Information and Digital Technology

Mandatory Focus Area: Diagnostic testing

Welcome: This module will assist you to review and revise the content of the **mandatory focus area: Diagnostic testing.**  Each focus area prescribes the scope of learning for the HSC and is drawn from associated units of competency.

You will have studied the unit of competency [ICTSAS308 Run standard diagnostic tests](https://training.gov.au/Training/Details/ICTSAS308) which addresses the scope of learning found in HSC Focus Areas.

This module is broken up into:

* Important Notes
* Key terms and concepts
* Activities
* Putting the theory into practice
* HSC Focus Areas

**How to use this resource**

Work through the notes and the suggested activities. Great revision techniques include working through how a problem is solved, explaining the concept, testing yourself and retrieving information from your memory. Spread your revision over a number of sessions rather than sitting at one subject for lengthy periods.

Discuss your responses with your teacher, fellow students or an interested family member.

All images, apart from those acknowledged, are © NSW Department of Education.

# Important notes

You should use the information in this section as a prompt and guide when revising your **study** **notes** or **text-book information** or **other resources** provided by your teacher.

[ICTSAS308 Run standard diagnostic tests](https://training.gov.au/Training/Details/ICTSAS308) describes the skills and knowledge required to troubleshoot problems, identify and implement preventative maintenance techniques, and conduct diagnostic tests on a range of platforms.

The outcomes of the HSC mandatory focus area ‘Diagnostic testing’ require that the student:

* analyses common symptoms and causes of hardware and operating system problems
* selects and justifies appropriate diagnostic tests for a range of platforms
* explains the purpose of preventative maintenance
* demonstrates an understanding of destructive and malicious software and its removal.

## System security guidelines

Business organisations understand that their information systems and networks can be affected by both internal and external risks. As a result, companies develop guidelines to safeguard the security of their information systems and networks.

These guidelines are directed at the organisation’s operators and users to develop an awareness of the risks and an understanding that security failures may significantly harm systems and networks, paramount to their core business.

IT managers are responsible for the configuration of, and available updates for, their system, and the development of good practices that they can implement to enhance security.

Employees are accountable (in a manner appropriate to their individual roles) for the security of their information systems and networks.

System security policies may include safeguards for:

* confidentiality of information
* integrity of data
* assets
* efficient and appropriate use
* system availability

The Acceptable Use Policy is the one you see when you access your school email.

visit <https://www.digitalcitizenship.nsw.edu.au/articles/using-technology-in-schools>



Swinburne University of Technology has some excellent Information Technology Policies.
Click here to locate the university’s [IT acceptable use guidelines](http://www.swinburne.edu.au/about/leadership-governance/policies-regulations/procedures-guidelines/acceptable-use-guidelines/)

## Backing up

A backup policy states what decisions have been made and what should be happening. It does not detail specifically how the backups will be carried out on a day-to-day basis. For this, you may need to create backup procedures based on your individual policy.

There can be no ‘best-practice’ or ‘ideal’ policy because each organisation has different needs. The best policy will be the one that is easy to implement but ensures that all the data that you may wish to restore, at some point in the future, can be recovered.

By completing a policy document for your organisation, you can become aware of what data is being backed up, how it is being backed up, and whether the existing processes can be improved. It is also a way of assigning responsibility for tasks, to designated roles or persons, so that there is accountability for the processes.

A backup and trial-restore policy is a document that lists all the important strategic decisions about your backup and restore scheme. For example, the policy may state the following:

* the organisation backing up the data
* what files/folders are to be backed up
* which PCs will be backed up
* how often the files/folders are to be backed up
* what backup media is to be used
* what backup drive is to be used
* how the backup will be performed
* what time the backup will be performed
* what backup software will be used
* what backup type is to be used
* what backup options will be used
* how often the media will be rotated
* how often the media will be replaced
* when the media is next due for replacement
* what disk/tape maintenance procedures will be carried out
* what media maintenance procedures will be carried out
* how often the disk/tape drive will be maintained
* how often the media will be maintained
* how often trial restores will be carried out
* who is responsible for backups
* who is responsible for restores
* who is responsible for maintenance
* who is responsible for replacements
* where the media is stored (both on-site and off-site)
* how the media is to be stored (both on-site and off-site)
* who is responsible for delivering and storing the off-site media
* what is the availability of the off-site media

## Viruses

A virus is a program which reproduces its own code, by attaching itself to other programs, in such a way that the virus code is executed, when the infected program is executed. What makes viruses special, is that they work by placing self-replicating code in other programs. This self-replicating program, when trig­gered by some event, may be harmful to your computer.

Here are a few things to keep in mind when considering viruses:

* you can only get a virus by executing an infected program or booting from an infected storage device. Any storage device, even a non-bootable one, can be infected by a boot sector virus.
* you cannot get a virus simply by being on a bulletin board system (BBS), Internet or an on-line service. You will only become infected if you download an infected file and execute that file (including the Microsoft Office related files - use a viewer program for viewing rather than using the actual software).
* keep backups of all your files.
* check all new software for viruses. Even shrink-wrapped software from a major publisher may contain a virus.

The main methods of virus protection are:

* monitoring and identifying unusual disk activity, using a resident program.
* scanning program and data files on your computer, using software such as CA/Vet and Norton/Symantec.
* scanning incoming on-line data (from the Internet, for example) for macro viruses.

If you detect a virus, it is essential that you notify your supervisor, IT support department and any other parties who may be affected.

### Virus types

Viruses come in many different forms, but they all potentially have two phases:

#### Infection phase

When the virus executes, it will infect other programs. What is often not clearly understood, is precisely when it will infect the other programs. Some viruses infect other programs each time they are executed; others infect only upon a certain trigger. This trigger could be anything - a day or time, an external event on your PC, or a counter within the virus. Some viruses are very selective about when they infect programs, as this is vital to the virus's survival. If the virus infects too often, it is more likely to be discovered before it can spread far.

Many viruses reside in the memory of your PC as a terminate and stay resident (TSR) program. This means that the virus can wait for some external event, such as inserting a diskette, copying a file or executing a program to actually infect another program. This makes these viruses very dangerous, since it is hard to guess what trigger condition they use for their infection. Resident viruses frequently corrupt the system software on the PC, to hide their existence.

#### Attack phase

In the attack phase, many viruses do things such as deleting files, changing random data on your disk or merely slowing down your computer. Some viruses do less harmful things, such as playing music or creating messages or animation on your screen. Just as the virus's infection phase can be triggered by some event, the attack phase also has its own trigger.

#### System sector viruses

As their name indicates, system sector (or boot sector) viruses plant themselves in the computer's system sectors. System sectors are special areas on the disk, con­taining programs that are executed, when you boot your PC. Sectors are not files, but simply small areas on the disk, that the hardware reads in single chunks. These sectors are invisible to normal programs but are vital for correct operation of your PC. They are a common target for viruses.

There are two types of system sectors found on DOS/Windows PCs: DOS boot sectors and partition sectors (also known as master boot records or MBR). System sector viruses modify the program in either the DOS boot sector or the partition sector. Since there is not much room in the system sector, these viruses often have to hide their code somewhere else on the disk. They sometimes cause problems when this spot already contains data, which is then overwritten.

Some viruses, such as the Pakistani Brain virus, mark the spot where they hide their code, as having bad sectors. These viruses usually go resident in the memory on your PC and infect any removable storage media which you access.

#### File viruses

File viruses are the most common kind of virus. The simplest file virus works by locating a type of file that they know how to affect, (usually a file name ending in .com or .exe) and overwriting part of the program they are infecting. When this program is executed, the virus code executes and infects more files. These overwriting viruses do not tend to be very successful, since the overwritten program rarely continues to function correctly, and the virus is almost immediately discovered.

The more sophisticated file viruses modify the program, so that the original instructions are saved, and execute after the virus finishes. Just as system sector viruses can remain resident in memory and use ‘stealth’ techniques to hide their presence, file viruses can also hide this way. If you do a directory listing, you will not see any increase in the length of the file and if you attempt to read the file, the virus will intercept the request and return your original uninfected program to you.

Many file viruses (such as 4086, which is also known as Frodo) also infect overlay files, as well as the more usual \*.com and \*.exe files. Overlay files have various extensions, but ‘ovr’ and ‘ovl’ are common examples.

#### Macro viruses

The files from the Microsoft Office applications (MS Word, MS Excel, MS Access and so on) are all programs that have their own built-in macro language (a BASIC-like language). The programs (in macro language) are executed when the file is loaded into the associated product. The program inside the file is interpreted by the MS Office application. Since anything that contains a program can poten­tially be infected by a virus, these files can harbour viruses. Even MS Access data­base files (\*.mdb) can contain macro viruses.

What gives these viruses a chance to act is the fact that Microsoft has defined special macros that will automatically execute. The mere act of opening an infected MS Excel spreadsheet, for example, can allow the virus macros to be executed. One simple way to prevent this type of virus is to use the freely available (from Microsoft) viewer programs, rather than MS Word or MS Excel, to view these types of files. These viewers cannot run the Macro Language code, and this reduces the risks involved with working with these types of files.

Macro viruses have been very successful because most people regard spread­sheets and documents as data, not as programs. If you use a mail reader or Web browser, it is very important to use a viewer, rather than the full MS Office pro­gram, if you want to automatically open downloaded MS Word documents or MS Excel spreadsheets.

#### Destructive software

Viruses are one specific type of program, written deliberately, to cause harm to some­one's computer, or to use that computer in an unauthorised way. There are many forms of malicious software - sometimes the media calls all malicious software `vi­ruses', but it is important to understand the distinction between the various types.

#### Logic bombs

Just like a bomb, a logic bomb will lie dormant until triggered by some event. The trigger can be a specific date, the number of times executed, a random number, or even a specific event, such as any modification in the record. When the logic bomb is triggered, itwill usually do something unpleasant. This can range from changing a random byte of data, somewhere on your disk, to making the entire disk unreadable. The primary difference between a logic bomb and the average computer virus is that the logic bomb will not attempt to infect other files or computers.

The classic use for a logic bomb is to ensure payment for software. If payment is not made by a certain date, the logic bomb activates, and the software automatically deletes itself. A more malicious form of that logic bomb would also delete other data on the system.

#### Trojans

Trojans are named after the Trojan horse, which carried Greek soldiers inside it, into the city of Troy. Likewise, a Trojan program is a delivery vehicle for destructive code (such as a logic bomb or virus) into a computer. The Trojan pro­gram appears to be a useful program, but when a certain event occurs, it will attack your PC in some way.

A Trojan Horse virus is also capable of stealing important information from the user's computer. It will then send this information to Internet servers that have been designated by the developer of the virus. The developer will then be able to gain a level of control over the computer through this Trojan virus. While these things take place, the user will notice that the infected computer has become very slow or unexpected windows pop up, without any activity from the user. Later on, this will result in a computer crash.

A Trojan Horse virus is most commonly spread through email attachments.

#### Worms

A worm is a self-reproducing program, which does not infect other programs as a virus will, but instead creates copies of itself, which create even more copies. These are usually seen on networks and on multi-processing operating systems, where the worm will create copies of itself, which are also executed.

Due to the copying nature of a worm and its capability to travel across networks, the end result in most cases, is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding.

#### Hoaxes

Virus hoaxes are false reports about non-existent viruses, sent via email. Many of these e-mail hoaxes will trick you into forwarding messages about fake viruses or other fabricated stories. These e-mails waste time and clog inboxes.

### Virus detection

Viruses are detected by anti-virus software in two basic ways: through a full scan of your computer resources (local or network) or through a scan in real-time, as each file is accessed. It is critical that anti-virus software provide both these features, especially real-time protection. Full and real-time scans detect known viruses using **signature codes**(like virus fingerprints), which identify a program as a virus. Some anti-virus software also uses advanced techniques to identify potential viruses and check memory and system files for viruses. The total number of viruses an anti-virus software program can detect is known as the **detection rate**.

Commonly used virus protection software includes:

* BIOS anti-virus software
* commercially available anti-virus software that scans data on your computer and scans incoming data on a network.

The most common form of virus protection today is based on software that you can purchase and install on your computer. Products such as CA Vet (virus eradication technology), McAfee Virus Scan and Norton's Anti-Virus are widely used.

Detection is the essence of any anti-virus strategy. If a virus is found, appropriate action can be taken - the virus can be removed, the disk wiped clean, or the infected files replaced by clean backup copies. At the very least, the infected machine can be taken out of use until the virus has been dealt with, thus protecting the other computers.

#### Scanning

The aim of detection is to find a virus before it activates. There are two ways to do this: ‘heuristic analysis’ and*‘*scanning’:

**Heuristic** **analysis** involves looking at the program code itself, to determine if any part of that program could cause any damage. This approach has the advantage of not needing to know about the virus before detecting it. However, it does consume more resources and may lead to false alarms.

A **scanner** reads the content of executable files, looking for virus code and notifying the user when any is found. Some scanners ask the user if they want to remove the virus from the infected file, while others leave that task to a sep­arate utility from the same anti-virus package. Every effective anti-virus package comes with a good scanner as its main element.

A signature database is at the heart of all scanners. This is a collection of bit pat­terns, found in files infected by a range of known viruses. The simplest scanners check each file for the existence of any of the virus signatures in the database. Using a single signature can lead to a high rate of false positives, however, and so the best way to reduce the incidence of false positives is to use two or more signa­tures for each virus. If the first signature is found, the scanner checks for the exis­tence of the second signature, before concluding that the virus is present. Most scanners use multiple signatures. Advanced scanners also decrypt code, allowing them to detect polymorphic viruses with a high rate of success.

There are two types of scanner utilities:

**On-demand scanners**execute either by the user issuing a command when they decide to check a disk, or from a command line in a batch file. They per­form a thorough scan of all executable files on a disk, searching for known viruses.

**Memory-resident scanners**are loaded into memory when the computer starts up, and they remain until the computer is shut down, scanning files as they are accessed. If a virus is detected, the scanner reports it and warns the user to disinfect the machine. Some memory-resident scanners lock the PC as soon as they display their warning message, as the virus is by that stage in RAM and ready to infect.

##### BIOS anti-virus software

BIOS anti-virus software is normally installed in the BIOS or on the hard disk by the computer manufacturer.

The following steps show you how to check the BIOS settings of the computer you are working on. Before you begin this activity, check with your tutor that you have access to the BIOS on your machine.

Follow these steps:

1. Shut your computer down by the proper means and then switch it off.
2. Turn your computer on and watch the screen as it boots up. Press the DELETE key when the prompt saying Press delete to run setup appears.
3. When you have pressed DELETE, the system may prompt you for a pass­word. Ask your tutor for the password if necessary. The CMOS settings screen will appear.
4. Select the menu option that says Advanced CMOS settings. This screen offers many options. Be careful to only change the settings that you are told to in the next step.
5. There should be an Enable virus protection option on this screen. Enable this virus protection option. A message will appear on the screen during the boot process that will say something like Chip away virus protection enabled.
6. Save your changes by following the instructions on the screen.
7. Exit the CMOS settings screen and reboot your computer. You should now see the virus protection message when booting up.

This is not necessarily real virus protection, which is better provided by virus detection software. It may only warn when the disk boot sector is accessed for writing. Some operating systems or environments may do this regularly.

Sometimes it is hard to judge from these warnings, whether they are coming from normal system activity or from virus attacks. Use this option if it is necessary in the absence of virus detection software.

Once a virus is detected, it is essential that you follow these 4 steps:

**1. Deactivate the virus**

Not much can be done while the virus is in memory. The first step must be to stop it from running. (Obviously, this step is not required where a virus is inactive and detected during a routine scan of a workstation.) First, turn off the computer as soon as the virus is detected. If the computer belongs to a Network, then disconnect the computer from the network whilst it is turned off. Then reboot the computer with a start up or recovery disk. The computer will now be running with the hard drive accessible and the virus inactive.

**2. Clean (remove) the virus**

With the virus inactive and the computer running, load the disinfection util­ity. You may have to access the internet from another computer to download the latest virus definition files. Follow the instructions for the product you are using and attempt to remove the virus. The procedure may or may not be straightforward - it depends on the type of virus and the capabilities of your anti-virus package.

**3. Recover any lost or damaged data**

Some viruses will suddenly wipe the contents of a disk or overwrite the contents with garbage. Others are more insidious, changing a bit or two now and then - this type may slowly corrupt data over time before being detected. It may not be obvious which files have been damaged, so you might need to examine each one separately. Consider whether the contents of these files are sufficiently important to justify this type of examination. In the case of applications directories, the sim­plest thing may be to restore the entire directory from the backup or to reinstall it from scratch. However, even restoration from a backup might not be entirely safe. If an infected file were inadvertently backed up, you could reintroduce the virus, so check your backup before using it to restore your files.

**4. Prevent a recurrence**

Alert your supervisor and/or IT support department to the presence of the virus. Do this in writing and include as many details as possible about the virus, its source, and action taken.

Alert your workmates and, if necessary, the person who supplied the source of the virus.
Document the occurrence of the virus. Most organisations have a central register of detected viruses

##### Updating anti-virus software

Because there is no absolute definition of what constitutes virus activity, it is not possible to write a program that will be 100% accurate in its diagnosis. This is especially true of disk activity monitoring. Checking for signatures or patterns is far more accurate but requires that the software be frequently and continually updated, since new viruses are being written all the time. It has been suggested that up to two hundred new viruses are written every week.

Because of the number of new viruses, it is essential that you continually update your anti-virus software. Most vendors of anti-virus software have a Website where you can download the most current version of their software.

### Virus protection software

#### Commercially available

The most common method of virus protection is the use of commercially available packaged software. This software is installed on your computer to detect and eradicate viruses, and repair any damage caused.

Anti-virus software works in two ways. Firstly, it has a big ‘dictionary’ of viruses, allowing it to scan files and flag any that are known to be viral. Secondly, the software monitors the system for any suspicious activity.

Once the antivirus software has detected a virus's signature, it identifies the virus by compar­ing it with a table of known signatures and then eradicates the virus and repairs any damaged files. Most anti-virus software can print a report of any viruses detected and an explana­tion of the action taken. The software will also record this information in a log.

All anti-virus software allows you to scan your computer manually.

#### Network server

Network server software is usually installed on a server, and scans all incoming data, particularly that embedded in email, for potential viruses. This software operates in a similar way to that employed by the anti-virus software which you install on a computer. The software checks each incoming network packet, attempting to find a pattern which could be identified as a virus. This is then compared to a table of known virus signatures. If a signature is detected, action is taken to remove or report the virus and repair any damage.

#### Operating System Software

Most malicious software, also known as **malware,**is targeted at Windows based operating systems. As a result, Microsoft has addressed the problem by incorporating Windows Defender real-time antivirus software.

## Maintenance

Routine or preventative maintenance ensures that the computer equipment, both hardware and software, will remain in good working order. To ensure that maintenance is carried out at the correct times a schedule of tasks needs to be developed.

### Hardware maintenance

|  |  |  |
| --- | --- | --- |
| Component | Maintenance | Frequency |
| Inside the case | Make sure air vents are clear.Use compressed air to blow the dust out of the case.Make sure that chips & expansion cards are securely seated.Clean the contacts on the expansion cards. | Yearly |
| CMOS setup | Keep a record of the setup details of the CMOS; there are various software utilities that can be used for this purpose. | At each change in the setup |
| Floppy drive | To save unnecessary wear on the heads, clean only when the drive appears to be causing problems. | When the drive fails |
| Hard drive | Do regular backups of data files.Use a virus program, preferably having it execute at start up.Defragment the drive.Do not eat, drink or smoke near the computer.Place the computer where it cannot get bumped. | At least weeklyDailyMonthly |
| Keyboard | Clean the keyboard. | Monthly |
| Mouse | Clean the mouse. | Monthly |
| Monitor | Clean the screen with a soft cloth and clean dust from the rest of the casing of the monitor. | Monthly |
| Printer | Clean out the dust and bits of paper.Clean the paper paths with a soft cloth. | Monthly |
| Maintain a logbook | Record all software, including version numbers & OS installed on the computer.Record all hardware components installed, include hardware setting.Record when and what maintenance is performed.Log all faults and what is done to correct them.Record any repairs done. | Whenever a change occurs |

### Software maintenance

|  |  |
| --- | --- |
| Activity | Frequency |
| Data backup | Daily |
| Scan for viruses | Daily |
| Scan file system for errors | Daily or Weekly |
| Check hard drive free space | Weekly |
| Full backup | Weekly or Monthly |
| Defragment hard drive | Monthly |
| Check for software and data updates | Weekly |
| Clean out old files | Monthly or Quarterly |
| Check system properties | Quarterly |

#### Useful equipment for maintenance

Listed below are a few items that are useful to a computer owner in the maintenance of a computer system:

* a soft bristled paint brush
* lint free cloth
* a can of compressed air
* small (hand-held battery operated) vacuum cleaner with a brush attachment
* cotton swabs
* CD drive cleaning kit
* cleaning materials, for example, alcohol-based screen wipes for monitor screens and scanner glass
* cleaning appliances for plastics
* precision toolkit containing small screwdrivers, custom pliers and
* tweezers
* a torch
* an earth strap
* any consumables needed by the device like printer cartridges or paper.

# Key terms and concepts

|  |  |
| --- | --- |
| Key term or concept | and definition |
| Backup | A method of storing files for use in an emergency. The backup medium includes tape, disk or CD. |
| Boot sector infectors | Viruses that infect the boot sector of a floppy or hard disk. |
| Defrag | Defragmentation is the process of locating the non-contiguous fragments of data, into which a computer file may be divided, as it is stored on a hard disk, and rearranging the fragments and restoring them into fewer fragments or into the whole file. |
| File infectors | Viruses that attack and modify program files, usually .exe and .com files. When the program is run the virus is executed. |
| Logic bombs | Viruses that activate when they detect certain conditions, eg a certain date. |
| Macro viruses | These viruses make use of the built-in programming languages in Microsoft Word and Excel (VBA); a malevolent macro that duplicates into other documents, and spreads like any other virus once the file has been opened. |
| Maintenance | Maintenance refers to rectifying faults and changing settings or components, to ensure that equipment continues to work effectively. |
| Non-routine maintenance | When a device or its components are serviced to rectify a specific fault. Procedures such as replacing a faulty CD/DVD drive or adding extra RAM to a poorly performing computer are examples of non-routine maintenance. |
| Preventative maintenance | Regular inspection of the computer’s hardware to prevent things from going wrong. |
| Polymorphic viruses | Viruses which modify their program codes every time they attach themselves to another program or file. |
| Routine maintenance | When a device or its components are serviced as a matter of course. Procedures such as adding paper to the printer tray, aligning the print heads or changing toner cartridges are some examples of routine maintenance. |
| Scandisk | Scandisk is a Windows utility used to check your hard disk for errors and to correct problems that are found. |
| Trojan horse | A destructive program that masquerades as a harmless application. While Trojan horses do not copy themself, they can do as much damage as viruses. |
| Virus | A program that is loaded onto your computer without your knowledge and runs without your consent. Most viruses can also replicate themselves. |
| Virus signature | The virus signature is like a fingerprint, in that it can be used to detect and identify specific viruses. It consists of a unique string of bits, or the binary pattern, of a virus. Anti-virus software uses the virus signature to scan for the presence of malicious code. |

# Activities

### Activity 1: Questions

1. A tablet device is very slow and keeps shutting down unexpectedly. Outline the possible causes of these issues. How would you fix this?
2. Justify strategies that a business could implement to maintain the reliability of its desktop computers.
3. Why should we backup?
4. List 5 risks to a user’s computer data.
5. List 6 different types of media that can be used to backup data.
6. How would you determine what the backup requirements of an organisation actually are? What factors would you consider?
7. What are the 3 different types of backup? In your answer explain the difference between them.
8. When you have set up a backup system, you would establish a backup register. What information do you think you would record in this register?
9. What does the term ‘retention period’ mean?
10. How do ‘rotation systems’ work in relation to backups?
11. What is a ‘Disaster Recovery Plan’ and what factors would you need to consider when creating this plan?
12. What is a computer virus?
13. What are the 3 main categories of virus?
14. What is a ‘Trojan Horse’ program?
15. List 7 ways of preventing viruses from infecting your computer system.
16. If you were the assistant Computer Support Officer (say for a large company) and discovered a computer virus, what action do you think you would take?
17. What are some symptoms of viruses?
18. What does a ‘virus definition file’ contain?
19. List 5 commercial anti-virus programs.
20. Which file attribute is vital to the backup process? Explain how this attribute is used in the backup process.
21. What is the purpose of the ‘ScanDisk’ utility program provided with Windows?
22. Assume you have backup software, a tape drive and a number of tapes that are capable of storing a maximum of 50 gigabytes each. Examine the scenarios below.
	1. ***Scenario One***
	A file server has 40 gigabytes of data files. Each day 30 gigabytes of these data files are changed. A full backup of data files is performed each night.
	Explain why the backup method described is appropriate for this scenario.
	2. ***Scenario Two***
	A file server has 100 gigabytes of data files. Each day 10 gigabytes of these data files are changed. Since the last full backup a partial differential backup of data files has been created each night.

	Explain why the backup method described is appropriate for this scenario.
23. A file server has 200 gigabytes of data files. Each day 100 gigabytes of these data files are changed. A full backup is performed every Friday night and partial incremental backups are performed on Monday, Tuesday, Wednesday and Thursday nights.
	1. What is the minimum number of tapes required to store one week of backup data? (Show all working.)
	2. There was a hard drive failure 15 minutes before business commenced on Wednesday. Propose a sequence of steps to restore the lost data onto a newly formatted hard drive.
24. Why is it necessary to eject a mass storage device before removing it?
25. What is a UPS and how does it work?
26. What is a diagnostic card used for?
27. What is the CMOS?
28. Why is it NOT necessary to run a disk defragmenting utility on a solid state drive?
29. The following is part of a server backup log from a small business.



Using the information in the backup log, describe and justify the most efficient procedure for restoring the full system in the event of a hardware failure on10/10/2014.

1. An organisation is experiencing frequent computer virus infections. Outline actions that could be taken to prevent this from continuing. Explain how the infection may impact on the business.

### Activity 2: Past HSC Questions

The following questions are from [past years’ NSW HSC examination papers](https://educationstandards.nsw.edu.au/wps/portal/nesa/11-12/resources/hsc-exam-papers) for this subject. HSC exams are intended to be rigorous and to challenge students of all abilities. To better understand a question, you should look for key words and identify the aspect of the course to which these relate. You are then in a position to formulate your answer from relevant knowledge, understanding and skills.

All questions in this activity are acknowledged © [2019 NSW Education Standards Authority (NESA) for and on behalf of the Crown in right of the State of New South Wales.](https://educationstandards.nsw.edu.au/wps/portal/nesa/mini-footer/copyright)

#### Multiple choice

1. Some computer viruses take advantage of a vulnerability in an operating system. What would be the most effective method to avoid being infected by this type of virus?
	1. Update virus and spyware definitions
	2. Complete a full scan on your computer
	3. Replace your virus protection software with the latest version
	4. Install a patch provided by the operating system manufacturer
2. A home network connects to the internet via ADSL. However, on a particular evening, no computers on the network can access the internet.

When the network connection on one of the computers was checked, the network cable was plugged in and the port indicator lights were active.

Which of the following is the most likely cause of the issue?

* 1. A. The router has no power.
	2. The ethernet cable is not plugged into the router.
	3. The web browser has not been updated since installation.
	4. The telephone cable is not plugged into the correct socket.
1. Ashley has a stand-alone computer. His work requires him to spend a lot of time on the Internet downloading modules of code and graphics from websites. His computer is running slowly, freezing and creating duplicate copies of existing files.

What is the most likely cause of these problems?

* 1. The hard drive is full.
	2. Downloading has consumed RAM.
	3. The web browser needs to be updated.
	4. A virus has been downloaded and activated.
1. Which of the following actions demonstrates the use of an operating system tool to determine and change hardware properties and status?
	1. Downloading a free spyware tool to scan the hard drive for unwanted applications.
	2. Purchasing a virus protection application to detect and remove viruses attached to any files stored on the hard drive.
	3. Using a free file compression application to increase the number of files that can be stored on the hard drive.
	4. Using disk cleanup or disk defragmentation tools to reduce the time needed to access files stored on the hard drive.
2. You have been instructed to install additional RAM into a company computer.

Which is the correct order of steps that you should follow to install the RAM safely?

* 1. Install RAM, isolate computer from power supply, connect anti-static strap to wrist
	2. Connect anti-static strap to wrist, install RAM, isolate computer from power supply
	3. Isolate computer from power supply, install RAM, connect anti-static strap to wrist
	4. Isolate computer from power supply, connect anti-static strap to wrist, install RAM
1. This diagram displays the results of running a scandisk utility on the hard disk drive of a workstation. What does ‘B’ represent?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|   |   |   |   |   |   |   |   |   | B |
| B | B | B |   |   |   | B | B | B |   |
|   |   |   |   |   |   |   |   |   |   |
|   |   |   | B | B | B |   |   |   | B |

* 1. Faulty sections on the disk
	2. Fragmented files on the disk
	3. Binary data stored on the disk
	4. The location of blocks on the disk
1. While installing a new workstation in the sales department, you notice a power point with exposed electrical wires.

What is the first thing you should do in this situation?

* 1. Use another power point.
	2. Repair the power point yourself.
	3. Report the problem to your supervisor.
	4. Provide warning signs in order to isolate the problem.
1. What is the primary source of information about specifications for a hardware device?

	1. The manufacturer’s manual
	2. The occupational health and safety legislation
	3. The organisation’s policy and systems manual
	4. The requirements on the hardware purchase order
2. When would the factory recovery partition on a computer be used?

	1. To install a new driver
	2. To recover deleted emails
	3. To recover corrupted user files
	4. To reinstall the operating system
3. Before a new hard disk can be used to store files, it needs to be

	1. defragged.
	2. formatted.
	3. partitioned.
	4. scanned.
4. Which type of malicious software transfers itself to other computers without any user action?

	1. Worm
	2. Trojan
	3. Key logging
	4. Boot sector virus
5. What is the main purpose of an uninterruptible power supply (UPS) and its software?

	1. To boost the power supply for a server
	2. To provide a low cost power supply for a server
	3. To convert mains power to the lower voltages that are used internally by a server
	4. To enable a server to be safely shut down in the event of a prolonged power failure
6. A user in an office has reported that a networked computer is no longer able to access the internet. All other computers in the office can access the internet. Which of the following would be the most effective strategy to troubleshoot this problem?
	1. Use the PING command to determine connectivity
	2. Ask the user to wait 20 minutes in case the internet is down
	3. Use IPCONFIG to determine whether the hard disk has sufficient space
	4. Check the BIOS of the computer to determine whether the internet is operational
7. What type of documentation should system requirements be obtained for software installation?
	1. Help desk log
	2. Alert message
	3. Technical specification
	4. Service level agreement
8. A desktop computer seems to be operating normally, but the lights on the network interface card are not lit. What is the most likely cause of this problem?
	1. The internet is down.
	2. The CMOS battery is faulty
	3. The network cable is unplugged.
	4. The power supply of the computer is faulty.
9. Employees in an organisation are frequently being interrupted with a fake pop-up alert message, even when not using a browser. The company’s computers are regularly scanned with antivirus software. Which of the following is most likely to overcome this problem?
	1. Perform a disk cleanup
	2. Defragment the hard disk
	3. Run a real-time virus scan
	4. Update the virus definitions
10. Which of the following is an example of Diagnostic testing?
	1. Running a file search on a hard drive
	2. Configuring partitions on a hard drive
	3. Backing up a faulty hard drive to a new hard drive
	4. Checking the number of bad blocks on a hard drive
11. What is a virus signature?
	1. The damage done by a computer virus
	2. The code used to specifically identify a virus
	3. The trail left behind after a virus infects a computer
	4. The specific message the virus leaves on a computer
12. This graph was produced using an administrative tool.



Which row of the table correctly identifies the administrative tool and system status?



1. What does this symbol represent? 
	1. Battery
	2. Bluetooth
	3. Volume
	4. Wi-Fi

#### Questions from Section II of the HSC exam

Question 1

* 1. A tablet device is very slow and keeps shutting down unexpectedly. Outline the possible causes of these issues (3 marks)

* 1. Justify strategies that a business could implement to maintain the reliability of its desktop computers. (4 marks)

Question 2

An organisation is experiencing frequent computer virus infections. Outline actions that could be taken to prevent this from continuing. (3 marks)

Question 3

A web design business has a file server and 20 workstations. Explain why an uninterruptable power supply (UPS) would be recommended for this business.
(3 marks)

Question 4

* 1. Explain how a business may be affected by malicious software. (2 marks)

* 1. A user reports that they cannot log on to the network. What troubleshooting steps should be taken to resolve this issue? (3 marks)

#### Questions from Section IV of the exam.

In the HSC there will be one extended response question based on the **mandatory focus areas** with an expected response of around four pages of an examination writing booklet (approximately 600 words). You should allow about 25 minutes for a question in Section IV in the exam.

Your answer will be assessed on how well you:

* demonstrate knowledge and understanding relevant to the question
* communicate ideas and information using relevant workplace examples and industry terminology
* present a logical and cohesive response

You will note that the questions from Section IV usually require you to bring together knowledge from several areas of study/competencies to do justice to the answer. In each of the following, map out your answer using post-it notes or a sheet of paper. Pay particular attention to incorporating a variety of aspects of your IDT curriculum into the plan. Consider why we have included this question within this module and what other areas of study you would need to draw upon.

Question 1

A web design company has 20 identical networked desktop computers. It wishes to install a new version of the operating system on these computers. The business operates between 8.30 am and 5.00 pm Monday to Friday.

You have been asked by the management to recommend an installation plan that would allow the installation to be completed with minimal disruption to the company. In your recommendation, compare the different installation options available and outline an installation plan based on the most suitable option.

Question 2

A small business is experiencing trouble with its computers. Its employees have complained that their computers are running slow, have annoying pop-ups, make sparking noises and are losing data. There have also been reports that email attachments sent by the employees contained viruses.

Justify strategies that the business could adopt to address these issues.

# Putting the theory into practice

1. Create a routine maintenance schedule of tasks that need to be undertaken weekly, fortnightly monthly on hardware and software

|  |  |
| --- | --- |
| Frequency | Activities |
| Daily |  |
| Weekly |  |
| Fortnightly |  |
| Monthly |  |
| Quarterly |  |
| Yearly |  |

1. Use the backup program that comes with your operating system, eg, Microsoft Backup, to backup selected files on a PC.
2. Rename some of the files you backed up in question 1, and then restore those files from your backup.
3. Use an archive program, eg, Winzip, to compress a number of files.
4. Use the internet to locate and download a free anti-virus program. Install the anti-virus program onto your computer.
5. Download a virus library update for the anti-virus program and install it.
6. Scan your system for viruses.
7. Research the current virus threat level
8. Run a system diagnostic program and interpret the results
9. Defrag your hard drive.
10. Research each of the following scenarios outline your trouble shooting steps and diagnose the possible problem.
	* The computer won’t start
	* The screen is blank
	* The operating system is unresponsive acting up
	* Windows won’t boot
	* The screen is frozen
	* Computer is running slow
	* Strange noises are coming from inside the computer
	* The internet is very slow
	* Computer seems to be overheating
	* Internet connections keep dropping out

# HSC Focus Areas

For the purposes of the HSC, all students undertaking the 240 HSC indicative hours course in Information and Digital Technology must address **all of the mandatory focus area** **content** plus **one** **stream** **focus area.**

IDT **Mandatory** focus areas

* Working in the industry
* Operating system software
* **Diagnostic testing**
* Safety

IDT **Stream** focus areas (know which **one** of the stream focus areas you are studying)

* Web and software applications
* Networking and hardware
* Digital animation

The scope of learning describes the breadth and depth of the HSC Content and has been grouped together into key ideas/areas. The scope of learning describes the minimum content that must be addressed, and the underpinning knowledge drawn from the associated unit of competency [ICTSAS308 Run standard diagnostic tests](https://training.gov.au/Training/Details/ICTSAS308)

How to use the scope of learning for ‘Diagnostic testing’ (which follows over).

* draw up your own mind map showing the connection between the various concepts listed; examples appear on the last page of this module
* use the key terms and concepts to add to your mind map
* add examples or case study prompts to show how the concept is applied in the information technology working environment

The following information is taken directly from page 33 ff of [Information and Digital Technology Curriculum Framework Stage 6 Syllabus (NSW Education Standards Authority) for implementation from 2020.](https://educationstandards.nsw.edu.au/wps/wcm/connect/852daa22-4180-4a58-b57f-c2a09540e5e7/vet-information-digital-technology-11-12-syllabus-based-on-V.5.0-jan-2020.pdf?MOD=AJPERES&CVID=) © [2019 NSW Education Standards Authority (NESA) for and on behalf of the Crown in right of the State of New South Wales.](https://educationstandards.nsw.edu.au/wps/portal/nesa/mini-footer/copyright)

|  |
| --- |
| client business context |
| * importance of understanding that a workplace’s function relies on computers working properly and free of destructive or malicious software
 |
| * workplace policy, procedures and guidelines for the protection of computer systems and networks related to:
* diagnostics
* preventative maintenance
* system security
* troubleshooting
* virus protection
 |
| troubleshooting |
| * general features, selection and use of hardware and software diagnostic tools commonly used in the information and communications technology (ICT) industry for a range of platforms
 |
| * common symptoms of problems with:
* operating systems
* desktop applications
* laptops
* tablets and other mobile devices
* printers
* other common peripherals
 |
| * awareness of root causes of different types of problems, including those related to:
* electrical issues
* hardware
* operator/user
* peripherals
* software
* connectivity
 |
| * identify and use sources of information for computer-related problems and the diagnostic tools that may be used to troubleshoot them, including vendor online help, manual and reference material
 |
| * strategies for troubleshooting common problems:
* identify the possible problem
* perform backup procedures before making changes
* establish likely cause
* run diagnostic tests using appropriate diagnostic programs:
* interpret the results of diagnostic test undertaken
* take follow-up action:
 |

|  |
| --- |
| troubleshooting cont/d |
| * re-run diagnostic tests, or escalate them, if the likely cause is not confirmed
* resolve the problem if the likely cause is confirmed
* resolve the identified problem:
* determine suitable plan of action
* implement the solution, including backups before making modifications
* verify full system functionality
* implement preventative measures to reduce the chance of future problems
* document findings, actions and outcomes
* liaise with clients to check their satisfaction with how the problem has been resolved
 |
| preventative maintenance |
| * strategies and techniques for maintaining computer hardware, software and peripherals in good working order:
* physical inspection of equipment
* backup procedures:
* full backups
* partial backups including incremental and differential
* implementing a schedule for tasks associated with routine maintenance:
* virus scanning
* installing updates
* cleaning and repairing of hard drives
* proper environment for the use of computer equipment:
* protection of power sources:
* surge protectors
* uninterruptible power supply (UPS)
* software shutdown
* providing advice on appropriate environmental conditions
* acceptable usage policy
 |
| destructive and malicious software protection |
| * awareness of current destructive and malicious software:
* viruses and virus signatures, Trojans, worms and other malware (destructive software)
* malware and phishing (malicious techniques)
* typical methods of transmission
* negative impact of destructive and malicious software on the workplace and individuals
 |
| * role of destructive and malicious software protection tools in:
* scheduled scanning
* detecting and deactivating destructive and malicious software
 |
| * procedures for removing destructive and malicious software:
* deactivating the destructive and malicious software
 |
| destructive and malicious software protection cont/d |
| * cleaning or removing the destructive and malicious software
* recovering lost or damaged data, including using backups to restore data, where possible
* taking action to prevent a recurrence
 |
| * reporting and recording of destructive and malicious software activity, its symptoms and action taken:
* to supervisor and ICT support staff
* through workplace documentation commonly used to maintain information about destructive and malicious software
 |

Example of mind map for components of Diagnostic testing

