

Protecting Business Information Keeping It Confidential

The issues raised in this and the companion booklet *Protecting Business Information – Understanding the Risks* are intended to make you aware of your potential vulnerability to loss of information. They provide general guidance only and, if fully implemented, can only reduce, not eliminate, your vulnerability. They should not be taken as providing specific advice applicable to your particular circumstances. The Secretary of State for Trade and Industry, the DTI and those who have helped develop these booklets cannot be held liable for any loss or damage due to any negligent statements or omissions.

This booklet has been prepared by the following companies, organisations and government departments on behalf of the DTI:-

The British Petroleum Company plc
British Aerospace plc
British Standards Institution (DISC)
British Telecommunications plc
Cabinet Office
Communications-Electronics Security Group
Coopers & Lybrand
Coutts Group
CSC Computer Sciences Ltd
Defence Research Agency
Deloitte & Touche
DMR Group Ltd
ICL
Institute of Chartered Accountants
in England & Wales
Lloyds TSB Group plc
Midland Bank plc
Nationwide Building Society
Prudential Assurance Co Ltd
The Security Service
Sema Group plc
Shell International Ltd
Unilever plc
Xisec Consultants Ltd

Contents

- 1 Background
- 2 Introduction and Objectives
– How to use this booklet
- 3 Security Classification and Marking
- 4 Protection
- 5 Trusted Partners

- Interoperability between organisations
- 6 Management and Assurance
- 7 Implementation
- Appendix A
 - Secure Computer Systems
- Appendix B
 - Definitions

1. Background

An organisation's information is one of its most important assets. It needs to be protected, particularly since it is often shared within the organisation and with trading partners.

You may have read the companion booklet *Protecting Business Information – Understanding the Risks* which explains how widespread and serious the problem can be. This booklet sets out in greater detail some suggested solutions.

Many organisations already have an information security programme in place, that ensures consistent identification and protection of sensitive material. However, you can't make assumptions about how your trading partners may protect your information. Few organisations follow a common approach to sharing information securely.

Following the approach in this booklet, you should be able to:

- protect your company's sensitive information consistently and appropriately
- protect information entrusted to you by other organisations

By doing this, you should:

- reduce the risk of damage to your company's reputation, profitability or interests due to loss of sensitive information
- reduce the risk of embarrassment or loss of business arising from loss of another organisation's sensitive information
- increase confidence in trading partnerships and in the outsourcing of sensitive work
- simplify the exchange of sensitive information with third parties, while ensuring risks are managed.

Who should read this booklet?

This booklet is intended for managers in organisations that need to protect sensitive information, in any form. In particular, it should be of interest and value to:

- Board Members
- Senior Managers
- Internal Auditors
- Security Managers

2. Introduction and Objectives

This booklet provides current best practice guidance on a common approach to appropriate marking and protection of confidential information in industry and commerce.

It has been developed by a group of leading UK companies and organisations, on behalf of the Department of Trade and Industry.

Scope

The guidance covers:

- classification of information, and appropriate marking or labelling, to show
- the information is sensitive. This should ensure that recipients know to employ appropriate protective measures
- protection of information in an appropriate, practical and cost-effective way, that is proportionate to the business risk of disclosure. The need for protection is indicated by the classification marking, which may be used within the organisation or when shared with other commercial or government organisations
- compatibility between individual companies' security classification schemes, and also with the Government's protective marking system
- assurance of effective management of information protection in organisations.

The security measures outlined in this booklet are considered appropriate to the UK business environment. They represent a minimum baseline for each level of classification. Extra security measures may be necessary in some circumstances.

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 national security information, although national security obligations must continue to take precedence.

How to use this booklet

It's important to understand the principles of effective information security. Chapter Three explains the concept of classification, and Chapter Four covers security risk management and protection. You could use this to assess the risks to your organisation, and in particular to the departments and functions likely to be handling sensitive information.

Chapter Five describes inter-operation between different organisations.

Chapter Six covers management and assurance – how to ensure security standards are followed and complied with on a daily basis.

The implementation section (Chapter Seven), covers four categories of organisation:

- Commercial organisations that do not have a formal security classification and protection policy framework

- Commercial organisations that do have a formal security classification and protection policy framework
- Government departments
- Government contractors working with protectively-marked Government information.

Appendix A describes some measures of protection of confidential information on IT systems.

Appendix B provides a glossary of terms used in this booklet.

3. Security Classification and Marking

Classified information is marked so that people know to apply appropriate security protection. The classification is dependent upon the impact or damage likely to occur if the information was leaked or disclosed to the wrong people.

Exactly how information is protected will vary from company to company, or even from department to department, but the level of protection should be the same.

This guidance defines three levels of classification (see below). Several UK companies and UK Government have matched these against their own internal schemes.

Unified Classification Markings – Definitions

SEC1 Information whose unauthorised disclosure, particularly outside the organisation, would be inappropriate and inconvenient. This is routine information which an organisation simply wishes to keep private. This classification may not need to be marked on information; it refers to the majority of information.

SEC2 Information whose unauthorised disclosure (even within the organisation) would cause significant harm to the interests of the organisation. This would normally inflict harm by virtue of financial loss; loss of profitability or opportunity; embarrassment or loss of reputation. This information might include:

- Negotiating positions
- Marketing information
- Competitor assessments
- Personnel information
- Customer information
- Material protectively-marked RESTRICTED by UK Government

SEC2 should be marked or communicated with any material to which it applies.

SEC3 Information whose unauthorised disclosure (even within the organisation)

would cause serious damage to the interests of the organisation. It would normally inflict harm by virtue of serious financial loss, severe loss of profitability or opportunity, grave embarrassment or loss of reputation. This information might include:

- 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 secrecy information
- Material protectively-marked CONFIDENTIAL by UK Government

SEC3 should be marked or communicated with any material to which it applies.

The above defines the three security (SEC) levels. Organisations should use their own terminology to describe these levels, and should relate them to their business in terms of the impact or damage which would arise from unauthorised disclosure.

Organisations that have their own security schemes can match their definitions and classification levels against those in the table. They can then continue to use their own markings but should add the 'SEC' marking at the end, to enable others to recognise the level of classification. Organisations that share sensitive information with others should agree on the classification terminology that will be used in advance of any information sharing.

Information identified as SEC2 or SEC3 should always be marked – whether it is on paper, cassette, disk, slide, flip chart, film, microfiche, photographs or any other media.

Some companies may not need to define SEC3 for their own company's confidential information; SEC2 may be all that is needed. In this case, they should make clear to trading partners that they do not handle SEC3 information securely.

You should not map your existing classification scheme arbitrarily onto this guidance. You may have an internal classification level that falls between SEC1 and SEC2. If material bearing this intermediate marking is passed to another organisation, it should be marked at the higher level, ie. SEC2. You should not under-protect another organisation's information.

Downgrading

Some information is only sensitive for a specific period of time. In this case, the marking should therefore indicate a date, or event, after which the information can be de-classified. This avoids unnecessary protection of information.

4. Protection

Information should be protected in accordance with the business risk of unauthorised disclosure. This guidance is based on the low-threat scenario usually encountered in the UK. If the level of threat is constant, the required level of protection will be proportionate to the damage likely to result from unauthorised disclosure – the security classification level.

Risk management

Security measures should be justifiable, practical and necessary. They should be balanced against the business risk of disclosure. Business risk is assessed in the following terms:

Impact	What would be the impact on the organisation if the information were disclosed? This is the basis of security classification and is used to determine the SEC level.
Threat	Which individuals or organisations are likely to want to obtain your information? How effective might they be? What methods might they use and what resources and capabilities do they have?
Vulnerability	Where is your information most vulnerable? How can it be compromised?

By assessing these three aspects, you'll get an idea of the threats to your information and the business risk to the organisation.

Minimum standards

Classified and protectively-marked information should be protected properly.

The minimum standards of protection, which are appropriate to commercial information within the UK, are described in the following tables. Additional current good practice advice on how to achieve these minimum standards is set out in italics. Overseas, risks may be greater and additional measures may be necessary.

SEC1

disclosure would be inappropriate or inconvenient

Due diligence

Optional

Handle as information which bears no protective marking.

SEC2

disclosure would cause significant harm

Access limited to those with a need-to-know.

Store under conditions which make accidental or opportunist compromise unlikely and deter deliberate compromise.

Handle, transmit and use with care and take basic precautions against accident and opportunist attack.

When destroying, make reconstitution unlikely.

Papers should be marked clearly with the internal classification marking, followed by sec2 if passed outside the organisation, to leave no doubt as to the sensitivity.

All physical media should be clearly marked with the internal classification marking, followed by sec2 if passed outside the organisation.

Show the security classification marking in capital letters, at least 5mm high, at the top and bottom of each page.

Handle as UK RESTRICTED information.

SEC3

disclosure would cause serious damage

Access limited to those authorised to see and handle the information.

Store under conditions which make accidental compromise unlikely, offer a degree of resistance to deliberate compromise, and make actual or attempted compromise likely to be detected.

Handle, use and transmit to make accidental and deliberate compromise unlikely. Make actual or attempted compromise likely to be detected.

When destroying, make actual or attempted compromise likely to be detected.

Papers should be marked clearly with the internal classification marking, followed by sec3 if passed outside the organisation, to leave no doubt as to the sensitivity.

All physical media should be clearly marked with the internal classification marking, followed by sec3 if passed outside the organisation.

Show the security classification marking in capital letters, at least 5mm high, at the top and bottom of each page.

Handle as UK CONFIDENTIAL information.

SEC1

disclosure would be inappropriate or inconvenient

Optional

Handle within a secure perimeter.

Store within a secure perimeter. Recommend all material and documents are cleared away at the end of the day.

SEC2

disclosure would cause significant harm

Personnel security checks should be carried out for staff who need to access SEC2 information.

Handle within a secure perimeter. Ensure the material cannot be observed by unauthorised people.
If left unattended and no trusted staff are supervising, the information should be secured.

Material should be locked in a cabinet within a managed security perimeter when not in use.

Materials carrying secondary imprints (such as typewriter and printer ribbons) should also be locked away as SEC2 information when unattended for long periods of time.

SEC3

disclosure would cause serious damage

Personnel security checks should be carried out for staff who need to access SEC3 information.

Handle within a secure perimeter. Ensure the material cannot be observed by unauthorised people.

If left unattended and no staff are supervising, the material should be locked away in an approved security container.

Material should always be locked in an approved security container within a managed security perimeter when not in use.

Materials carrying secondary imprints (such as typewriter and printer ribbons) should be locked away as SEC3 information when unattended for long periods of time.

A clear desk policy, where all papers are locked away when not in use, should be strictly enforced. This provides good assurance that SEC3 information cannot accidentally be left lying under less sensitive papers and not be locked away.

SEC1

disclosure would be inappropriate or inconvenient

Process within a secure perimeter.

Removable material should be put away and equipment switched off when not in use.

SEC2

disclosure would cause significant harm

IT systems should be located within a managed security perimeter, which includes any connected networks.

Effective access controls should be in force and monitoring procedures should be in place to detect unauthorised access.

Otherwise information should be stored on removable media and SEC2 physical security applied, or the entire IT system protected by physical security consistent with SEC2 protection for physical material, with no network connections. In this case, only authorised staff with a need to access all the information on the system should be given physical access.

SEC3

disclosure would cause serious damage

IT systems should be located within a managed security perimeter, which includes any connected networks.

IT systems should be strongly secured with trusted approved access controls which are highly resistant to penetration by a capable attacker. Highly effective monitoring procedures should be in place to detect unauthorised access.

Information may alternatively be stored in an encrypted form and protected to SEC3 level when not in use.

Otherwise, information should be stored on removable media and SEC2 physical security applies, or the entire IT system protected by physical security consistent with SEC2 protection for physical material, with no network connections. In this case, only authorised staff with a need to access all the information on the system should be given physical access.

SEC1

disclosure would be inappropriate or inconvenient

May be made available to anyone within the organisation, unless an additional marking or indication restricts this.

Release outside the organisation requires justification and satisfaction of the intent of the information owner.

No restrictions

SEC2

disclosure would cause significant harm

Not to be disclosed unless there is a business, contractual or legislative need.

Should be disclosed only on a need-to-know basis, in ways which are consistent with the information owner's wishes.

Steps should be taken to ensure that the recipient knows the sensitivity level and is aware of the implications for its protection.

It should only be released to trusted partners covered by an agreement.

Should be carried out or supervised by trusted individuals or trusted partners. Extra or spoilt copies should be destroyed.

SEC3

disclosure would cause serious damage

Not to be disclosed unless there is a business, contractual or legislative need.

Should be disclosed only on a strict need-to-know basis, with referral to the information owner.

Assurance should be sought from the recipient that they understand the sensitivity and that they know how to protect the information.

It should only be released to trusted partners covered by an agreement.

To control distribution more strictly, put a clear additional marking to this effect on the document.

Copying must be authorised by the information owner. There should be strict control over copying of SEC3 material.

Copying should be carried out or supervised by trusted individuals or trusted partners and positive steps taken to find and destroy extra or spoilt copies.

Clear distribution lists and numbering of copies provide strict control over copying. If sent to government, the document should be marked 'not to be copied further' if this is the intent.

SEC1

disclosure would be inappropriate or inconvenient

No restrictions

External mail should be sealed.

SEC2

disclosure would cause significant harm

Should not take place in a public place where conversations can be overheard.

Should be sealed and sent in such a way that the sensitivity level of the information cannot be deduced from the outside of the letter.

May be sent 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. Double envelopes (as for SEC3) are recommended.

SEC3

disclosure would cause serious damage

Discussions should only take place where assurance can be gained that there is little risk of the conversations being overheard directly or by eavesdropping or surveillance technology.

Should be sealed and sent in such a way that the sensitivity level is not apparent from the outside covering and that safeguards exist to prevent and detect attempts to read the contents. The security marking should however be made clear to the recipient.

Should be delivered by a trusted individual or sent by a trustworthy courier (including Royal Mail in the UK) in a double sealed envelope. The inner one should be marked with the security marking (i.e. SEC3). The outer envelope may be optionally marked with the label 'to be opened by the addressee only'. The outer envelope should bear no security markings which gives away the sensitivity level. A receipt should be enclosed for the recipient to send back.

SEC1

disclosure would be inappropriate or inconvenient

No restrictions

No restrictions

No restrictions

SEC2

disclosure would cause significant harm

Steps should be taken to ensure that the fax is being sent to the correct station.

Verify that the receiving station is the required one. Confirm that the receiving station is ready to receive and that the machine is physically secured to SEC2 level or attended by a trusted person. Transmission should be carried out or supervised by a trusted person.

Conversations only permitted over approved communications facilities, ensuring the conversation cannot be overheard.

Analogue (non-GSM) mobile phones, hotel phones, public phones and those in high-risk locations (e.g. overseas, competitor's offices) should not be used as calls could be monitored or overheard.

As for telephones

SEC3

disclosure would cause serious damage

Faxes may be sent only over approved secure fax systems and steps should be taken to ensure that the fax is being sent to the correct station.

Verify that the receiving station is the required one. Confirm that the receiving station is ready to receive and that the machine is physically secured to SEC3 level or attended by a trusted person. Transmission should be carried out or supervised by a trusted person.

Encryption should be used.

Conversations only permitted over approved secure telephones.

Steps should be taken to ensure both parties cannot be overheard speaking into their telephones.

Analogue (non-GSM) mobile phones, hotel phones, public phones and those in high-risk locations (e.g. overseas, competitor's offices) should not be used as calls could be monitored or overheard.

Encryption should be used.

As for telephones

SEC1

disclosure would be inappropriate or inconvenient

Should be sent, received and conveyed over IT systems and networks secure to SEC1 level.

Messages should only be sent over the Internet if they contain no sensitive or contentious information at all, unless secure approved encryption is used.

No restrictions, unless sent via the Internet, in which case encryption should be used.

Connections should only be made via an approved secure network firewall.

SEC2

disclosure would cause significant harm

Should be sent, received and conveyed over IT systems and networks secure to SEC2 level. If secure approved encryption is used, intermediate networks and IT systems need not be secure, but sending and receiving system should still be secured to SEC2 level.

The electronic mail system should be specially secured to prevent accidental or deliberate mis-routing of messages, unless secure approved encryption is used. Any messages sent via the Internet should be encrypted using secure approved encryption.

Should be sent over an approved network or conveyed on physical media.

Encryption should be used on insecure networks.

Connections should be made via an approved secure network firewall.

SEC3

disclosure would cause serious damage

Should be sent, received and conveyed over IT systems and networks secure to SEC3 level. If secure approved encryption is used, intermediate networks and IT systems need not be secure, but sending and receiving system should still be secured to SEC3 level.

The electronic mail system should be specially secured to prevent accidental or deliberate mis-routing of messages, unless secure approved encryption is used. Any messages sent via the Internet should be encrypted using secure approved encryption.

Government information protectively-marked

'UK CONFIDENTIAL' must not be transmitted over the internet, even if encrypted.

Should only be sent over approved specially secured networks.

Networks should be fully physically secured, encrypted, or both.

Connections should only be made via a very strong approved secure network firewall.

Government information protectively-marked 'UK CONFIDENTIAL' must never be stored on an IT system connected in any way to the internet or other publicly-accessible network.

SEC1

disclosure would be inappropriate or inconvenient

Physically secure as for SEC1 papers.

Dispose of office waste using an approved company where appropriate.

Delete files (including backup copies).

No restrictions

No restrictions

SEC2

disclosure would cause significant harm

Physically secure as for SEC2 papers, unless approved encryption is used.

Destroy by approved cross-cut shredding, pulverising, burning or pulping, carried out by a trusted approved person or organisation.

Protect to SEC2 level before destruction.

Over-write removable media before re-use. Over-write hard disks before relinquishing control of a computer system. Media which cannot be overwritten or which is damaged should be destroyed by an approved company.

Ensure all image, archive and backup copies are destroyed or protected as appropriate.

Home working should be approved by the organisation and appropriate, approved security facilities provided to the SEC2 level.

Information should not be discussed on aeroplanes or other forms of public transport, or where an untrusted driver or persons are present.

Documents and portable computers should be locked inside hotel safety deposit boxes when trusted and individual keys are available, or kept supervised at all times.

SEC3

disclosure would cause serious damage

Physically secure as for SEC3 papers, unless approved encryption is used.

Destroy by approved cross-shredding, pulverising, burning or pulping, carried out by a trusted approved person or organisation.

Protect to SEC3 level before destruction.

Destruction should be recorded.

Hard disks should be overwritten using a secure approved utility. Removable media should be degaussed or destroyed as for paper. Media which cannot be over written or is damaged should be destroyed by an approved company.

Ensure all image, archive and backup copies are destroyed or protected as appropriate.

Home working should be approved by the organisation and appropriate, approved security facilities provided to the SEC3 level.

Information should not be discussed on aeroplanes or other forms of public transport, or where an untrusted driver or persons are present.

Should not be discussed in public places, hotel rooms or restaurants.

Documents and portable computers should be secured to SEC3 standards at trusted offices or kept supervised at all times.

5. Trusted Partners

Exchanging sensitive information between organisations should be simplified if all parties follow this guidance.

Secure sharing of sensitive information is always important, but especially during activities such as:

- forming or operating a joint venture. This might involve exchanging sensitive strategies, marketing plans, commercial information and product plans;
- contracting out work which is likely to involve handling sensitive information;
- negotiating with other organisations, perhaps as part of a company disposal, merger or acquisition; and
- discussions with Government.

If sensitive information is given to another organisation, you should ensure that they understand the need for protection and agree to protect it properly. They can follow the guidance in this booklet, which should assist them to give appropriate protection to information bearing a unified classification marking (e.g. SEC2, SEC3).

You may wish to satisfy yourself that they meet your security requirements (see Chapter six), either by self-audit or external audit review.

You should also consider including confidentiality clauses in contracts with third parties. These might reference this guidance and specify how it applies to your organisation. Effective security measures will only work if everyone involved is familiar with appropriate security procedures.

When information is passed to another organisation, it should be marked with the appropriate unified classification marking, in addition to any internal marking. The receiving organisation should handle and protect it appropriately.

In some circumstances, for example, where there is a higher level of threat, you may need to give the recipient additional advice, and build special security provisions into contracts.

6. Management and Assurance

You will need to use a combination of pro-active management and verification in order to assure yourself that an organisation is going to protect your sensitive information properly. This in turn requires awareness, support and, crucially, commitment from top management.

Awareness of the Risks

It is vital that management and staff are aware of the risks. Keeping summary records of internal and external security incidents, and briefing staff on them and other threats, is of great value. On-going awareness programmes are essential.

Clear Management Commitment

Top management should demonstrate their commitment to protecting sensitive information by setting clear company policy. At a minimum this policy should:

- confirm the need for security and recognise the need for necessary security resources;
- define clear responsibilities and accountabilities for information security;

- stress that measures should always be proportionate to the assessed risks;
- ensure regular monitoring and reporting of security performance and incidents;
- appoint an Information Security Manager to maintain the policy, to provide guidance on security measures;
- ensure clear and simple security standards are developed and followed by employees.

Assurance

It is important that security policies and standards are followed and that these standards are in line with good practice guidance. You could achieve this using one of the following methods:

- Internal self-assessment, based on limited implementation of the guidance. Organisations exchanging sensitive information might agree with each other the scope of compliance.
- Internal self-assessment, based on implementation of this guidance. Contractual agreements should make it clear that detailed security arrangements within each other's organisation will remain in line with stated minimum standards.
- Full assessment. Organisations are externally reviewed and formally certified. Each organisation must fully implement its own documented security procedures taken from the minimum standards, as well as any facilities it documents as 'approved'. This assurance can then be relied upon within contractual arrangements, without the need for contract-specific agreements and verification. Each approved facility should be documented, showing the grounds for approval. The documented security procedures and approvals should be made available on request to any organisation, which has signed a confidentiality agreement, with whom confidential information is shared.

7. Implementation

This section provides guidance on the minimum steps companies should take to protect information. It divides organisations into four categories: Beginners, or those with no protection policy in place; Advanced – those that already have a formal policy; Government departments; and Government contractors – companies working on Government contracts involving protectively marked Government information.

Beginners

Commercial organisations with no formal security classification and protection policy framework in place, should follow the steps listed below:

- Step 1 Make all staff aware of the need for sensitive information security, and the principles behind classification marking
- Step 2 Develop and implement a policy for information security and standards, perhaps alongside business partners who already have classification schemes in place.

This will involve:

- Defining high-level statements and gaining management acceptance.

- These statements don't have to be complex – the simpler the better.
- Deciding what security classification levels you need (see Chapter Three). Some organisations may not need to use the highest level.
- Assessing the risks to the organisation, and establishing how to define each classification level in terms that staff understand.
- Defining and clearly documenting easy-to-understand standards and procedures for marking and handling classification-marked information. These should meet the minimum standards in Chapter Four. Document any minor trade-offs which may have been made. Ideally, the standards and procedures for general use should be complete, yet concise enough to fit on to an A4 card.
- Ensuring the necessary cabinets, locks, IT controls, perimeter controls and personnel measures are in place. Organisations must very clearly document – and implement – their approved security facilities.
- Reviewing compliance and following-up areas of non-compliance.
- Maintaining awareness through team briefings, posters etc.

- Step 3 Begin marking and protecting internal information.
- Step 4 Raise awareness of the benefits of protecting sensitive information sent to – and received from – other organisations. Brief managers in departments likely to be involved in this on the risks, and on the secure exchange of confidential information (see Chapter Five).
- Step 5 Begin using the guidance in this booklet when exchanging sensitive information with business partners.
- Step 6 Determine what level of assurance is needed (see Chapter Six), and take steps to achieve it, and use this to inform senior management, business partners and customers.

Advanced

Commercial organisations which have already implemented a formal security classification and protection policy framework.

The organisation's Security Manager should follow these steps:

- Step 1 Assess the definitions of internal security classification markings against the unified classification in Chapter Three. Match up internal and unified markings using agreed rationale.
- Step 2 Review your security standards for each internal classification level against the minimum standards for the corresponding unified classification level.
- Step 3 Clearly document and explain any trade-offs. These may need to be inspected during assurance reviews. Clearly document approved security facilities, where appropriate. If internal security standards consistently fall below the corresponding minimum standards (especially at the SEC3 level), you may have to decide whether to avoid handling external SEC3 information, to upgrade internal procedures, or to implement special internal procedures for SEC3 material.
- Step 4 Update existing security standards and procedures to include how to

- send sensitive material outside the organisation using the unified classification markings.
- Step 5 Update existing security standards or procedures to include how the unified classification markings correspond with internal security classification markings. Protect any incoming information in accordance with the existing internal markings.
- Step 6 Use the guidance when exchanging sensitive information with business partners. Use the SEC markings in addition to your own internal markings.
- Step 7 Raise awareness of the benefits of protecting sensitive information sent to – and received from – other organisations. Brief managers of departments likely to be involved with other organisations (see Chapter Five) on the benefits and use of this guidance.
- Step 8 Decide what level of assurance is needed (see Chapter Six), and take steps to achieve it and use this to inform senior management, business partners and customers.

Government Departments

UK protective security markings have been assessed against the unified classification scheme. These are:

not protectively marked	SEC1
RESTRICTED	SEC2
CONFIDENTIAL	SEC3

Departmental Security Officers should raise awareness and update security instructions so that:

- Protectively-marked government information sent to non-Government organisations, other than those approved by Government, should be marked with the corresponding SEC unified marking beside the UK protective marking. This may be used when discussing matters involving commercial confidentiality.
- Information received from non-Government organisations bearing a SEC marking should be protected in accordance with the corresponding UK protective marking.
- Government information sent to approved contractors can bear the appropriate UK protective marking without a SEC marking.

Departmental Security Officers should explain the benefits of protecting sensitive information sent to – and received from – other organisations. They should brief managers likely to be involved with other organisations (see chapter five) in the use of this guidance.

Government Contractors

UK protective security markings are already assessed against the unified classification scheme:

not protectively marked	SEC1
RESTRICTED	SEC2
CONFIDENTIAL	SEC3

The implementation guidance in (1) or (2) above should be followed for commercial security requirements. An organisation could seek to adopt a unified set of security measures, rather than operating two separate security regimes.

Appendix A – Secure Computer Systems

The British Standard BS7799 provides a framework for operating effective information security on computer systems. For further information on BS7799 telephone BSI on: 020 8996 7424.

The ITSEC Scheme, managed by the Communications Electronics Security Group (CESG), provides a way of identifying independently tested assured computer security products. Some organisations have found that unless computer security products are independently assured, there is a very high chance that security flaws exist which can be exploited, or that necessary security facilities are missing. Products are certified to different assurance levels, ranging from E1-E6. For further information on ITSEC telephone the ITSEC certification body on 01242 238739.

SEC2

At SEC2 level, computer systems should have a set of personnel, physical, procedural and technical IT controls which meet the SEC 2 ‘intent behind protection’, namely:

- to limit access effectively to those with a need-to-know;
- to store under conditions which make accidental or opportunist compromise unlikely and deter deliberate compromise;
- to handle, transmit and use with care; and to take basic precautions against accidental and opportunist attack;
- to make reconstitution unlikely, when destroying or deleting.

This implies SEC2 information should be processed and held on systems such that:

- 1 Effective access control systems are used which require physical security to control access on a person-by-person basis, or passwords or other authentication methods. Access should be granted to SEC2 information on an individual basis for each location where SEC2 information is stored.

Access controls should ensure no-one without a ‘need-to-know’ can gain access to the information. Procedures should ensure that users’ identities are clear on registration – and that they are de-registered and that access is denied when they no longer have a ‘need-to-know’.

- 2 Monitoring systems are operated to gather information on users accessing systems holding SEC2 information; and procedures should ensure potential attackers are deterred by effective review of fit-for-purpose audit logs.
- 3 There should be reasonable assurance that computer security measures cannot be easily bypassed. These principles apply to single systems as well as networked systems, and networks themselves. Use of computer system software which has been certified by the ITSEC scheme to E2, should give effective protection.

- 4 Data stored on IT systems and subsequently deleted should be erased from disks.

SEC3

At the SEC3 level, computer systems should have a set of security measures consisting of personnel, physical, procedural and technical IT controls which meet the SEC 3 'intent behind protection', namely:

- to limit access effectively to those authorised to see and handle the information.
- to store under conditions which make accidental compromise unlikely, offer a degree of resistance to deliberate compromise, and make actual or attempted compromise likely to be detected.
- to handle, transmit and use to make accidental and deliberate compromise unlikely. Make actual or attempted compromise likely to be detected.
- to make actual or attempted compromise likely to be detected when destroying or deleting.

At the SEC3 level, computer systems will need to be either:

- a Stand-alone and reliant on physical security, or
- b Accessible to multiple users, all of which are authorised to see all the SEC3 information on the system (though not all may have a need to see all of it), or
- c Accessible to multiple users, where very strong access control is enforced. This will be through formally certified secure computer systems which have secure partitioning or mandatory access control capability to ITSEC E3 assurance and F-B1 functionality.

This implies SEC3 information should be processed and held on systems such that:

- 1 Very effective access control systems are in use which require individual physical access controls, or use passwords or other authentication methods. Access to SEC3 information should be granted on an individual basis for each location where SEC3 information is held.

Access controls should ensure that no-one without specific authorisation and a need-to-know, can gain access to the information.

Procedures should ensure user identities are clear on registration – and are de-registered and access-denied quickly and effectively when they no longer have a need-to-know.

- 2 Monitoring systems are operated to gather information on users accessing systems holding SEC3 information; and procedures should ensure potential attackers are deterred by effective review of fit-for-purpose audit logs.

The audit trails should ensure that any attempt to penetrate security or otherwise compromise SEC3 information will be detected and logged.

- 3 Seek positive assurance that security measures cannot easily be bypassed by a thief or hacker. These principles apply to single systems as well as networked systems, and networks themselves, which should be given effective protection against interception (such as physical security or encryption). Use of computer system software which has been certified by the ITSEC scheme to E3, should give effective protection.
- 4 Data stored on IT systems and subsequently deleted should be erased from storage media to prevent unused areas being trawled for information. Storage media removed from the system to be re-deployed or maintained should be protected to SEC3 level until physically destroyed or thoroughly demagnetised using approved equipment.

Appendix B – Definitions

Access Controls

IT access controls perform the same function as locks in securing information on computer systems. However, access controls can be insecure. Take care to ensure IT security measures have assured strength against penetration, in the same way that locks should be checked to ensure they cannot be forced or picked.

Approved

This means the organisation's expert security adviser has investigated the issue or product and has determined that the required levels of protection are provided. The criteria and rationale for approval should be clearly documented for each approved facility, device or procedure.

Cross-cut Shredder

This is a type of shredder which cuts paper both vertically and horizontally into small fragments. Ideally these should be no larger than about 2mm by 14mm.

Data

This includes:

- Information on any size or form of computer
- Information on computer-readable media
- Computer-transmitted information
- Electronic Mail
- Electronic commerce, including EDI

Encryption

This is a means of enciphering or encoding information which is essentially unreadable without a key to decode it. Different encryption products may provide different levels of security.

Some fax machines have a 'secure option'. This is not encryption and transmissions can still be intercepted. Encrypted telephones are available.

Managed Security/Secure Perimeter

This means that the security environment is maintained by some means of access control or locked outer doors which prevents and deters intruders. This should be combined with some form of guarding or intruder detection, especially when the premises are otherwise unattended.

Set clear responsibilities for operating these procedures, and regularly check that they remain effective.

Network Firewall

A network firewall is an IT system, consisting of both hardware and software, which is programmed to filter the traffic and control access between an untrusted, insecure network (e.g. the Internet) and an organisation's internal network. It should be designed and operated to be highly resilient to a very capable, malicious technical attack by hackers.

Paper

This includes:

- Printed paper
- Hand-written notes
- Computer output
- Presentation transparencies
- Flip charts
- Wall charts and maps
- Photographs
- Posters
- Videos
- Microfiche
- Physical computer media

Personnel Security Checks

The most critical aspect of protecting sensitive information is ensuring that people with authorised access to the information can be trusted. Companies can be infiltrated and staff can be coerced or influenced to disclose sensitive information.

Basic checks should be carried out for all staff with access to any sensitive information, especially at SEC2 or SEC3 levels. Measures should also be taken when employing contract, temporary, agency and consultancy staff. The following measures may be appropriate:

- seek clear proof of identity, such as a birth certificate or valid passport,
- confirm the validity of academic and employment references, and when risk is high consider other checks (eg. credit-rating, criminal convictions etc.),

- ensure a confidentiality agreement is signed.

Security Container

This is a security cabinet designed to offer a degree of resistance to an attacker using force and having access to a limited range of hand tools. The cabinet should also resist 'flexing' or other manipulation which would allow a thief to insert probes or devices to gain access. The container should be fitted with a high security lock.

Trusted Partner

This applies to a party who agrees to a legally binding agreement or contract to protect information, and where due diligence checks show the party is trustworthy. Assurance checks should indicate that they meet the minimum requirements of this guidance.

After signing the agreement both organisations should explain to each other the threats they need to protect against, since threats to one organisation are often unimaginable to another.

DTI's Information Security Policy Group aims to help business manage information security effectively.

The Group works with industry to raise awareness of information security issues, provide guidance on best practice and promote the development of solutions.

It also represents the information security interests of business at UK and international levels.

To obtain further copies of this publication and other publications on information security, contact the UK online for business infoline on 0845 715 2000.

To obtain general advice on information security, contact:

The Information Security Policy Group
Communications and Information Industries Directorate
Department of Trade and Industry
151 Buckingham Palace Road
London SW1W 9SS

Tel 020 7215 1962
Fax 020 7931 7194
Web <http://www.dti.gov.uk>

Department of Trade and Industry
© Crown Copyright
URN 00/1395