Data Protection Good Practice Note
Security of personal information

Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

This good practice note aims to alert small and medium sized organisations to the security measures they should have in place to protect the personal information they hold. The Data Protection Act 1998 (the Act) requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage.

It is not intended, and cannot be, a comprehensive guide to all aspects of security in all circumstances and for all organisations. The British Standards Institute (BSI) has an information assurance standard that can be tailored to individual circumstances. The Department for Business, Enterprise and Regulatory Reform have also produced guides and checklists which will help you to tailor your security measures to your needs. Their contact details are at the end of this note. However, this good practice note includes guidance on what the Act requires in terms of security and takes into account our experience of where problems often occur.

The situation

We recognise that some organisations, particularly those of a smaller and medium size, are less likely to have available internal security expertise. This guidance aims to help them decide what approach they should take about the security of the personal information they have.

Recommended good practice

The following information is intended to act as a guide or prompt to consider what action is appropriate in the circumstances of the organisation concerned to protect the personal information they hold.

1 What have you got? How valuable or sensitive is it?

One of the **first** things any organisation will need to do is to review what personal information they control, whether they actually process the information, or whether this is carried out by someone acting on their behalf.

- How valuable, sensitive or confidential is the information?
- What damage or distress could be caused to individuals if there was a security breach?

- What effect would a security breach have on your organisation? In cost? To your reputation? To the trust of your customers or clients?

This will help you assess what security measures you need to have in place.

> **For example:**
> If you only have information that is publicly available then your security measures will focus more on protecting your premises, equipment, and any interruption of business a security breach could cause. If you have highly sensitive or confidential personal information, for example, about people's health or finances that could cause them damage or distress if this information fell into the hands of others, you will need to concentrate on any potential threat to the information and the vulnerabilities of your security measures.

2 Who is in charge?

Someone in an organisation has to have day-to-day responsibility for security measures, whether this is discussing with senior colleagues what measures should be adopted, writing procedures for staff to follow, organising training for staff, checking whether they are following procedures and that the measures work, monitoring change or investigating a security incident. Otherwise it will not get done and your security will quickly become flawed and out of date.

3 Security measures

What security you need will depend on your own circumstances. This will include the personal information you have and how you need to use it for your business, your premises, computer systems, how many staff you have and what access they have to personal information and so on. You will need to consider the following subjects in the light of this.

A Organisational measures.

You will need to decide what organisational changes you need to make, if any.

- Has a risk assessment been carried out that takes account of what it is you need to protect, the type of security problems that could occur, the effectiveness of your current security measures? This should then inform what changes you are going to make.
- Does the person with responsibility for security have the standing and resources to make sure the job gets done? Any security manager needs backing from the top.
- Do you have an overall security policy?
- Are there security procedures in place for staff to follow?

- Is there co-ordination between key people in the organisation? For example, the security manager will certainly need to know about the commissioning and disposal of any new IT equipment.
- Are checks made that people are taking their security responsibilities seriously?
- Is there a procedure to make sure security incidents are investigated and lessons are learned?
- Is access given to anyone outside the organisation, for example, for computer maintenance? Are you clear about what they need access to and why, and what security you need to have in place to oversee what they do?
- **Using another organisation to process personal information** is a situation that often causes security problems. You need to be very careful about this because you take the legal responsibility for what they do with the personal information they handle for you. For example, you could receive claims for compensation under the Act from someone who has suffered damage as a result of their lack of security. And if you use another organisation to process personal information for you there are steps laid down in the Act which you must take.

    - You must choose an organisation that offers you guarantees about the security of the processing they will do for you.

    - You must have a written contract with them that sets out what you allow them to do with the information. At a minimum you would expect the contract to be clear about their use and disclosure of the information. The contract must also require them to have in place security measures that are the equivalent of those you would need if you were doing the job for yourself.

    - You must take reasonable steps to check that the organisation is taking those security measures.

- Have you made business continuity arrangements that identify how to protect and recover the personal information you hold?
- Do you check your compliance with legal obligations such as copyright or licensing requirements?
- Do you do periodic checks of your security arrangements to make sure that they are still appropriate and up to date?

B Staff

Analysis of security incidents show a high proportion are staff related so this is an important area to consider. The Act also requires you to take reasonable steps to ensure the reliability of employees that have access to personal information.

- Do you take reasonable steps at the recruitment stage to check the identity and reliability of your staff? For example, by getting references and checking that these and the person's qualifications are valid.

- Do you lay down in your employment contract or in a confidentiality agreement what staff can and cannot do with the personal information they handle?
- Do you train your staff in their responsibilities about the personal information you process? For example, do you make it clear if information is confidential and the restrictions on how this should be used?
- Are staff aware of the dangers of someone trying to trick them into making disclosures of information or changing an address when they should not do this because the enquirer is not who they say they are? Do they know the proper procedures to use to identify callers? Do you warn your staff about possible 'phishing' attacks (which is a similar type of attack via email) so they know not to get taken in by these deceptions?
- Do they know they can commit a criminal offence if they deliberately give out personal information without your consent? The guidance we produce on training staff and our video/DVD 'The lights are on' may help you with this. Do they know that they can commit a criminal offence if they try to access or obtain personal information without your authority?
- Are staff told what personal use they can make of the computers or phones? While you may not mind them making some personal use of your computers, you may want to consider if there are restrictions you want to put on their use to avoid, for example, virus infection, spam, or visiting sites where illegal material such as pornography may be seen.

C Physical security

A lot of emphasis is put on technical security measures to protect computerised information – and rightly so. However, many security incidents relate to the theft of laptops or briefcases or abandoning paper-based material or computers. So physical security is just as important.

- How secure are your premises? Are there good quality doors and locks? Do you have an alarm? Is the exterior well lit?
- Do you lock up paper based personal information at night?
- Are you on the ground floor and additionally vulnerable? Do you need to prevent people being able to see your computers and screens from outside?
- Do you control access to your premises? Are visitors supervised or kept only to certain public areas?
- Do you lock up your laptops and other portable equipment and computer media like discs or memory sticks at night?
- Do you dispose of paper waste containing personal information securely? For example, by shredding.

D Computer security

Your computer security will need to be appropriate to the extent of your system and what you use it for. The Act requires that organisation should take into account technological developments when they decide on security measures but it is a frequent misunderstanding that the Act requires 'state of the art' technology. This is not the case. The Act specifically allows organisations to take cost into account. But the measures you take must be appropriate for the harm that could result and the nature of the information you process.

A networked system will need more controls than a stand-alone computer. A stand-alone that is connected to the internet and email will need more protection than one that is not. This is because of the greater vulnerabilities and threats networking and connection to the internet poses. Taking into account the nature of the information will also affect what security controls you need to adopt. You can use tools such as the BERR security checklist to help you but, depending on the sophistication of your system and the technical expertise available to you in-house, you may well need specialist information security advice. Remember that you will need a contract with these advisers if they are going to have access to the personal information you have on the system.

You should consider whether you have sufficient security arrangements to manage the system securely. Here are some prompts for you to consider what action is right for your organisation.

- How do you manage the operation of your computer systems? Is this done with procedures and by documenting change or is it on ad-hoc basis? Do you have checks and balances in the job roles to help prevent unauthorised changes or even fraud?
- If you have servers they will need extra security and you will need to limit access to them. You will probably need specialist security help to address these security needs. There is advice on this topic at the government and business sponsored website http://www.getsafeonline.org/nqcontent.cfm?a_id=1099
- Do you have protection against the possible loss of information because the power supply fails? Do you make sure your equipment is properly maintained to prevent against loss or interruption to your work?
- Do you control the access to your computer systems? Do staff have their own password and only use the system using their own and no-one else's? Do you require a password strength that will not be easily broken? If you have information that only certain people should see, do you control access to it? For example, by setting the privileges to certain parts of your network? How do you control access to your computers when they are unattended?
- Do you regularly get the security updates for your software that fix any vulnerability that has been discovered?

- Do you have laptops and portable media (such as memory sticks, disks or so on) containing personal information that could be taken out of the office? Are they transported securely and with your permission? How sensitive is the information? Could it cause damage or distress to the people concerned? Are hard disks or individual documents encrypted to keep the information secure? Is the encryption product you are using of a good quality? Please see our approach to encryption at 'Our views' at http://www.ico.gov.uk/

  You may also find the information sources at the end of this note helpful.

- Do you have procedures to securely delete information held on computers? Information can be recovered even if someone thinks they 'deleted' it using the delete button. Securely deleting information will mean using techniques like overwriting the material a number of times or, if you are getting rid of the equipment, destroying the hard disk. Getting rid of equipment containing personal information without securely removing or destroying the information on it is a frequent reason for a security breach.
- Do you take back ups of the information you hold? How often? Are they stored in a different location so that if, for example, you have a fire, your information is recoverable? Do you test recovering information from your back ups to see if it works?
- Do you use the internet or email? If you do, then you need to review your security measures carefully to detect and protect against malicious software that could be downloaded onto your system. You should make sure your firewall and virus protection is kept up to date. Do you have procedures and systems in place to use if your computers do become infected or are hacked into? Do you warn your staff about the insecurity of email and make sure that any sensitive information sent electronically is encrypted or sent by other means?
- If you trade electronically have you taken proper steps to make sure any personal information that is obtained is protected from being disclosed or changed? Do you have the means to check that someone is who they claim to be, for example, by use of log on details and passwords?

More information

The following is a list of helpful sources of information about security. They do not reflect any form of endorsement but may provide information or services that you may find useful. This is not an exhaustive list and you should research companies and products carefully before buying goods or services.

The Department for Business, Enterprise and Regulatory Reform has very useful general advice on security, with further references for greater detail at http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html

And more advice for small and medium sized businesses at
http://www.berr.gov.uk/sectors/infosec/

Their health check tool is at http://www.securityhealthcheck.berr.gov.uk/

They are also developing an interactive e-learning package on security awareness which aims to be both practical and appealing. Please visit www.bobs-business.co.uk

Getsafeonline, which is sponsored by HM government and business, has more advice for small businesses about being safe on line at
http://www.getsafeonline.org/nqcontent.cfm?a_id=1046

Other information on security from the Cabinet Office unit, the central sponsor for Information Assurance, can be found at
http://www.cabinetoffice.gov.uk/csia.aspx

You can also find information about the UK's first ever quality award scheme that makes sure off-the-shelf IT security products do what they say on the label at
http://www.cabinetoffice.gov.uk/csia/claims_tested_mark.aspx

Microsoft bring out regular security updates for software and a newsletter with information about the latest scams or threats and how to avoid them.

Microsoft security for technical users
http://www.microsoft.com/technet/abouttn/default.mspx

Microsoft security for home computer users
Microsoft@newsletters.microsoft.com

There is **an international standard** for information security management, ISO 27001. This takes an information security management system approach which makes sure that security is maintained on a continuous basis.
For more information see http://www.27001-online.com

A further contact is the British Standards Institute (BSI**)**
BSI
389 Chiswick High Road
London W4 4AL
Phone: 0208 995 7799
Fax: 0208 996 6411
Website: www.bsi-global.com

If you need any more information about this or any other aspect of data protection, please contact us.

Phone: 08456 30 60 60
01625 54 57 45

E-mail: please use the online enquiry form on our website

Website: www.ico.gov.uk