

## **Security of ICT Systems– Keep safe!**

---

### **ASSIGNMENT OBJECTIVES**

In this assignment you are to provide evidence that you can:

- Understand potential breaches of security and the need to protect data in ICT-based systems
- Know how to protect the data of individuals and organisations using appropriate security measures.

---

### **TASK INTRODUCTION**

You have been asked to review the security of the school's network as some intrusions to the system have recently been made. You need to present your work in a report format.

---

### **TASK 1 (P1)**

In the first part of your report, explain and describe using examples the types of security breaches, their possible causes (why) and impact (consequences).

You need to find at least four examples that can be out of school context (shop, bank...)

---

### **Shop**

Security breaches	Causes	Impact	Legislation	ICT system
unauthorized removal of data	accidental, malicious, system issues	loss of confidence, loss of profit and theft.	Data Protection Act 1998	standalone PCs

### **Bank**

Security breaches	Causes	Impact	Legislation	ICT system
leading to identity theft	accidental, malicious, negligent; system issues, hacking	due to downtime, data loss, loss of confidence, identity theft, loss of money.	Crime and Security Act 2001	internet enabled systems

### **Doctor surgery**

Security breaches	Causes	Impact	Legislation	ICT system
damage to physical systems	incorrect installation, configuration, operation; viruses, spyware	physical loss of equipment; security audits; contingency plans and disaster recovery	Crime and Security Act 2001	networked PCs

### **Home**

Security breaches	Causes	Impact	Legislation	ICT system
unauthorized removal of data	email viruses, worms, macro viruses, Trojans	contingency plans and disaster recovery	Computer Misuse Act 1990	standalone PCs

## **TASK 2 (P2)**

In the second part, describe what a school/company needs to do to meet the current legislation and protect their data and ICT system.

For this you need to list the current laws (short summary) and explain how to conform to them in the school context.

### **Computer Misuse Act (1990)**

The Computer Misuse Act became law in August 1990. Under the Act hacking and the introduction of viruses are criminal offences. Universities and colleges need to co-operate to take action under the Act as the offences are likely to be committed by members of universities and colleges, students in particular, and are often perpetrated on machines or networks within the sector. For offences committed within the higher education sector institutions may wish to use the speedier process of internal disciplinary measures rather than resort to the law. The aim of this Guidance is to ensure that universities recognize the seriousness of these offences and to encourage a greater degree of common practice in dealing with the people who carry out these actions, whether action is taken under the criminal law or through the use of disciplinary procedures.

Ref: <http://www.lancs.ac.uk/iss/rules/cmisuse.htm>

### **The Copyright, Design and Patents Act (1988)**

The Copyright, Designs and Patents Act 1988, is the current UK copyright law. It gives the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used. The rights cover: Broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public. In many cases, the creator will also have the right to be identified as the author and to object to distortions of his work.

Ref: [http://www.copyrightservice.co.uk/copyright/uk\\_law\\_summary](http://www.copyrightservice.co.uk/copyright/uk_law_summary)

### **Data Protection Act (1998)**

- Personal data must be obtained fairly and lawfully. The data subject should be informed of who the data controller is (the institution); who the data controller's representative is; the purpose or purposes for which the data are intended to be processed; and to whom the data will be disclosed. For students this is done by the University during registration. Personal data processing may only take place if specific conditions have been met- these include the subject having given consent or the processing being necessary for the legitimate interests of the data controller. Additional conditions must be satisfied for the processing of sensitive personal data, that relating to

ethnicity, political opinion, religion, trade union membership, health, sexuality or criminal record of the data subject.

- The new Act covers personal data in both electronic form and manual form (e.g. paper files, card indices) if the data are held in a relevant, structured filing system
- Personal data processing must be in accordance with the purposes notified by the University to the data protection commissioner- if any 'new processing' is to take place the Data Protection Representative, must be consulted
- Personal data must be kept accurate and up to date and shall not be kept for longer than is necessary
- Appropriate security measures must be taken against unlawful or unauthorized processing of personal data and against accidental loss of, or damage to, personal data. These include both technical measures, e.g. data encryption and the regular backing-up of data files and organizational measures, e.g. staff data protection training
- Personal data shall not be transferred to a country outside the European Economic Area unless specific exemptions apply (e.g. if the data subject has given consent) this includes the publication of personal data on the internet

Ref: <http://www.dpa.lancs.ac.uk/summary.htm>

## **Official Secrets Acts (1911-1989)**

### **Computer Misuse Act**

The Computer Misuse Act was introduced in 1990 to secure computer material against unauthorized access or modification. Three categories of criminal offences were established to cover the following conduct:

1. Unauthorized access to computer material (basic hacking) including the illicit copying of software held in any computer.
  - Penalty: Up to six months imprisonment or up to a £5,000 fine.
2. Unauthorized access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking.
  - Penalty: Up to five years of imprisonment and an unlimited fine.
3. Unauthorized modification of computer material, which includes:
  1. Intentional and unauthorized destruction of software or data.
  2. The circulation of "infected" materials on-line.
  3. An unauthorized addition of a password to a data file.
    - Penalty: Up to five years of imprisonment and an unlimited fine.

### **You must not:**

- **Display any information which enables others to gain unauthorized access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate hacking).**
- **Display any information that may lead to any unauthorized modification of computer materials (such modification would include activities such as the circulation of "infected" software or the unauthorized addition of a password).**
- **display any material which may incite or encourage others to carry out unauthorized access to or modification of computer materials**

Ref: <http://www.mmu.ac.uk/services/isu/network/legislation.html>

### **The Police and Criminal Evidence Act (1984)**

The Police and Criminal Evidence Act (PACE) and the PACE Codes of Practice provide the core framework of police powers and safeguards around stop and search, arrest, detention, investigation, identification and interviewing detainees.

PACE sets out to strike the right balance between the [powers of the police](#) and the rights and freedoms of the public. Maintaining that balance is a key element of PACE.

Ref: <http://police.homeoffice.gov.uk/operational-policing/powers-pace-codes/pace-code-intro/>

### **Crime and security act 2001**

The **Anti-Terrorism, Crime and Security Act 2001** was formally introduced into the Parliament of the United Kingdom on 19 November 2001, two months after the terrorist attacks on New York on 11 September. It received royal assent and came into force on 14 December 2001. Many of its measures are not specifically related to terrorism, and a Parliamentary committee was critical of the swift timetable for such a long Bill including non emergency measures.

On 16 December 2004 the Law Lords ruled that Part 4 was incompatible with the European Convention on Human Rights, but under the terms of the Human Rights Act 1998 it remained in force. It has since been replaced by the Prevention of Terrorism Act 2005.

Ref: [http://en.wikipedia.org/wiki/Anti-terrorism,\\_Crime\\_and\\_Security\\_Act\\_2001](http://en.wikipedia.org/wiki/Anti-terrorism,_Crime_and_Security_Act_2001)

- Schools should keep data safe by having a password
- Internet security


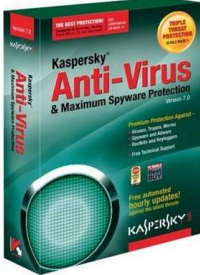
### **TASK 3 (P3, M1, D1)**



**The third part of your report will be about your recommendation as an expert.**



**You will need to:**



**List the measures you would put in place to protect data in a general context (not only school). (P3) (What would you do to protect data in School i.e. Passwords on systems, LAN School?, CCTV etc)**

**For this task it may be better for you to create a table:**

<b>Measures put in place</b>	<b>Description of measure/examples:</b>	<b>Picture/diagram</b>
Virus protection	<b>Viruses such as Trojans can be prevented from entering the computer by making sure there is a firewall in place and a suitable internet security such as McAfee.</b>	 <p>Ref:  <a href="http://edge.fatwallet.com/static/i/deals/mcafee-total-protection-2010-3user.jpg">http://edge.fatwallet.com/static/i/deals/mcafee-total-protection-2010-3user.jpg</a> </p>
Spyware and adware protection	Unwanted spyware and adware can be avoided by buying up to date internet security e.g. Norton 360 or Kaspersky. It can also be avoided by hiding your IP address, using peer block or simply not file sharing from sources you don't trust.	 <p>Ref:  <a href="http://2.bp.blogspot.com/_AQgtDDczPik/SesHgOvsOFI/AAAAAAAAAeY/XWNMY1CFUI8/s400/Kaspersky.jpg">http://2.bp.blogspot.com/_AQgtDDczPik/SesHgOvsOFI/AAAAAAAAAeY/XWNMY1CFUI8/s400/Kaspersky.jpg</a> </p>
Data encryption software	WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) for encrypting wireless Communications RSA (named after the inventors – Rivest, Shamir and Adleman), which is often used in electronic commerce	

Use of passwords and access codes	<p>A password or access code is a sequence of characters, numbers or a combination of characters and numbers that a user keys in to gain access to a specific computer or network. This code should be secret (not given to anyone else) and should be something that another person is unlikely to be able to guess.</p>	 <p>Ref:  <a href="http://www.shareasale.com/images/1PasswordIcon.jpg">http://www.shareasale.com/images/1PasswordIcon.jpg</a> </p>
Backup and storage	<p>Removable storage is a must for systems that hold volumes of Important data. This is used to back up the data on a regular basis – with the backup copy removed to another location for Safe keeping. Work and data should be back up at least once a month; however there is quite a significant amount of work maybe every week or even every day.</p>	 <p>Ref:  <a href="http://www.techfuels.com/attachments/optical-drives/2132d1213174993-genica-ide-mobile-rack-removable-rack-genica-ide-mobile-rack-removable-rack.jpg">http://www.techfuels.com/attachments/optical-drives/2132d1213174993-genica-ide-mobile-rack-removable-rack-genica-ide-mobile-rack-removable-rack.jpg</a> </p>

System facilities	<p>A UPS is a device that sits between the plug socket and the system plugs. The system devices are then plugged into the unit, which is designed to prevent some of the undesirable features of power supplies from affecting the machine (this includes full power losses, brown-outs – drops in power, surges – or power spikes).</p>	 <p>Ref: <a href="http://images.tigerdirect.com/skuimages/large/UPS_main_mm.jpg">http://images.tigerdirect.com/skuimages/large/UPS_main_mm.jpg</a></p>
Surveillance and monitoring	<p>Software is commercially available which enables a workstation to be <b>monitored remotely</b> by an administrator. Such software will also let the administrator <b>take control</b> of the remote PC via their keyboard and mouse.</p>	
Firewalls	<p>A <b>firewall</b> is a program which monitors a workstation's <b>incoming</b> and <b>outgoing</b> network data communication. The firewall can be programmed to <b>permit</b> or <b>deny</b> any transfer it detects. Firewalls can be installed on the <b>workstation</b> itself or may be a <b>separate PC</b> devoted screening network traffic. Some firewalls are built in to other devices, such as</p>	 <p>Ref: <a href="http://www.jabzweb.com/wp-content/uploads/2009/10/Windows_Firewall_Vista_icon.png">http://www.jabzweb.com/wp-content/uploads/2009/10/Windows_Firewall_Vista_icon.png</a></p>

	<b>routers.</b>	
CCTV	<p>Depending on the organization and the sensitivity of the data they hold and use some companies resort to surveillance and monitoring systems. In many respects, these are quite easy to set up as they can be put together using simple components like a computer and a webcam.</p> <p>The concept is that these cameras will be active at all times and will record computer access, use and the general comings and goings in a designated environment.</p>	 <p>Ref:  <a href="http://unambig.files.wordpress.com/2009/10/cctv.jpg">http://unambig.files.wordpress.com/2009/10/cctv.jpg</a> </p>
Lan School	<p>Lan school is in placed in schools to block inappropriate material or material that might be a threat to the system.</p>	 <p>Ref:  <a href="http://www.itsltduk.co.uk/uploadedImages/Partners/LanSchool.jpg">http://www.itsltduk.co.uk/uploadedImages/Partners/LanSchool.jpg</a> </p>

Username/ Passwords	<p>Username and passwords are used to keep data hidden from prying eyes and people who might want to corrupt or steal it.</p>	
------------------------	---	--

Ref: GenDATA\ICT\BTEC\Student Resources\Year 11\Unit 17

### Identify/list appropriate security measures for the school. (M1)

#### Security considerations

If you are asked to take responsibility for ICT security, you should remember the range of

Measures available to you:

#### 1. Physical security measures, such as:

- CCTV
- Keypad locks
- Building passes

#### 2. Logical security measures, such as:

- Anti-virus protection
- Firewalls
- Adware protection
- Spyware protection
- Encryption software
- Passwords and access codes.

**For each recommendation, explain the reason why you need to put this in place. (D1)**

### **CCTV**

If for example some one breaks into the premises and attempts to thief property. The concept is that these cameras will be active at all times and will record computer access, use and the general comings and goings in a designated environment.

### **Keypad locks**

Keypad locks, for example, can either be activated by a single key press sequence used by all users, or can require each user to have a different number. In the event that users have their own unique numbers, this information can be recorded and stamped with the date and time of access  
Keep out people who might be un-trust worthy. Only those who are allowed to access the area that is normally restricted to others will be allowed to enter.

### **Building passes**

Sometimes working alongside a keypad lock, swipe cards are also increasingly used. These cards carry detail in the magnetic strip, and, providing the correct information is read from the strip, the lock will release. These are often used to gain access to particular parts of buildings where not all staff are allowed.

.Keep out people that do not attend the school, therefore keeping its, staff, pupils and property safe

### **Anti-virus protection**

Anti-virus software can identify and block many viruses before they can infect your computer.

## Firewalls

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. Firewalls can be configured to block data from certain locations while allowing the relevant and necessary data through. Keep hackers and identity thieves from accessing your computer.

## Adware and spyware protection

Adware is another invasive product, which effectively keeps displaying advertisements whether the user wants them displayed or not. To protect against invasion by spyware and adware programs, programs that can identify and destroy these often irritating software applications can be downloaded and installed. These include:

- NoAdware Ad-Aware
- Javacool Software Spyware Blaster 3.5.1
- StopZILLA Spyware Remover 4.0
- Microsoft Antispyware Beta 1

## Encryption software

Encryption software is a popular tool used to protect data from prying eyes. Some forms of encryption are extremely complex and exceptionally difficult to break.

E.g. PGP (Pretty Good Privacy), invented by Phil Zimmermann, is popular for encrypting data files and email – it is often described as a **military-grade** encryption algorithm because of its complexity.

## Passwords and access codes

Passwords and access codes are commonplace. It is likely that you will have a **username** and **password** to log on to your school or college systems. A password or access code is a sequence of characters, numbers or a combination of characters and numbers that a user keys in to gain access to a specific computer or network. This code should be secret (not given to anyone else) and should be something that another person is unlikely to be able to guess.

#### **Task 4 (M2)**

In the fourth part, explain with examples how an individual in an organisation can contribute to the security of data.

There are numerous ways how an individual in an organisation such as Microsoft can contribute to the security of data. Firstly he can set a password to all the computer programs that contain delicate information, they access at home. The individual must also make sure to change their password on a regular basis, perhaps, once a week or every fourth night. They should also be careful not to give passwords away to anyone who does not work to the organisation even if they are a family member. They should not misplace their key passes, as this should let it end up in the wrong hands and possibly cause the company some damage financial, etc. Private information about the companies, e.g. bills and memos should also be shredded if not needed using a diamond shredder or kept locked up in a safe space where others can not access, preferably locked with a key pad.