environmental risks
- ensure the protection given to back-up information is consistent with the standards applied to the information itself
- store a minimum level of back-up information (as well as accurate and complete records of the back-up copies) in a remote location
- adequate back-up arrangements and facilities should be provided and regularly tested to ensure that all critical business information can be recovered following a disaster or systems failure
- back-up and restoration procedures should be available and should be regularly checked and tested to ensure they remain effective

## 6.4 DISPOSAL OF INFORMATION

OBJECTIVE: To prevent loss, damage or compromise of assets (reference ISO/IEC 17799:2000 clause 7.2.6).

**Integrity and availability**

Typical controls include:

- information for disposal should be clearly and unambiguously identified and appropriate approval should be obtained (e.g. by the information owner) before disposal
- a record of all disposals should be kept

**Confidentiality**

Typical controls include:

- dispose of office waste, using an approved company where appropriate
- destroy by approved cross-cut shredding, physical destruction, burning or pulping, carried out by a trusted approved person or organisation
- delete files on desk top computers, laptops and other devices (including backup copies) using a wipe utility to overwrite

## 6.5 DISPOSAL OR REUSE OF EQUIPMENT AND MEDIA

**Integrity and availability**

Typical controls include:

- consider if damaged storage devices containing sensitive data require a risk assessment to determine if the items should be destroyed or discarded or whether they could be repaired and re-used
- test equipment and media prior to re-use to ensure reliable functioning
- overwrite removable media before re-use
- overwrite hard disc before relinquishing control of an IT system

**Confidentiality**

Typical controls include:

- dispose of equipment and storage devices (sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function) - overwrite removable media before re-use
- overwrite hard discs before relinquishing control of an IT system
- use an approved company to destroy media which cannot be overwritten, or is damaged
- ensure all images, archive and back-up copies are destroyed or protected as appropriate and subsequently removed from the asset register

## 6.6 EXCHANGES OF INFORMATION INCLUDING THE USE OF INTERNET AND OTHER PUBLICLY ACCESSIBLE NETWORKS

**Integrity and availability**

Typical controls include:

- verify the integrity of on-line transactions e.g. using electronic signatures
- check the integrity of electronically published information e.g. on the internet prior to publishing, and ensure the information is only published after appropriate authorisation
- review information that is electronically published e.g. on a website on a regular basis for accuracy and completeness

**Confidentiality**

Typical controls include:

- protect physical media against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries
- protect internal systems from external connections and networked systems using an appropriately configured and maintained firewall
- ensure that information that is sensitive or critical is not stored on an ICT system connected in any way to the internet or other publicly accessible network (i.e. any network you don't control or trust)
- only send information that is sensitive over the internet or other publicly accessible network in an encrypted form (e.g. using currently available mechanisms such as SSL Secure Sockets Layer)
- encrypt on-line transactions

## 6.7 SYSTEMS ACCEPTANCE AND CAPACITY PLANNING

OBJECTIVE: To minimise the risk of system failures and to ensure availability of adequate capacity and resources (reference ISO/IEC 17799:2000 clause 8.2).

**Integrity**

Typical controls include:

- ensure the capacity of existing systems is sufficient to allow correct working and interaction of all business applications
- ensure system acceptance criteria have been met before new systems are put into operation; all associated controls and procedures should be in place
- error recovery and restart procedures (and business continuity arrangements) should be in place for new systems, to ensure that the system and the information processed on the system, is not corrupted
- test the correct functioning of new systems and the interaction with existing systems to ensure correct processing
- ensure users are given appropriate training in the operation of new systems

**Availability**

Typical controls include:

- apply monitoring controls to identify current system use and potential problems, especially for important systems and system resources, and use controls to indicate capacity problems immediately
- make projections of future requirements, taking account of new business applications and related system requirements
- ensure new systems fulfil the identified performance and capacity requirements
- put error recovery and restart procedures in place for new systems, as well as business continuity and fallback arrangements, to ensure sufficient availability of the systems
- test the reliable working of new systems, taking into account the effect on existing

systems, especially in peak processing times, to ensure the required availability of all systems
- train users in the operation of new systems

**Confidentiality**

Typical controls include:

- identify confidentiality requirements of new systems and implement appropriate controls and procedures, ensuring the required confidentiality protection
- test new systems before introducing them, taking into account the possible effects on existing systems as well as the confidentiality of information processed

## 6.8 MOBILE COMPUTING DEVICES AND PHONES AND SECURITY OF OTHER EQUIPMENT OFF-PREMISES

OBJECTIVE: To ensure information security is in place and appropriate when using mobile computing and teleworking facilities (reference ISO/IEC 17799:2000 clauses 7.2.5 and 9.8).

**Integrity, availability and confidentiality**

Typical controls include:

- warn company personnel not to discuss information of a sensitive or critical nature in public places to avoid being overheard or intercepted e.g. when using mobile phones, when travelling with colleagues or at external meetings or conferences
- ensure that the information security of off-site equipment is equivalent to that of on-site equipment used for the same level of information classification; this should take into account the risks of working outside the organisation's premises. For example documents, laptops and other mobile computing devices should be locked inside hotel safety deposit boxes or should be supervised at all times
- put in place protection for the connection of mobile devices to the organisation's networks; this should include user identification and authentication to avoid compromise of the information on the organisation's network, e.g. in case the equipment has been stolen
- put guidelines in place for protection against malicious code, and take appropriate backup of all information on mobile devices to protect against information loss should the equipment itself be lost or stolen

## 6.9 POSTAL AND COURIER SERVICES

OBJECTIVE: To ensure the protection of information being sent by post, avoiding disclosure, theft, damage, misuse or corruption of the information in transit.

**Integrity and availability**

Information being sent through the post should be protected against theft, damage, misuse or corruption during transportation beyond an organisation's physical boundaries. This can be done by:

- using a trustworthy courier service and using packaging that makes any attempt to access the content obvious
- asking the recipient to verify receipt and to confirm that the envelope or package does not appear to have been tampered with.

**Confidentiality**

Sensitive information should be protected against unauthorised access during transportation beyond an organisation's physical boundaries. Typical controls include:

- package sensitive information in such a way that the sensitivity level of the information is not externally apparent
- send information that is sensitive but not at

the highest level in a single sealed envelope optionally marked ‘to be opened by the addressee only’. If sent externally, no security marking should appear on the outer envelope
- the use of double envelopes is recommended for the highest levels of sensitive information and these should be sent by a trustworthy courier. The outer envelope should bear no security marking

## 7 INFORMATION SECURITY POLICY

The organisation should have a policy in place which demonstrates management commitment and its approach to managing information security and the protection of its information assets (the DTI publication, "Information Security: A Business Manager's Guide" URN 04/623 includes a security policy template). This policy should cover all types of information and will apply to information owned by the organisation or owned by someone else but in the care of the organisation. At a minimum this policy should:

- make statements about the business objectives, scope and importance of information security as an enabling mechanism for information sharing within the organisation
- recognise the need for necessary security resources
- define clear responsibilities and accountabilities for information security
- provide a framework for the management of risk and setting control objectives and controls proportionate to the assessed risks
- ensure regular monitoring and reporting of security performance and incidents
- appoint an Information Security Manager to maintain the policy and to provide guidance on security measures
- ensure clear and simple security standards are developed and are followed by employees.

## GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at http://www.businesslink.gov.uk or calling 0845 600 9 006.

Published by the Department of Trade and Industry. http://www.dti.gov.uk