dti

ACHIEVING BEST PRACTICE IN YOUR BUSINESS

Information Security: A Business Manager's Guide

dti

The DTI drives our ambition of 'prosperity for all' by working to create the best environment for business success in the UK. We help people and companies become more productive by promoting enterprise, innovation and creativity.

We champion UK business at home and abroad. We invest heavily in world-class science and technology. We protect the rights of working people and consumers. And we stand up for fair and open markets in the UK, Europe and the world.

Achieving best practice in your business is a key theme within DTI's approach to business support solutions, providing ideas and insights into how you can improve performance across your business. By showing what works in other businesses, we can help you see what can help you, and then support you in implementation. This brochure focuses on these solutions.

This guide provides an introduction to information security for business managers. It provides help and advice so that you can start to address the issues of information security. It describes what information security is, why it's important and how to implement appropriate information security solutions. Find out how to identify the risks your business faces, and how to work out the security requirements needed to minimise them. There's also guidance on how to develop a security policy, the supporting security roles and responsibilities you should consider, and how to use best practice controls to manage your risks.

In many ways, protecting information is similar to protecting your own personal possessions and valuables. This analogy is used throughout the guide to help you understand what's involved.

Who this brochure is for: any business that wants advice and help when addressing its information security issues.

What it covers: the steps you can take to start to ensure your business information is better protected.

Contents

What is information security?

In business, having the correct information at the right time can make the difference between profit and loss, success and failure. Information security can help you control and secure information from inadvertent or malicious changes and deletions or from unauthorised disclosure.

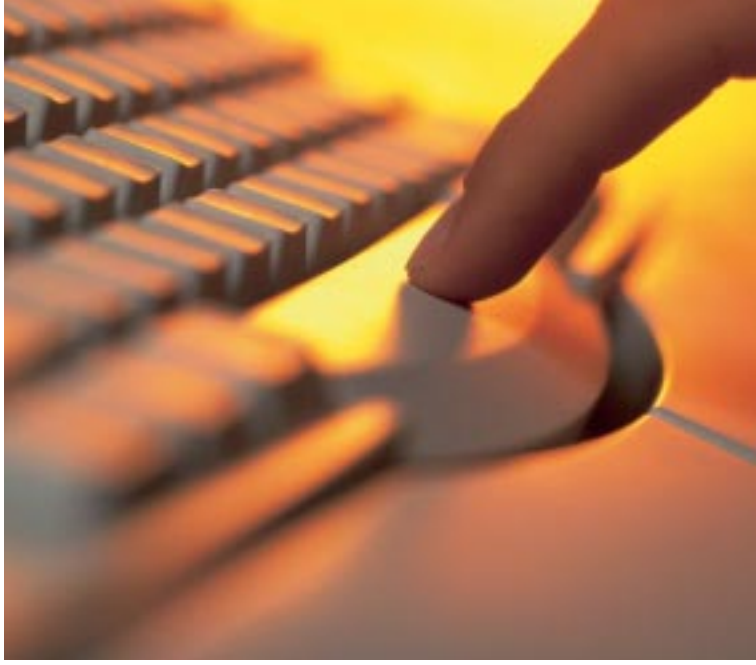
There are three aspects of information security:

CONFIDENTIALITY
Protecting information from unauthorised disclosure, perhaps to a competitor or to the press.

INTEGRITY
Protecting information from unauthorised modification, and ensuring that information, such as a price list, is accurate and complete.

AVAILABILITY
Ensuring information is available when you need it.

Ensuring the confidentiality, integrity and availability of information is essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image and branding.



What information should I protect?

You should protect all information that is sensitive, critical or is of commercial value to your organisation. Information can exist in many forms. It can be:

- printed or written on paper
- stored electronically
- transmitted by post or using electronic means
- stored on tape or video
- spoken in conversation.

We all demonstrate aspects of information security in our everyday lives. For example, we make sure that deeds and insurance documents are stored safely so that they are available when we need them. We also check that the information contained in bills or bank statements is correct.

Your company information should be treated in the same way.

Why is information security important to me?

Information is an essential resource for all businesses today; it can be the key to growth and success.

Sharing information is an increasing business activity. Your information is a key business asset that is very valuable. Its availability, integrity, and confidentiality may be critical for the continued success of your organisation. Your security can be breached in a number of ways, for example by system failure, theft, inappropriate usage, unauthorised access or computer viruses.

The impact of an information security breach may be far greater than you would expect. Not only will the loss of sensitive or critical business information directly affect your competitiveness and cash flow, it could also damage your reputation and have a long-term detrimental effect. It might take an organisation ten years to establish its reputation and image as a trustworthy and reliable business but a security breach could destroy this in a matter of hours.

Information also needs to be protected if you share it with other organisations.
For many businesses, the Internet has replaced traditional paper based ways of exchanging information. It has enabled information to be sent and received faster, more frequently and in greater volume – not just simple text but also multimedia. Today it is quite common for companies to use the Internet for exchanging information and for e-commerce.

The Internet brings its own security issues which businesses need to consider.

We automatically protect our house and valuables from unauthorised entry, theft and damage.

Your company information requires the same protection.

"It won't happen to me"

Unfortunately a security breach could happen to you and maybe it has already happened but you haven't yet experienced the impact – the effects may not be obvious immediately. As an increasingly large number of companies have found out to their cost, security incidents and breaches are quite common and are a growing problem. In the DTI's 2004 Information Security Breaches Survey, over 70% of organisations reported that they had suffered a security breach in the previous year.

Copies of the DTI's most recent Information Security Breaches Survey (which is conducted on a biennial basis) can be downloaded or ordered from the DTI's website at www.dti.gov.uk/industries/information_security

Hard copies of the survey can be ordered from the DTI's Publications Orderline on 0870 150 2500, quoting URN 04/617 (Technical Report) and URN 04/618 (Executive Summary)

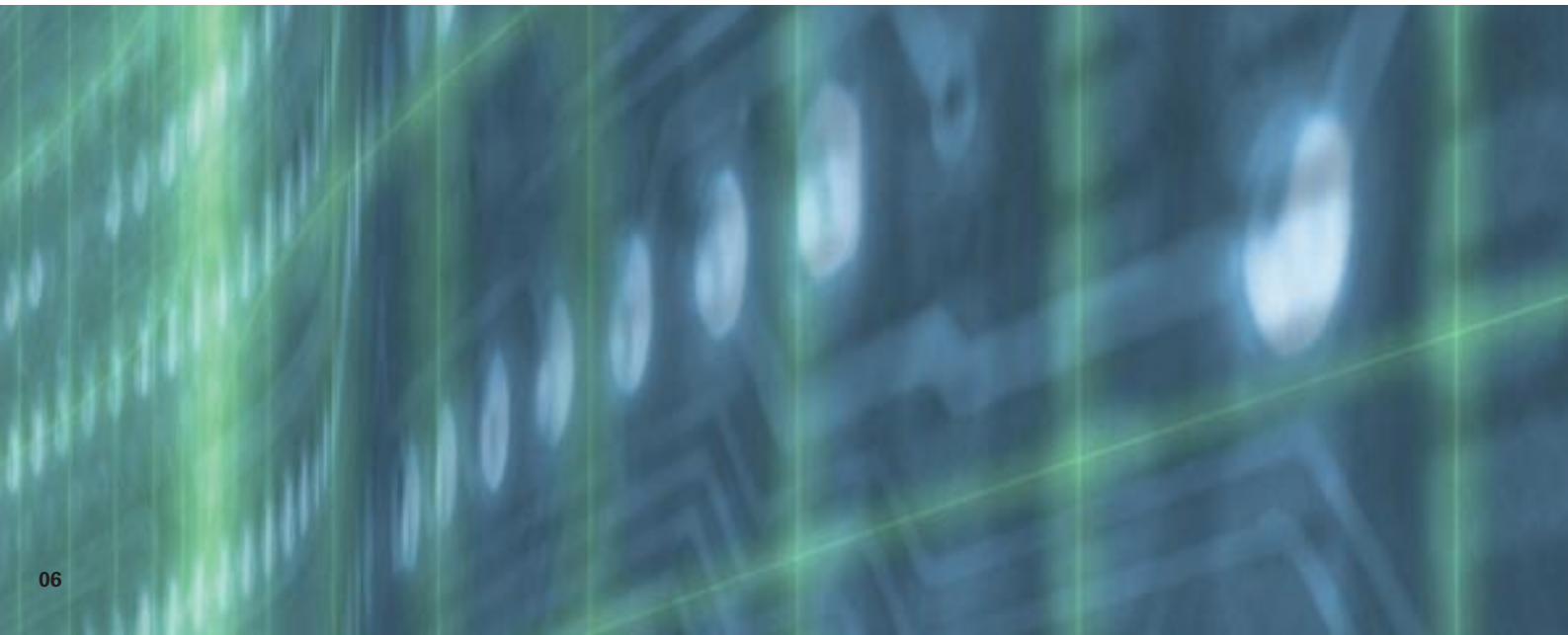
What is the best approach to provide security?

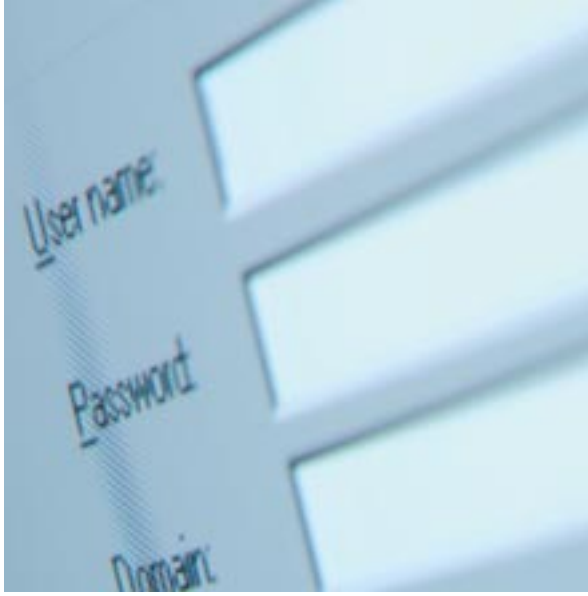
The best way of providing information security is to use a well-tried and tested approach to meet your own specific security requirements. This will ensure that you concentrate on the important areas.

The British Standard, BS 7799, helps businesses implement best practice in information security management. Part 1 of this standard is a code of practice. It was originally published in 1995 and revised in 1999. It then became an international standard ISO/IEC 17799 in 2000. This standard provides a comprehensive set of security controls comprising the best information security practices in current use by organisations across the world and in all market sectors. Its objectives are to provide organisations with a common basis for information security and to enable information to be shared between organisations.

Part 2 of BS 7799 defines a management framework for identifying security requirements and applying the best practice controls defined in ISO/IEC 17799. Part 2 defines a step-by-step process which can be used to design, implement and maintain an effective information security management system:

- **Design the management system** for protecting your information. This sets the policy and objectives of information security, assesses your security risks, evaluates the options for treating the risks, and selects controls from ISO/IEC 17799 to reduce the identified risks to an acceptable level. Spending on controls should be balanced against the value of the information and other assets at risk, and the implications of these risks for your business.





- **Implement the management system** by putting into practice the selected controls to manage the identified risks. This includes implementing suitable procedures, providing appropriate awareness and training, assigning roles and responsibilities and deploying any necessary technical controls.

- **Monitor and review the management system** to check it is still 'fit for purpose' to manage the risks the business faces. This includes monitoring how effective the controls are at managing the risks, re-assessing the risks taking account of any changes to the business, and reviewing policies and procedures.

- **Update and improve the management system** to implement changes to existing controls as well as putting into practice new controls to ensure it is maintained as 'fit for purpose'.

Both ISO/IEC 17799 and BS 7799 Part 2 can be used by any size of business in any sector, with any type of information system, whether manual or computerised.

BS 7799 – information security starting point

There are some controls in ISO/IEC 17799 which are applicable to all business environments. Of course the implementation will vary depending on the risks the business faces. These basic starting point controls include:

LEGISLATIVE REQUIREMENTS

- intellectual property rights
- safeguarding of organisational records
- data protection and privacy of personal information.

SOME COMMON PRACTICE

- information security policy document
- allocation of information security responsibilities
- information security education and training
- reporting security incidents
- business continuity management.

We protect our personal possessions and valuables based on our understanding of the risks we face. You should protect your corporate information systems using a similar systematic approach and introduce relevant countermeasures to deal with and manage the risks your business faces.

What security roles and responsibilities should I consider?

An important implementation aspect is the definition and allocation of roles and responsibilities for information security. All staff within your organisation should know who is nominated to fulfil these roles and what their own general responsibilities are in this respect. This is essential for the effective application of the organisation's information security procedures.

For example:

- **Chairman or CEO** should provide management direction and support for information security and formally approve the company's information security policy.
- An **information security policy owner** should be identified. He or she should be responsible for the publication, distribution, maintenance and review of the policy.
- **Senior management** should actively support and implement the policy within their own business areas. They should also ensure staff are aware of their responsibilities as well as security issues generally.
- An **information security manager** should ensure that the information security policy and supporting procedures are properly implemented.
- **Asset owners** should be accountable for the protection of assets in accordance with the information security policy and supporting procedures.
- **Users** should follow the information security policy and supporting procedures.

Responsibilities may vary according to the size and nature of the organisation. Some smaller businesses may not need a full-time information security manager, but nevertheless this role should be clearly defined within an employee's job description and should be put into practice in the day-to-day operation of the business. Large organisations may need to employ a team of people to support the role of a full-time information security manager.

These security roles and responsibilities should complement the business processes.

To protect our own possessions and valuables, we make sure we have effective security in place. Similarly, someone in your organisation should take responsibility for ensuring that company information is appropriately protected.

What risks do I face and what security do I need?

Inadequate security measures or procedures can result in a security breach. On the other hand, too many controls may be unduly expensive and time-consuming. Knowing the risks we face and how to manage these appropriately can enable us to:

- ensure the availability and continuity of business processes
- reduce unproductive time spent in dealing with problems
- reduce the cost of downtime and service outage
- protect the brand name and image
- protect our IPR, share value, market share, and
- avoid penalties arising from failure to comply with legal requirements.

Managers make business decisions about the risks they face on a daily basis. It is important they have sufficient information to make informed decisions and to ensure effective deployment of the organisation's resources to manage the risks.

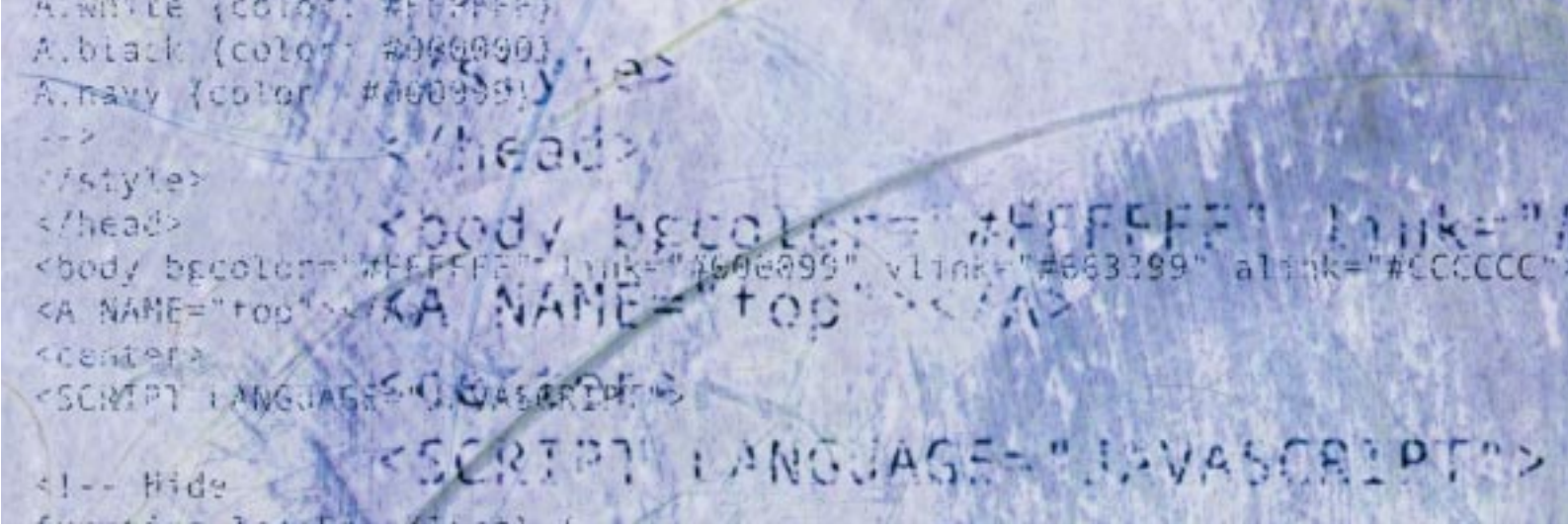
Information security risks should be identified and evaluated to assess the likely threat to the business. This will allow appropriate decisions to be taken to protect the business and to help make the best use of the organisation's resources with regard to security measures and controls.

BUSINESS ASSETS

An important first step in a risk assessment is to identify your assets and their value or importance to the business. These could be tangible assets such as people and equipment or intangible assets such as reputation and image. For example, do you know how much sensitive or critical information you have and how important it is to your business? What is the value of this information? Does it need to be protected in order to comply with legislation?

THREATS

Having identified and valued the assets, the next step is to consider the threats to these assets. You also need to consider any vulnerabilities or weaknesses in your business processes or systems which these threats could exploit. If, for instance, a laptop is left unattended there is an obvious risk of hardware or information theft if there are no access controls in place. You may face the threat of a virus attack which could damage your business systems, either through a lack of user awareness of the appropriate procedures, a lack of anti-virus protection or failure to update existing anti-virus protection.



IMPACTS

Having identified assets and threats you should then look at the possible impact to your business if the worst happens. If your sensitive or critical information were lost or damaged could you recover it and how much would that recovery cost? If a back up of the information were kept then the cost of recovery would be minimal. If no backup is in place, what is the cost of reproducing this information? In addition there could be a cost resulting from the theft and/or misuse of information. To take the example of the laptop, the stolen information could be sold to a competitor resulting in a possible loss of revenue and a subsequent downturn in profit. Awareness of such an impact provides a measure of both how important the asset is to your business and the level of the protection that should be considered.

CONTROLS

Using this information, you can then determine the level of security necessary to protect your assets and to ensure effective use of your organisation's resources. This should result in an appropriate system of controls and procedures.

All organisations depend on information to drive their business processes. Much of this information is stored and processed on computers and exchanged over public networks. Information processing technology has revolutionised the world of business, opening up new ways of working, particularly e-commerce.

E-commerce means that you will need to consider and assess the level of risk involved in linking up with a third party such as a trading partner. The DTI publication 'Information Security: Business Assurance Guidelines' provides more detailed advice. Copies of this and other publications can be downloaded or ordered from the DTI website at www.dti.gov.uk/industries/information_security. Alternatively, copies can be ordered from the DTI's Publications Orderline on 0870 150 2500, quoting URN 04/625.

We all make a form of risk assessment when we decide how to protect our personal property and possessions. We start by identifying what needs to be protected and its value and importance to us. We then evaluate the threats that we may face from thieves, vandals and the environment and we make a decision about the necessary steps to take to provide appropriate protection.

How do I develop my information security policy?

Management should set clear policy direction and provide support for information security by means of an information security policy. Such a policy needs to be issued across the organisation and should be reviewed and maintained on a regular basis.

It should complement the organisation's mission statement and reflect the desire of the business to operate in a controlled and secure manner.

As a minimum the information security policy should include guidance on the following:

- The definition of information security – scope, objectives and importance to the business.
- A statement of intent from management supporting the goals and principles of information security.
- Brief explanation and statements indicating minimum standards, procedures, requirements and objectives of particular importance to the business:
  - consequences of security policy violations
  - legal, regulatory and contractual compliance and obligations
  - security awareness and educational requirements
  - prevention and detection of viruses and other malicious software
  - business continuity planning.
- Definitions of general and specific roles and responsibilities for information security.
- Details of the process for reporting, responding to and resolving security incidents.
- References to supporting documentation, such as more detailed security policies, procedures, implementation guides or security specifications and standards.

An example of a corporate information security policy is set out opposite.

Information Security Policy Statement

OBJECTIVE

The purpose and objective of this Information Security Policy is to protect the company's information assets (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

POLICY

- The Chief Executive Officer has approved the Information Security Policy.
- It is the Policy of the [company] to ensure that:
  - a Information will be protected from a loss of: confidentiality (note 2), integrity (note 3) and availability (note 4).
  - b Regulatory and legislative requirements will be met (note 5).
  - c Business continuity plans will be produced, maintained and tested (note 6).
  - d Information security training will be available to all staff.
  - e All breaches of information security, actual or suspected, will be reported to, and investigated by, the Information Security Manager.
- Guidance and procedures will be produced to support this policy. These may/will include incident handling, information backup, system access, virus controls, passwords and encryption.
- The role and responsibility of the designated Information Security Manager (note 7) is to manage information security and to provide advice and guidance on implementation of the Information Security Policy.
- The designated owner of the Information Security Policy [name] has direct responsibility for maintaining and reviewing the Information Security Policy.
- All managers are directly responsible for implementing the Information Security Policy within their business areas.
- It is the responsibility of each employee to adhere to the Information Security Policy.

NOTES

1 Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation.
2 Confidentiality: ensuring that information is accessible only to authorised individuals.
3 Integrity: safeguarding the accuracy and completeness of information and processing methods.
4 Availability: ensuring that authorised users have access to relevant information when required.
5 This includes the requirements of legislation such as the Companies Act, the Data Protection Act, the Computer Misuse Act and the Copyright, Design and Patents Act.
6 This will ensure that information and vital services are available to users whenever they need them.
7 Depending on the size and nature of the business this may be a part or full-time role for the nominated person.

Signed _____ Title _____ Date _____

(The Policy will be reviewed by the designated owner of the Information Security Policy, typically not more than 1 year from the date signed)

How do I provide security solutions?

Assessing security risks was covered in the section 'What risks do I face and what security do I need?' on p 10. In this section we give some examples of the security solutions you need to consider to help reduce your security risks to an acceptable level.

A good basis for selecting a system of security controls is ISO/IEC 17799. The following are examples of some of the controls you should be considering to implement information security.

BEST PRACTICE FOR INFORMATION SECURITY

Information security policy document

The section on 'How do I develop my information security policy?' on page 12 of this booklet provides advice on this.

Allocation of information security responsibilities

The section 'What security roles and responsibilities should I consider?' on page 9 of this booklet covers this.

Information security education and training

You should provide all employees of the organisation and, where relevant, third party users (such as on-site contractors), with appropriate training. Users should be suitably trained to support the Information Security Policy, as well as the company's security procedures and the correct use of its business processes and systems. They should also receive training on the use of correct information processing facilities such as log-on procedures and policy on the use of software packages, before access to information, systems or services is granted. Employees should understand why security is important, what the company's policies are, and their own responsibilities.

Reporting of security incidents

You will need to provide guidance on the actions that should be taken following any security incident, including procedures for reporting and responding to such incidents. This topic should also be included in your Information Security Policy and appropriate education and training should be given.

Business continuity management

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures, whether these are natural incidents such as equipment failures or malicious incidents such as large scale network attacks. To reduce these risks to an acceptable level you will need a combination of corrective, preventative and recovery controls. An analysis of the consequences of a disaster, system failure, major security breach and/or severe loss of service would then need to be undertaken.

You should develop and implement contingency plans to ensure that business processes can be restored within the required timescales. You should maintain, test and practice such plans in order to ensure that they become an integral part of your management processes.

You will find that the identification of your security risks discussed in the section titled "What risks do I face and what security do I need?" on page 10 will help you to identify the vital business functions that you would need to maintain following a disaster.

If, for example, an assessment of your home has identified a high level of risk, whether because of the high incidence of local robberies or perhaps because you are often away from home, you may well decide to install a burglar alarm. You will then need to

decide on the system best suited to your requirements, and you will need to find a reputable supplier who can provide you with an effective system and appropriate after sales care. Your organisation should be subject to the same form of risk assessment so that you can decide on the proper level of protection.

ESSENTIAL CONTROLS FROM A LEGISLATIVE POINT OF VIEW

Intellectual property rights (IPR)

You will need to implement appropriate procedures to ensure compliance with legal restrictions such as copyright, design rights, patents or trade marks. Copyright infringement can lead to legal action that may involve criminal proceedings.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, this may mean that only material that is licensed or provided by the developer can be used. Proprietary software products are usually supplied under a licence agreement that limits the use of those products to specified machines and may limit copying to the creation of back-up copies. Your Information Security Policy will need to have adequate mechanisms in place to ensure that all staff comply with the legal requirements on intellectual property. You should introduce a policy requiring all staff to comply with software licences.

Safeguarding of organisational records

You will probably find that you are doing much of this as part of your compliance with the Companies Act. You should, however, ensure that organisational records held on a computer also comply with the Act.

Data protection and privacy of personal information

The processing and transmission of personal data is subject to legislative controls. Principle 7 of the 1998 Data Protection Act (DPA), requires organisations to demonstrate to the Information Commissioner that adequate mechanisms are in place to prevent unauthorised/unlawful processing, or accidental loss or damage to personal data. The Act came into force on 1 March 2000.

Further guidance on how the security requirements of the 1998 DPA can be met is described in a separate DTI publication titled 'Information Security: BS7799 and the Data Protection Act'. You can download or order a copy from the DTI web site at www.dti.gov.uk/industries/information_security or alternatively you can phone the DTI's Publications Orderline on 0870 150 2500, quoting URN 04/621.

Further help and advice

INFORMATION SECURITY ISSUES

For help and advice on information security issues contact:

The Information Security Policy Team
Department of Trade and Industry
151 Buckingham Palace Road
London SW1W 9SS
Tel: 020 7215 1962
Fax: 020 7215 1966
E-mail: InfosecPolicyTeam@dti.gsi.gov.uk

Further guidance and full listing of all our information security publications can be found at: www.dti.gov.uk/industries/information_security

Or look at our information security business advice pages at: www.dti.gov/uk/bestpractice/infosec

For information on data protection, contact
The Information Commissioner's Office
Wycliffe House
Water Lane,
Wilmslow
Cheshire SK9 5AF
Tel: 01625 545 745
Fax: 01625 524 510
Web site:
www.informationcommissioner.gov.uk
Email: mail@ico.gsi.gov.uk

SUPPORT TO IMPLEMENT BEST BUSINESS PRACTICE

To get help bringing best practice to your business, contact Business Link – the national business advice service. Backed by the DTI, Business Link is an easy-to-use business support and information service, which can put you in touch with one of its network of experienced business advisers:

- Visit the Business Link website at www.businesslink.gov.uk
- Call Business Link on 0845 600 9 006.

ACHIEVING BEST PRACTICE IN YOUR BUSINESS

Achieving best practice in your business is a key theme within DTI's approach to business support solutions, providing ideas and insights into how you can improve performance across your business. By showing what works in other businesses, we can help you see what approaches can help you, and then support you in implementation.

To access free information and publications on best practice:

- visit our website at www.dti.gov.uk/bestpractice
- call the DTI Publications Orderline on 0870 150 2500 or visit www.dti.gov.uk/publications

GENERAL BUSINESS ADVICE
You can also get a range of general business advice from the following organisations:

England
- Call Business Link on 0845 600 9 006
- Visit the website at www.businesslink.gov.uk

Scotland
- Call Business Gateway on 0845 609 6611
- Visit the website at www.bgateway.com

Wales
- Call Business Eye/Llygad Busnes on 08457 96 97 98
- Visit the website at www.businesseye.org.uk

Northern Ireland
- Call Invest Northern Ireland on 028 9023 9090
- Visit the website at www.investni.com

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