



**dti**

**ACHIEVING BEST PRACTICE  
IN YOUR BUSINESS**

Information Security:  
BS 7799 and the  
Data Protection Act



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.

The Data Protection Act makes it a legal requirement for businesses to collect, hold and process personal data in a secure way. It outlines important principles for safeguarding information about people.

**This brochure is for:** All businesses that hold and use personal data.

**It covers:** The benefits of information security and how BS 7799 can contribute towards meeting the requirements of the Data Protection Act.



# The 1998 Data Protection Act

## Have you considered using BS 7799?

Information and people are probably the most important business assets in any organisation. The 1998 Data Protection Act came into force on 1 March 2000 and means you are obliged to ensure that information held about people is adequately protected. The Data Protection Act concerns personal data, i.e. information about living, identifiable individuals ('data subjects') and details important principles for the security of such information.

Businesses have to be open about their use of personal data, and follow sound and proper practices in how they treat it. By implementing good information security practice, businesses are better equipped to keep their information accurate and up to date. They can also ensure it is accessed by the right people, and in a secure way. If the security of your information is compromised, it can cost your business a great deal – financially and in terms of reputation.





# Increased security implications of the 1998 Data Protection Act

## **SCOPE AND SECURITY PRINCIPLES**

At the heart of the legislation is a set of eight principles. Good information security practice is implied in all eight, but explicitly in Principle 7, which relates to the prevention of unauthorised or unlawful processing, and of accidental loss or damage to data. It requires that organisational as well as technical means be used to protect personal information. It also requires that a security regime must be technologically up to date. All organisations have to comply with the eight principles.

## **RECORDS**

The 1998 Data Protection Act applies to computerised records, as well as to certain manual records involving personal information.

## **NOTIFICATION**

If you register under the Data Protection Act 1998, you will be asked to fill in a security statement to help the Information Commissioner decide whether you are likely to satisfy the requirements of Principle 7 of the Act.

# International and British Standards on Information Security Management

ISO/IEC 17799 is the international standard for information security management. It provides best practice across a wide range of business requirements.

Its companion standard, BS 7799 Part 2, specifies an Information Security Management System (ISMS). This can help your business

develop, implement and maintain effective information security – it is effectively a framework for following the best practice in ISO/IEC 17799.

ISO/IEC 17799 and BS 7799 apply to all information regardless of where it is located and processed, or how it is stored.





The standards outline a number of key principles:

- The use of risk assessment – identifying and evaluating risks, and specifying appropriate security controls to help minimise loss or damage associated with these risks
- Periodic reviews of security and controls – this accounts for any changes that have taken place in your business, as well as identifying new threats and vulnerabilities
- Taking steps to implement information security – some are essential from a legislative point of view (such as data protection, privacy of personal information and safeguarding organisational records) whilst others are best practice recommendations (such as business continuity management, and information security awareness and training).



# Implementing an ISMS

To implement an ISMS, you will need to follow four steps:

## Step 1: Design the ISMS

At this stage, you would determine your policy and objectives regarding information security, assess your security risks, evaluate various ways of handling these risks, and select controls from the ISO/IEC 17799 standard that reduce risks.

Remember to compare the cost of risk control against the value of the information and other risks to your business.

## Step 2: Implement the ISMS

Put the selected controls in place to manage risks. This would involve setting up procedures and instructions for staff, raising awareness through training, assigning roles and responsibilities, and implementing any new systems.

## Step 3: Monitor and review the ISMS

This will help you ensure that the ISMS continues to manage the risks to your business data. This includes monitoring how effective the controls are in reducing the risks, re-assessing the risks taking account of any changes to the business, and reviewing policies and procedures.

## Step 4: Improve the ISMS

Maintain your system by improving existing controls, as well as putting into practice new controls.

## NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE

Any organisation, which has an Information Security Management System (ISMS) in place, should be in a good position to respond positively to questions which the Information Commissioner's Office may ask in the notification procedure.

# Considerations

ISO/IEC 17799 and BS 7799 Part 2 standards can be used by businesses of any size and in any sector that make use of information systems.

Though they won't make your business immune from security breaches, they do make them less likely and give you more control over possible risks. You will also be in a better position to minimise damage, cost and disruption if security breaches do occur.

The use of ISO/IEC 17799 and BS 7799 can help businesses to meet the information security requirements of the Data Protection Act.

## **ARE ISO/IEC 17799 AND BS 7799 FOR YOU?**

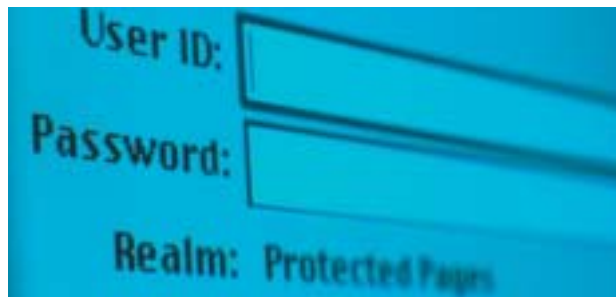
The DTI's own Information Security Breaches Surveys have regularly highlighted the costs to business of security breaches. Nor is it just a financial cost either; breaches disrupt the normal operations of a business and can impact on reputation and consumer and supplier confidence.

The DTI's more recent surveys have found that too few UK businesses have documented procedures to help them comply with the 1998 Data Protection Act. This could

indicate that a significant proportion of businesses are unaware of their data protection responsibilities, or maybe they see compliance as a low business priority. (Copies of the DTI's Information Security Breaches Surveys are available to download or order from the DTI website – see Page 8 for details).

There are distinct advantages to be gained by identifying and protecting the assets of a business. The advantage of using ISO/IEC 17799 and BS 7799 is that they are business-led best practice on information security management, providing ready-made guidance and processes for managing risks to information security.

As well as helping to satisfy the information security requirements of the 1998 Data Protection Act, third party certification can demonstrate to trading partners and the Information Commissioner that your business is compliant with BS 7799 Part 2.



# 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](mailto:InfosecPolicyTeam@dti.gsi.gov.uk)

Further guidance and a full listing of all our information security publications can be found at:  
[www.dti.gov.uk/industries/information\\_security](http://www.dti.gov.uk/industries/information_security)

Or look at our information security business advice pages at:  
[www.dti.gov.uk/bestpractice/infosec](http://www.dti.gov.uk/bestpractice/infosec)

For information about the UK ISO/IEC 17799 Users' Group, e-mail the DTI at:  
[isoiec17799usersgroup@dti.gsi.gov.uk](mailto:isoiec17799usersgroup@dti.gsi.gov.uk)

For information on the ISMS International Users' Group and the International Register of accredited BS 7799 Part 2 certificates: [www.xisec.com](http://www.xisec.com)

## For information on data protection:

The Information Commissioner's Office  
Wycliffe House,  
Water Lane,  
Wilmslow,  
Cheshire SK9 5AF  
Tel: 01625 545 745  
Fax: 01625 524 510  
E-mail: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)  
Website:  
[www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

## For detailed information on BS 7799 and ISO/IEC 17799:

British Standards Institute,  
389 Chiswick High Road,  
London W4 4AL  
Tel: 020 8996 9001  
Fax: 020 8996 7001  
E-mail: [cservices@bsi-global.com](mailto:cservices@bsi-global.com)  
Website: [www.bsi-global.com](http://www.bsi-global.com)

## For information on certification:

The United Kingdom Accreditation Service (UKAS),  
21-47 High Street,  
Feltham,  
Middlesex TW13 4UN  
Tel: 020 8917 8400  
Fax: 020 8917 8500  
E-mail: [info@ukas.com](mailto:info@ukas.com)  
Website: [www.ukas.com](http://www.ukas.com)

## **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](http://www.dti.gov.uk/bestpractice)
- call the DTI Publications Orderline on 0870 150 2500 or visit [www.dti.gov.uk/publications](http://www.dti.gov.uk/publications)

## **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](http://www.businesslink.gov.uk)
- Call Business Link on 0845 600 9 006

## **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](http://www.businesslink.gov.uk)

### **Scotland**

- Call Business Gateway on 0845 609 6611
- Visit the website at [www.bgateway.com](http://www.bgateway.com)

### **Wales**

- Call Business Eye/Llygad Busnes on 08457 96 97 98
- Visit the website at [www.busesseye.org.uk](http://www.busesseye.org.uk)

### **Northern Ireland**

- Call Invest Northern Ireland on 028 9023 9090
- Visit the website at [www.investni.com](http://www.investni.com)

