For Your Eyes Only

COPYRIGHT

Document contents

Navigation option:

Continue button is disabled until user has completed all interactions on the screen.

Welcome screens:

Welcome to **For Your Eyes Only**, a course that highlights the importance of information security and explains how to implement and adhere to SP AusNet's information security policies and procedures.

The course contains four core modules:

- **What is information security and why does it matter?**

  This module explains what is meant by information security and what SP AusNet's rules and procedures are designed to protect. It also highlights the possible consequences if rules and procedures are not implemented effectively, and illustrates why security should be taken seriously.

- **How does information security affect me?**

  This module demonstrates the practical steps that you should take to help secure information within SP AusNet.

Welcome to **For Your Eyes Only**, a course that highlights the importance of information security and explains how to implement and adhere to SP AusNet's information security policies and procedures.

The course contains four core modules:

- **Information security in action**

  This module shows information security measures in action in the context of a work-based scenario. Follow the action and try and put yourself in the shoes of the characters – what would you do in their place?

- **Management and IT responsibilities**

  This module explains the additional information security responsibilities of all organisation managers and IT specialists. It is important that everyone within SP AusNet understands these responsibilities, irrespective of whether they are managers or IT specialists. As such, all employees will need to complete this module.

The security challenge

The course also contains a challenging and entertaining self-assessment, designed to test the knowledge you have gained from the course. You can choose to take either the text-based assessment or an interactive challenge.

For Your Eyes Only should take just under two hours to complete. It consists of multiple small modules (each module will be approximately 7 to 10 minutes in duration). You can go through these modules at your own pace, leave and come back to the screen where you left off. If you need assistance at any time, click on the question mark below.

Note: Shortly we will also introduce a short course on physical security at our field sites, terminal stations and sub stations.

Always follow any instructions you are given on the screen. Throughout the program you will receive instructions to click on graphics or images to learn more about a topic. Ticks will appear next to items you have completed.

SP AusNet Information Security Policy can be found on Insite at Policies & procedures → IT/BSS → Information Technology → Information Security Policy

Information about SPIRACS can be found on Insite at Policies & procedures → and click SPIRACS link.

Enjoy the course – and good luck!

Main tutorial script:

FOR YOUR EYES ONLY

Module **Page**

Module 1 - What is information security and why does it matter?

Screen 1

What is information security?

Click on each drawer of the filing cabinet for possible definitions.

[Graphic: Four drawers of filing cabinet]

If selection = drawer 1

Header text:
'CONFIDENTIALITY'

Body text:
Information security is about ensuring that information is accessible only to those authorised to have access based on job role.

If selection = drawer 2

Header text:
'INTEGRITY'

Body text:
Information security is about safeguarding the accuracy and completeness of information, and protecting the systems used to process it.

If selection = drawer 3

Header text:
'AVAILABILITY'

Body text:
Information security is about ensuring authorised users have access to information and associated assets when required.

If selection = drawer 4

Header text:
'PREVENTION OF ACCESS'

Body text:
Information security is about protecting information and information systems by 'keeping people out', i.e., preventing access.

Do you agree with this statement?

Hot-spot options

Yes

No

In each case, feedback appears on screen in response to user selection. Instructional text will appear with feedbacks depending on whether user has completed all four drawers.

If user has not completed, the instructional text reads:

Please click on another drawer.

If user has completed all four drawers, the instructional text reads:

You have now completed all four drawers. Pick a drawer to review again, or click on the forward button to continue.

If drawer 1, selection = yes, feedback as below

Correct. Maintaining confidentiality by protecting restricted information from being inappropriately disclosed is an extremely important part of information security.

If drawer 1, selection = no, feedback as below

Incorrect. Maintaining confidentiality by protecting restricted information from being inappropriately disclosed is an extremely important part of information security.

If drawer 2, selection = yes, feedback as below

Correct. Taking measures to ensure that the information held is accurate and complete and that information and systems cannot be tampered with or accidentally damaged, lost or destroyed is an important aspect of any information security strategy.

If drawer 2, selection = no, feedback as below

Incorrect. In fact taking measures to ensure that the information you hold is accurate and complete and that information and systems cannot be tampered with or accidentally damaged, lost or destroyed is an important aspect of any information security strategy.

If drawer 3, selection = yes, feedback as below

That's correct. Maintaining the availability of information is critical to all organisations, and very much a part of any information security strategy.

If drawer 3, selection = no, feedback as below

Incorrect. Maintaining the availability of information is critical to all organisations, and very much a part of any information security strategy.

If drawer 4, selection = yes, feedback as below

Incorrect. The idea is to 'control' rather than 'prevent' access to information – to make information available, but only to the appropriate people. Information security allows 'authorised' people in, but keeps the 'unauthorised' people out.

If drawer 4, selection = no, feedback as below

Correct. The idea is to 'control' rather than 'prevent' access to information. Information security allows 'authorised' people in, but keeps the 'unauthorised' people out.

Forward button moves to screen 2

Screen 2

When people talk about information security, they are in fact talking about the protection and security of:

- Information
- Information systems
- Information hardware, e.g. telephones and computers
- Information management, e.g. the procedures for handling information

[Graphic: Security guard looking after cordoned off area, the inside of the area contains a graphic representing information (a file), information systems (software box) hardware (base unit), procedures (marked 'procedures manual').

Forward button moves to screen 3

Screen 3

But what's so special about information and the assets that go with it? Why is information security so important?

The best way to answer this question is to show you some of the consequences when information security fails…

[Graphic: Security guard looking after cordoned off area, the inside of the area contains a graphic representing information (a file), information systems (software box) hardware (base unit), procedures (marked 'procedures manual').

Forward button moves to screen 4

Screen 4

To discover the types of problems an information security program is designed to protect against, click on the microphone and drag it over each of the five people below in turn to interview them.

[Graphic: Five people looking hard done by sitting next to each other on a chair. A microphone will be dragged by the user over to each of the people on the chair in turn. The user is then presented with the text below. When the user has read their story, the person is removed from the chair and the user drags the microphone to the next person]

If selection = 1, picture detail expands to fill screen, text as below

"I've been the victim of an e-mail phishing scam. The e-mail deceptively lures people to a fake website which looks similar to the original website (example: Westpac Bank). The e-mail seemed plausible enough, and without thinking, I followed the instructions and entered the information requested on the website. I've now found out I've released my personal account details to fraudsters."

If selection = 2, picture detail expands to fill screen, text as below

"I'm implementing a major security review. A disgruntled employee has stolen highly confidential information. It seems some files were copied on to a USB stick and other information was simply photographed with a camera phone. These 'sneaker' devices pose a real threat to our organisation's sensitive and confidential information."

If selection = 3, picture detail expands to fill screen, text as below

"I lost my Blackberry the other day – what a disaster! I didn't report it and not only has someone been using it and running up a big bill, but more importantly, all that organisational confidential data is now lost. Anyone could have access to it now."

If selection = 4, picture detail expands to fill screen, text as below

"My colleague has just been accused of illegally accessing sensitive organisational information and selling it to a competitor. Imagine the damage to customer confidence and our reputation when this becomes public. Now both my colleague and the organisation could face legal action – my colleague for what he did and the organisation for not having the appropriate controls in place."

If selection = 5, picture details expands to fill screen, text as below

"I've been downloading files from the Internet, and unknown to me they were infected with a virus. I didn't deliberately expose the system to a virus, but that won't stop it from causing damage to the organisation's information systems."

Forward button moves to screen 5

Screen 5

In short, information security matters because it helps to make sure that information and information assets do not:

- Fall into the wrong hands
- Become irretrievably lost or altered
- Get misused or abused in any way

Information security helps to protect the reputation and public image of an organisation. It helps to reduce risk and to prevent and reduce financial loss for SP AusNet and, in many cases, our customers.

[Graphic: Character stealing 'Confidential' file from filing cabinet which is in the background]

Forward button moves to screen 6

Screen 6

So what *are* the risks and costs of failing to protect your information, systems and equipment?

Check how much you know already by answering the questions below.

[Graphic: Old-fashioned till with four buttons – A, B, C and a return key which flashes to indicate that the user needs to click on it to show the next question. The 'no sale' that appears when the return button is pressed is replaced by either a tick or a cross. Question and feedback text will be presented next to the till]

The first question is visible when the screen loads. The user clicks on A, B or C. The feedback appears and the forward button on the till flashes to indicate the user should click on it to show the next question. When the user clicks on the forward button on the till, the feedback disappears, the next question shows and the forward button stops flashing.

Question 1 appears on screen as follows

What is the average cost of a single information security breach for a large organisation?

Hot-spot options

A) $750,000

B) $150,000

C) $50,000

If a, feedback as below

That's a bit on the high side. The average cost is a little over $150,000. But this is only an average – the costs can be much higher.

This average would be much higher except for the dramatic increases in security investment by firms and the improved technology to cope with some types of threat. Click on the arrow on the cash register to continue.

If b, feedback as below

That's right. The average cost is a little over $150,000. But this is only an average – the costs can be much higher.

This average would be much higher except for the dramatic increases in security investment by firms and the improved technology to cope with some types of threat.

Click on the arrow on the cash register to continue.

If c, feedback as below

That's incorrect – you're well below the mark. The average cost is a little over $150,000. But this is only an average – the costs can be much higher.

This average would be much higher except for the dramatic increases in security investment by firms and the improved technology to cope with some types of threat.

Click on the arrow on the cash register to continue.

Script note: Source - The CSI/FBI "2006 Computer Crime and Security Survey"

Question 2 appears on screen as follows

What is the chance of a large organisation experiencing an information security breach that causes a financial loss?

Hot-spot options

A) 10%

B) 30%

C) 60%

If c, feedback as below

You're right. The likelihood of encountering an information security problem is quite high. Needless to say, good prevention helps to reduce the likelihood of such problems affecting SP AusNet!

Click on the arrow on the cash register to continue.

Else, feedback as below

That's incorrect – in fact it's approximately a 60% chance. The likelihood of encountering an information security problem is quite high. Needless to say, good prevention helps to reduce the likelihood of such problems affecting SP AusNet.

Click on the arrow on the cash register to continue.

Script note: Source - The CSI/FBI "2006 Computer Crime and Security Survey".

Question 3 appears on screen as follows

How long on average can an organisation survive the loss of its computer facilities and systems?

Hot-spot options

A) 3-4 hours

B) 3-4 days

C) 3-4 weeks

If a, feedback as below

The average is, in fact, 3-4 days. Even so, about 10% of organisations are in serious trouble if their systems are down for just 3-4 hours. However, the loss for SP AusNet should be very minimal because of the nature of our business.

You have now answered all of the questions. Please click on the forward button at the bottom of the screen to continue.

If b, feedback as below

Yes, 3-4 days is the average time that an organisation can keep going. Even so, about 10% of organisations are in serious trouble if their systems are down for just 3-4 hours. However, the loss for SP AusNet should be very minimal because of the nature of our business.

You have now answered all of the questions. Please click on the forward button at the bottom of the screen to continue.

If c, feedback as below

No organisation can keep going for this long without its systems! The average survival time without systems is about 3-4 days. Even so, about 10% of organisations are in serious trouble if their systems are down for just 3-4 hours. However, the loss for SP AusNet should be very minimal because of the nature of our business.

You have now answered all of the questions. Please click on the forward button at the bottom of the screen to continue.

Script note: Source - 2001 Cost of Downtime Survey Results, 2001.

Forward button moves to screen 7

Screen 7

It's not just SP AusNet that takes information security seriously – governments have also legislated on the issue. Accordingly, there are a number of important privacy and security regulations in different countries that are designed to prevent the misuse or abuse of the information and information systems held by organisations around the globe.

Click on the reports below to learn more about these requirements and to find out more about ISO 27002, an internationally recognised information security standard that can help organisations to comply with regulatory requirements. Our security policy is based on ISO 27002 (we previously used the earlier version, which is ISO 17799).

[Graphic: Two reports lying on a desk, on the left is a report entitled 'Security/Privacy Regulations'. On the right is report entitled 'ISO27002'. When clicked the reports open to reveal the text specified below]

If selection is privacy/security regulations:

Precise details vary from country to country. On a general level regulations usually require organisations to maintain robust internal information systems and procedures that are adequate to ensure the confidentiality, integrity and availability of organisational data.

Such systems are usually required to be tested, documented and audited. Governments often impose fines against organisations that don't follow the regulations – so if you have responsibilities in this area, ensure you are familiar with local legislation.

If selection is ISO 27002

ISO 27002 is a key part of a growing range of internationally recognised standards for information security best practice. ISO 27002 is the standard by which most companies worldwide gauge their internal information security programs. Our security policy is based on ISO 27002 (we previously used the earlier version, which is ISO 17799).

Forward button moves to screen 8

Screen 8

In general terms, the laws affecting information security mean that organisations need to take steps to regulate the use of any information, information equipment, or systems they hold by:

- Having procedures that ensure that information is maintained and kept accurate
- Having controls in place to ensure that information and assets are properly monitored and regulated, so no unauthorised or illegal activity is allowed to pass undetected
- Putting controls in place to ensure that information can be restored

[Graphic: Three scrolls with the headings 'Personal Information', 'Information Systems' and 'Software Copyright']

Forward button moves to screen 9

Screen 9

[Graphic: Three scrolls with the headings 'Personal Information', 'Information Systems' and 'Software Copyright'. When clicked the scrolls unravel to reveal the text as follows. Each scroll has a close button that will then return the user to the three scrolls, ready to start again]

Click on the scrolls to see what you, as an employee, should not do.

If selection is Personal Information,

As an employee, you should not:

- Disclose personal information without verifiable proof of authorisation and identity
- Store, transmit, or use personal information for anything other than authorised business purposes
- Knowingly create a situation in which the security of personal information might be tampered with, breached, or put at risk in any way

If selection is Information Systems,

As an employee, you should not:

- Access or attempt to access, store, transmit or use information for which you are not authorised by job role
- Assist another person to access, store, transmit or use information for which they are not authorised by job role

If selection is Software Copyright,

As an employee, you should not:

- Make unauthorised copies of software onto a CD, USB stick or any other removable storage device

- Download or use shareware or freeware not authorised by SP AusNet
- Use software that you know to be unlicensed

Once all interactions have been completed, instructional text changes to:

You have now viewed all of the scrolls. Please click on the forward button at the bottom of the screen to continue.

Forward button moves to screen 10

Screen 10

[Graphic: Small man behind prison bars]

Legal penalties

Breaking these laws could lead to serious penalties for both you and SP AusNet.

You could be dismissed from your job, fined, or made to pay compensation. In extreme cases, such as 'hacking' or identity theft, you might even go to prison. SP AusNet could also be prosecuted and fined if we were found not to have appropriate procedures and controls in place.

Clearly, it's in your best interest to take information security seriously – not just because of the damage a breach could cause for SP AusNet and our clients, but also because of the consequences that you personally might face, if you were to break the law.

You will find out more about how good information security practice affects your job role as you complete this course.

Forward button moves to screen 11

Screen 11

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

What is information security and why does it matter?

Information security is about ensuring the confidentiality, integrity and availability of information assets by protecting them from potential loss, damage, destruction or theft.

Information assets include:

- Any information held or maintained by SP AusNet
- Any systems and/or equipment used to store, process and transmit information
- Any software applications used to access or manipulate information

Forward button moves to screen 12

Screen 12

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

What is information security and why does it matter?

The three main principles with regard to protecting these assets are:

- **Confidentiality**
  Controlling access to information and keeping information confidential, where appropriate.
- **Integrity**
  Protecting information and information systems from unauthorised changes, corruption, damage or destruction.
- **Availability**
  Making sure that information can be made continuously available to all relevant authorised personnel.

Forward button moves to screen 13

Screen 13

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

What is information security and why does it matter?

The purpose of information security policies and procedures is to ensure that everyone within SP AusNet, including you, takes the precautions needed in order to keep information, information assets and information systems as secure as possible.

Any loss, destruction, damage, misuse or abuse of information and assets could:

- Put your job at risk
- Expose SP AusNet to potential financial loss
- Leave you and SP AusNet facing prosecution and substantial fines
- Damage our organisation's reputation
- Damage our organisation's relationship with customers and other shareholders
- In extreme cases, put SP AusNet out of business

It's not surprising, therefore, that SP AusNet takes information security so seriously – and so should you.

Forward button exits module

Module 2 - How does information security affect me?

Module **Page**

Module 2a - Entry control

Screen 1

Entry control is for the security and protection of the workforce, as much as for the protection of SP AusNet's information and other assets. You wouldn't want just anyone gaining unauthorised entry to your home and wandering around.

And it's the same with places of work.

[Graphic: Graphic of a visitor's badge saying 'Authorised Visitor']

SP AusNet needs to keep 'unauthorised' people out of our premises.

Forward button moves to screen 2

Screen 2

Click on each of the four items below for advice on your responsibilities in relation to entry control.

[Graphic: Small people looking at items – 1] a security guard standing by entrance door, 2) Signing in book alongside an 'Authorised Visitor' badge, 3) 'ID badge' on a clip, and 4) a 'Fire Exit' sign]

If user selects security guard by entrance

Monitoring door use enhances physical security, so you should never leave secure external doors open, even if you are heading out for a quick break. Watch out for 'piggybacking' (holding doors open for people you don't know) – the individual might be exploiting your courtesy to gain unauthorised entry to the premises! Be vigilant too with doors to data centres, wiring closets or other restricted areas within the building; never leave them propped open.

If user selects visitors badge / sign-in book

All visitors should be checked in properly- their details should be recorded in the visitor's log and they should be issued with a visitor's ID. Your visitors are your responsibility. Always follow SP AusNet's procedures when you are expecting visitors to your workplace. Make sure that they are wearing their visitor ID, that they are accompanied at all times while on the premises and that they are made aware of any areas that are off limits.

If user selects ID badge on a clip

Your ID badge identifies you as a member of staff. It distinguishes you from other people on the premises, including possible 'intruders'. Always display your ID badge while at work.

In many SP AusNet locations employees are issued with an electronic pass, which grants access rights according to the responsibilities and requirements of their job. Be sure to protect your ID badge or electronic pass/keypad code from loss or theft.

If user selects fire exit sign

Vulnerable physical entry points are those that combine isolation with relatively easy access, such as:

- Fire exits

- Loading/delivery areas
- Ground floor windows
- Unmanned field sites

Every time you work in or near a vulnerable entry point, ensure you remain vigilant at all times, following all appropriate security procedures.

Forward button moves to screen 3

Screen 3

Rules for entry control

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Visitor control

- Ensure that all visitors are checked in properly
- Make sure that visitors are accompanied at all times
- If you spot someone you don't know without an ID, politely ask them to display their ID. If they don't have ID, escort them to reception immediately
- Always wear your ID badge while at work to distinguish yourself from visitors

Forward button moves to screen 4

Screen 4

Rules for entry control

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Electronic pass control

- Keep your ID badge or pass with you – never leave it lying around
- Never lend your ID badge or pass to any other person
- If your ID badge or pass is lost or stolen, report it to Building Services immediately

Forward button moves to screen 5

Screen 5

Rules for entry control

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Physical security

- Never leave exit doors propped open
- Always close doors that require authorised access behind you
- Don't let people 'piggyback' in after you
- Remain vigilant and report any suspicious activity immediately

- Inform Building Services and/or your manager if you see any unattended briefcases, packages or luggage in the lobby or reception area

Forward button exits module

Module 2b - Clear desk and secure disposal policies

Screen 1

Cleaning up after yourself and keeping your desk clear is one of the most important contributions you can make to information security.

If things are left lying around, then the chances that they will be misplaced, scanned or 'picked up' by someone who shouldn't have them are greatly increased. That's the main reason why many organisations operate a strict 'clear desk policy'.

[Graphic: A clean tidy desk with a shredder alongside it]

Forward button moves to screen 2

Screen 2

Look around this office and click on any items where the clear desk policy has obviously not been followed. You have 13 items to find.

Number of items remaining counts down as user clicks each one

[When user clicks on item, the appropriate text is displayed. As each item is collected the item is erased from screen or animates]

Files labelled 'Project X' left lying in in-tray

Desk drawers are unlocked with 'personnel' 'file in it, key in lock

Computer screen is active, shows document headed 'Account Information'

Flipchart (showing what appear to be sales figures) labelled 'Competitive Intelligence'

'Confidential' pages left un-filed, on top of filing cabinet

Shelves on wall containing box files, labelled 'Confidential files'

Printer, sitting somewhere near the PC on the desk – where the user can spot it easily, with printed off document on it headed 'Confidential'

CD in drive

Stick-on note with 'Password = 12345' written on it

'Confidential' paper in a waste paper bin

Laptop with the words "Unsecured Wireless Network" on monitor

Stick-on note saying 'Joe's home: 734-8729'

Filing cabinet left open – folders are half-in-half-out (when closed show a key/padlock)]

When selection = files in in-tray, text as below

Empty in-trays and clear your work area before leaving it.

When selection = desk drawer unlocked, text as below

Lock drawers and keep keys in a secure place, away from view.

When selection = active computer screen, text as below

Secure your computer when leaving your work area unattended.

When selection = flipchart, text as below

Clear sensitive or confidential information from flipcharts and other presentation equipment, such as whiteboards and smartboards.

When selection = un-filed pages on cabinet, text as below

File documents away, in line with their degree of sensitivity, when you have finished with them.

When selection = shelves, text as below

Keep Confidential, Private and Sensitive information in secure storage.

When selection = printer

Information should never be left lying around on unattended printers or fax machines.

When selection = CD in drive

CDs and other removable storage devices should be stored away properly when not in use.

When selection = password on stick-on note

Passwords should be committed to memory and never written down.

When selection = waste paper bin

Wastebaskets or recycle bins are fine for ordinary rubbish but not for Confidential, Private or Sensitive documents, which should be disposed of securely.

When selection = Laptop

Portable equipment should never be left lying around unattended.

When selection = Joe's home number on post it note

Personal information should be kept secure at all times.

When selection = filing cabinet, text as below

Keep filing cabinets shut and locked, when unattended.

When user has clicked on all items message appears as follows:

Well done! You have identified all 13 items.

Click the forward button to continue.

Forward button moves to screen 3

Screen 3

[Graphic: Clear desk with a laptop and an external hard drive]

Keeping your desk clear is one of the most important contributions you can make to information security, but it mainly deals with current equipment and information.

Obsolete devices and information can still hold sensitive and confidential details so they must be disposed of securely and safely when no longer required.

There are often reports in the press detailing how sensitive information has leaked into the public domain due to careless disposal of electronic or paper-based information.

SP AusNet has placed locked recycle bins close to printers and you are encouraged to use these bins to recycle confidential paper-based information. For the disposal of other electronic information, contact your Information Security Manager.

Forward button moves to screen 4

Screen 4

[Graphic: Two separate montage graphics representing items to be disposed of and disposal methods:

1) Disposal items: Table with sign above it, saying 'FOR IMMEDIATE DISPOSAL', on table are: a) Old looking PC, b) A pile of paper files, c) A pile of CDs titled 'Backup' and a USB stick.

2) Disposal methods: a) A table with the sign 'Reusable items'. b) Disposal bin and shredder labelled 'Paper only' c) Man in overalls with logo "Secure Disposal Services']

Equipment and information should be disposed of securely and safely when no longer required. Click on each item and drag it over the most suitable method of disposal.

*Computer can be dragged onto the "Reusable items" table **OR** into "Secure Disposal Services"*

*CDs and USB stick can be dragged onto the "Reusable items" table **OR** into "Secure Disposal Services"*

*Paper can be only be dragged into "Paper only" **OR** into "Secure Disposal Services"*

N.B. if item drag/drop to wrong method it returns to its original place and user can attempt interaction again.

If user drag/drop PC into "Reusable items", Message appears on screen 'Deleting files' and then 'HARD DISK WIPED and REFORMATTED', Feedback text as below:

In some cases, computer equipment can be reused or recycled. In others, the equipment may be disposed of using secure disposal services. The choice will often depend on the type of equipment and our secure disposal policy. Before any computer equipment can be reused, any useful data must be backed up and all memory should then be deleted and reformatted. Check with the IT-Service Desk for information about wiping data from equipment, as this isn't the same as deleting it and may require specialist software.

If user drag/drop PC into "Secure disposal", Message appears on screen 'Deleting files' and then 'HARD DISK WIPED and REFORMATTED', Feedback text as below:

In some cases, computer equipment can be disposed of using secure disposal services. In others, the equipment may be reused or recycled. The choice will often depend on the type of equipment and our secure disposal policy. Before any computer equipment can be disposed of, any useful data must be backed up and all memory should then be deleted and reformatted. Check with the IT-Service Desk for information about wiping data from equipment, as this isn't the same as deleting it and may require specialist software.

If user drag/drop old paper files into "Paper only", the files transform gradually into a pile of shredded paper in the shredder and the bin bulges as though full. Feedback text as below:

Paper documents containing any sort of restricted information (often classified as Confidential, Private or Sensitive) should be either destroyed or disposed of in locked recycle bins. Familiarise yourself with our policy and procedures for secure disposal.

If user drag/drop old paper files into "Secure Disposal", the pile of files gradually disappear. Feedback text as below:

Paper documents containing any sort of restricted information (often classified as Confidential, Private or Sensitive) should be either destroyed or disposed of in locked recycle bins. Familiarise yourself with our policy and procedures for secure disposal.

If user drag/drop CDs / USB stick into "Secure Disposal" - label flashes on CDs saying 'BACK UP' then changes to 'CLEAN DISKS', feedback text as below

Reusable and removable storage devices such as external hard drives, USB sticks, rewrite-able CDs (CD-RW) etc. should be backed up then all memory deleted and reformatted before being disposed of. Non-erasable CDs should be destroyed or put into a 'special items' disposal bin.

If user drag/drop CDs / USB stick into "Reusable items" - label flashes on CDs saying 'BACK UP' then changes to 'CLEAN DISKS', feedback text as below

Reusable and removable storage devices such as external hard drives, USB sticks, rewrite-able CDs (CD-RW) etc. should be backed up then all memory deleted and reformatted before being distributed for reuse. Non-erasable CDs should be destroyed or put into a 'special items' disposal bin.

If user drags any incorrectly, the following feedback appears:

That's not correct. Try again.

Once all interactions have been completed, instructional text changes to:

You have now selected all the interactions. Please click on the forward button at the bottom of the screen to continue.

Forward button moves to screen 5

Screen 5

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for clear desk policy

- Empty in-trays and clear your work area of all restricted information (for example anything classified as Confidential, Private or Sensitive) before leaving, even for short periods
- Lock drawers and store keys in a secure place, away from view
- Secure your computer when leaving your work area unattended
- Clear restricted information from flipcharts and other presentation equipment, such as whiteboards, even in meeting and conference rooms
- Keep filing cabinets shut and locked, when unattended
- File documents away when you have finished with them
- Store all information appropriately according to its data classification level (Confidential, Private, Sensitive or Public)

Forward button moves to screen 6

Screen 6

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for secure disposal of data

- The internal memory in equipment should be wiped clean of data/reformatted before the equipment is disposed of, recycled, or distributed for reuse
- Paper documents containing any form of restricted information should be destroyed, for example by shredding, or disposed of in locked recycle bins
- Reusable storage devices should be wiped clean of data and reformatted before being disposed of or distributed for reuse, and read-only CDs should be destroyed

Forward button exits module

Module 2c - Password management

Screen 1

Passwords are:

- Simple
- Inexpensive
- Effective when used correctly

They are used the world over to control access to systems and information, but their effectiveness relies on you.

[Graphic: Rubik's cube as used on sub-menu]

Forward button moves to screen 2

Screen 2

[Graphic: Combination lock showing User ID with a small person holding key with key tag which has asterisks that represent the user's password, slight turn of key by 45 degrees in the lock which opens the top of the padlock]

Your password is linked to a personal User ID. The User ID is the electronic identity assigned to you by SP AusNet and which identifies you as an authorised user. The password is a separate validation code, chosen by you, that works in conjunction with your User ID in a two-factor authentication process.

When you 'log on', the system recognises your User ID and asks you to key in your password.

If the password you type in matches the one stored for your User ID, then the system has validated you as the authorised user and lets you in. It's as simple as that.

Forward button moves to screen 3

Screen 3

The goal of password management is to prevent 'impostors' from assuming the identity of another person, (such as you), in order to gain unauthorised access to the system.

[Graphic: Same graphic as screen 6 but with different shaped key and different coloured key tag – representing same User ID but different password]

Keeping your password confidential helps to ensure that others cannot access information systems or information assets using your electronic identity.

Make sure you know and follow SP AusNet's password policies and procedures.

Forward button moves to screen 3

Screen 4

How closely does what you do at the moment compare with best practice for password management?

Answer the following questions truthfully.

How many people know your password?

Hot-spot options

A) Anyone who needs it

B) A couple of people whom I trust

C) Nobody except me

Click on a padlock option.

If a or b, feedback text as below

This is not good practice. You should take greater care than this with your password. No one should know your password, except you.

If c, feedback text as below

That's good practice. No one should know your password, except you.

[Graphic: Combination lock with three buttons on it – A, B and C which the user presses to select their answer]

Forward button moves to screen 5

Screen 5

How closely does what you do at the moment compare with best practice for password management?

Answer the following questions truthfully.

How often do you change your password?

Hot-spot options

A) I have never changed it

B) Every now and then

C) Regularly

Click on a padlock option.

If a or b, feedback text as below

This is not good practice. In fact you should change your password regularly. This reduces the risk of someone else discovering your password, and having the opportunity to use it.

If c, feedback text as below

That's good practice. Regularly changing your password reduces the risk that someone else will discover it, and have an opportunity to use it.

[Graphic: Combination lock with three buttons on it – A, B and C which the user presses to select their answer]

Forward button moves to screen 6

Screen 6

How closely does what you do at the moment compare with best practice for password management?

Answer the following questions truthfully.

How do you remember your password?

Hot-spot options

A) I keep it on a stick-on note next to my computer

B) I keep it written on a piece of paper, in my wallet

C) I commit it to memory

Click on a padlock option.

If a or b, feedback text as below

This is not good practice. Committing your password to memory is the only failsafe way to keep it secret from others.

If c, feedback text as below

That's good practice. Committing your password to memory is the only failsafe way to keep it secret from others.

[Graphic: Combination lock with three buttons on it – A, B and C which the user presses to select their answer]

Forward button moves to screen 7

Screen 7

Your password should mean something to you – but not be so obvious that others will guess it. You should change your password regularly – according to SP AusNet's policy. This reduces the risk of someone discovering your password, and taking the opportunity to use it.

Never write it down; not on a stick-on note on your screen, not on the inside cover of your desk diary and not even on a slip of paper in your wallet. The only failsafe way to make sure that your password is secret is to commit it to memory.

[Graphic: Small character arranging a line of numbers and letters]

Forward button moves to screen 8

Screen 8

Some passwords are easier to break than others. To demonstrate this, try figuring out the password of the person whose desk is pictured below.

There are plenty of clues lying around. Study the clues, then type the password onto the computer screen and hit the Enter key. You have 60 seconds from your first keystroke to have as many attempts as you can, so keep an eye on the timer.

[Graphic: Montage of graphics representing a person's desk. Laptop; desk calendar turned to 'December, 22' comment written on calendar says 'my birthday!!'; mug with a generic looking logo on; photograph of a white dog in a frame, name beneath says 'Prince'; toy car on desk, with registration 195 TFL; child's painting which says 'to daddy, love from Cassie'. Official looking envelope which says 'Tim Baldwin, 195 Salt Dr., Melbourne,

VIC 3000, digital clock on desk which acts as counter with '60' (seconds) on it in large red font. When password is keyed in they should be displayed as asterisks]

Correct password = CASSIE (non-case sensitive).

As user keys in passwords asterisks appear on screen in picture, where flashing cursor shows.

Desk clock starts timing, as soon as user starts to key in.

When user hits enter and password is incorrect, message appears on terminal screen, as below:

ACCESS DENIED – TRY AGAIN

If user does not get password correct – timer flashes '0' and message appears on terminal screen, as below:

ACCESS DENIED – UNAUTHORISED USER

When user hits enter and password is correct, message appears on screen as below:

PASSWORD ACCEPTED – ACCESS GRANTED

If guessed in one second, text appears as below:

That took you 1 second – not much time at all!

A password needs to be something that people won't easily 'guess'. Family names, car number plates and key dates such as birthdays should all be avoided.

Can you be sure that *your* password cannot be broken this easily?

If guessed in 2-60 seconds text appears as below:

That took you *(Number of seconds taken)* seconds – not much time at all!

A password needs to be something that people won't easily 'guess'. Family names, car number plates and key dates such as birthdays should all be avoided.

Can you be sure that *your* password cannot be broken this easily?

Following text appears if password is not guessed

Bad luck – you're out of time. The password you are looking for is Cassie – the daughter of the man who sits at this desk. You would have discovered the password eventually if your time hadn't run out. A password needs to be something that people won't easily 'guess'. Family names, car number plates and key dates such as birthdays should all be avoided.

Forward button moves to screen 9

Screen 9

A strong password should be:

- Easy for you to remember but difficult for others to guess
- At least eight characters long
- A mix of upper and lower case letters, numbers and special characters

You could also try a 'first-character' password. Think of a phrase that includes a number that you can remember easily. For example: 'I met Margaret at work 3 years ago'. Now take the first letters to form your password: ImM@w3ya … Be creative!

[Graphic: Guard standing in front of a padlocked password, represented by 3D asterisks]

Forward button moves to screen 10

Screen 10

Examples of some secure passwords are as follows:

- L0nd0nC!ty
- 1luvFrid&y$
- W3lc0me!”£
- Bull$2w!n

And examples of passwords that are not secure:

- 12345
- George052000
- Name of organisation
- Log on credentials
- Words straight from a dictionary

Keep your password effective – change it regularly, when the system prompts, or immediately if you suspect someone else knows it, and never reuse an old one.

[Graphic: Rubik’s cube each a mix of upper and lower case letters, numbers and special characters, one on each square]

Forward button moves to screen 11

Screen 11

Which of the following follows the rules for a strong password?

Hot-spot options

A) Amanda12345

B) F1DO

C) Hawa!!

D) Tl0tf&thot8

Answer = D

If selection = D

Yes – this password is 8 characters long and includes a mix of upper and lower case letters together with a numeric character and a special character.

If selection ≠ D

No, a strong password should be at least 8 characters long and include a mix of upper and lower case letters, numbers and special characters. The best one from this list is therefore, Tl0tf&thot8.

[Graphic: Small character arranging a line of numbers and letters (as in screen 7)]

Forward button moves to screen 12

Screen 12

If you're *still* not convinced that password security matters, then here are some sobering thoughts.

If someone obtains your password, they can:

- Access and use SP AusNet's information system
- Access and use data for which they may not be authorised
- Make unauthorised changes, deletions or additions to data on the system
- Copy any data you have access rights to and remove it from the premises, and
- Do all this while pretending to be YOU

Their actions will be traced back to you, through your User ID. You could be held accountable, in part, for their actions.

That's a pretty strong incentive to follow the rules for password security!

[Graphic: Small person shrugging their shoulders, looking up at someone's shoes which represent authority]

Forward button moves to screen 13

Screen 13

Rules for password management

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Choosing passwords

- Avoid obvious words, dates or numbers, especially those that have personal associations such as birthdays, names of pets or family names
- Use a mix of upper and lower case letters, numbers and special characters
- Make your password at least eight characters in length
- Avoid words that appear in the dictionary
- Don't make the password so long or complicated that you will have trouble remembering it!

Forward button moves to screen 14

Screen 14

Rules for password management

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Using passwords

- Keep your password secret – reveal it to no one
- Commit it to memory
- Change it regularly
- Do not re-use your password

Forward button exits module

Module 2d - Classifying information

Screen 1

Why classify documents?

Different types of information need to be managed in different ways, as some are more confidential, sensitive or valuable than others. For example, sensitive sales information and last year's Annual Report should obviously be treated differently.

Because of this, businesses need systems to classify different documents, whether they are in hard copy or electronic form.

These classification systems need to be supported by policies and procedures for the different types of documents.

The need for information classification will vary greatly across organisations and will depend on the nature of the organisation's business. We will provide you with more information about classifying information in due course of time. Some generic and widely used classification examples are provided in the next few slides. This classification can be used as a guideline until we provide specific classification information.

[Graphic: Group of people looking up at a whiteboard with headings 'Confidential', 'Private', 'Sensitive', and 'Public'.]

Forward button moves to screen 2

Screen 2

Access management

Access management controls regulate who can access what information – and how. Typically, an organisation will select an ascending order of three or four classifications and although it can choose any label, many opt for the following: Confidential, Private, Sensitive and Public.

Regardless of its format, all data should be protected according to its classification whether at rest or in transit.

Click on each of the classifications below to learn more.

[Graphic: 'Confidential', 'Private', 'Sensitive' and 'Public' written on a slant as though using an inkpad stamp – coloured red, yellow, yellow, green respectively. Arrange stamps in traffic light order on screen with the two yellow stamps on the same level.]

[Graphic: PC behind curtain]

If selection = 'Confidential' move to screen 3

If selection = 'Private' move to screen 4

If selection = 'Sensitive' move to screen 5

If selection = 'Public' move to screen 6

Forward button moves to screen 7

Screen 3

Confidential

This is the highest level of classification. Information classified as Confidential:

- Is for use within SP AusNet only
- Could, if inappropriately disclosed, severely damage SP AusNet's business interests and professional reputation, seriously undermine customer confidence, and/or help the competition
- Will have a very limited circulation, and will usually be known only to a select few within SP AusNet's, e.g. the board of directors and most senior level of management
- Could include trade secrets, strategic plans, health care information, programming code and any other information that keeps us competitive

[Graphic: Padlock image - graphic is same colour as the stamp (i.e. red)]

Forward button returns to screen 2

Screen 4

Private

This is a middle level of classification. Private information is personal information that:

- Is for use only within SP AusNet
- If inappropriately disclosed, could adversely affect us or our personnel
- Will be disclosed only on a 'need to know' basis – information will be made available according to what people need to know in order to carry out their normal work duties
- Could include personnel records, work history and medical information

[Graphic: Employee swiping pass card in to reader by a closed (locked) office door marked "Private" – door sign is same colour as the stamp]

Forward button returns to screen 2

Screen 5

Sensitive

This too is a middle level of classification. Sensitive information is information that:

- Requires special precautions to ensure its integrity and completeness
- Must be protected from unauthorised access, modification and deletion
- Will be disclosed only on a 'need to know' basis
- If inappropriately disclosed, could expose SP AusNet to risk, or result in legal liability for SP AusNet and the individual
- Could include financial data, profit earnings and forecasts and details of projects

[Graphic: Man carrying folder marked "Sensitive" - folder is same colour as the stamp (yellow)]

Forward button returns to screen 2

Screen 6

Public

This is the lowest level of classification. Information classified as Public:

- Would not create an adverse impact for SP AusNet or its personnel if released to the public, even though disclosure may not be welcome
- May, in some cases, have been authorised for release into the public domain and therefore has no confidentiality attached to it at all
- Could include details of upcoming projects and published reports

[Graphic: A small woman pulling open drawer of filing cabinet - folder graphic is same colour as the stamp (green)]

Forward button returns to screen 2

Screen 7

[Graphic: Envelope with a string of encrypted data circling it]

In today's business world, the majority of documents are saved and stored – and often distributed – in electronic format. Although this is more convenient, it often can be less secure. After all, you can't lock an e-mail attachment in your desk drawer.

To prevent unauthorised access, many organisations choose to encrypt many of their documents prior to storage or transmission. The following are examples of documents that could require encryption:

- Financial information
- Client lists
- Sales figures
- User IDs and passwords
- Security risks and vulnerabilities
- Audit findings
- Trade secrets
- Business negotiations
- Security incidents
- Employee directories

Forward button moves to screen 8

Screen 8

What should you do?

Now imagine yourself in the following scenario:

You work in the Research & Development division of a large organisation, and are completing Confidential plans for a new product. You decide to spend the next day working from home. Should you:

A) Take the documents home in an unmarked envelope

B) Take the documents home in an envelope marked Confidential

C) Decide not to take them from the office at all

[Graphic: A, B, C buttons]

If selection = option A or B

That's incorrect. Documents classified as Confidential should never be taken out of the office – regardless of the type of envelope they are in.

If selection = option C

Correct. Documents classified as Confidential should never be taken out of the office – regardless of the type of envelope they are in.

[Graphic: Queue of document folders at security checkpoint]

Forward button moves to screen 9

Screen 9

What should you do?

You've left the Confidential documents in the office, but still decide to work from your home office. You want to pass on the report you have written to some of your colleagues – some of whom work in a different office.

You decide to send the report, which is classified as Sensitive, by e-mail. Who should you send it to?

A) Only those people who are actually working on the project

B) People working on the project, plus all of their managers

C) All organisational heads of department – who can then pass it on to any of their staff who are working on the project

[Graphic: A, B, C buttons]

If selection = option A

Yes. Documents classified as Sensitive should only be made accessible on a 'need to know' basis, and should only be e-mailed if appropriate encryption has been used.

If selection = option B or C

No. Documents classified as Sensitive should only be made accessible on a 'need to know' basis, and should only be e-mailed if appropriate encryption has been used.

[Graphic: PC with nothing onscreen]

Forward button moves to screen 9

Screen 10

Rules for handling classified information

Different types of information need to be treated in different ways depending on the degree of confidentiality and control required.

- Confidential, Private and Sensitive electronic documents should be protected by using passwords or data encryption
- Exercise caution when sending documents by e-mail
- Hard copy Confidential, Private and Sensitive documents should be secured appropriately when not in use, and should not be worked on in public places
- Confidential documents should not usually be taken out of the office

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Forward button exits module

Module 2e - Systems integrity

Screen 1

You need to think of SP AusNet's computer network, hardware and software applications as a single, secure information system.

SP AusNet's policies, procedures and processes guard and protect the system, as long as it remains unchanged.

Even a very small change or lapse in protocol can create a loophole, exposing the system and what it contains to potential risk.

Click on each of the two graphics for some examples.

[Graphic: Small people opening box of software labelled 'Software' go to screen 2, small people opening large box of equipment which says 'Hardware' and 'This way up' – go to screen 3]

If selection = 'Software' move to screen 2

If selection = 'Hardware' move to screen 3

Forward button moves to screen 4

Screen 2

[Graphic: Contents of box from previous screen, i.e. user guide, CD etc]

Installation of software

Use of unauthorised software or unauthorised copies of software introduces a variety of risks to SP AusNet.

- If it's a copy, then it may be illegal – in which case both you and SP AusNet may be in breach of the manufacturer's licensing terms and conditions, which could result in fines and legal action
- Freeware, shareware and unlicensed copies of software could all contain computer viruses, Trojan horses, spyware or other undesirable (and often hidden) content – in which case you are risking corruption and damage to both your own and the rest of SP AusNet's systems and data
- It could clash with other systems or software, causing them to fail; or it could exploit a weakness in the system's existing security controls, leaving your desktop PC and SP AusNet's entire information system exposed to unauthorised access

Therefore, software should only be installed according to SP AusNet's procedures.

Forward button returns to screen 1

Screen 3

[Graphic: Contents of box from previous screen]

Installation of hardware

Using hardware that (although legitimate in itself) has not been approved by SP AusNet introduces a range of dangers:

- It could cause your existing hardware or software to fail
- It could invalidate warranties on your equipment, which could have a financial impact

And perhaps most importantly of all…

- It could undermine your system's security controls by allowing others to exploit new internal or external routes into the system

From a security point of view, therefore, it is important that you follow SP AusNet's approved procedures for evaluating, installing and maintaining new hardware.

Forward button returns to screen 1

Screen 4

[Graphic: A person carrying a monitor, walking away from a desk on which there is now only a keyboard and mouse with cables leading to the space from which the monitor has been removed]

Just as with installation, the removal of any hardware or software should first be approved, then completed according to defined procedures.

If a hardware connection or a piece of software is missing the system may cease to function as intended; this could result in a breach of security, as well as causing many other problems.

It is therefore vital to ensure that SP AusNet's hardware and software platform remains complete and stable.

Forward button moves to screen 4a

Screen 4a

[Graphic: A server with 3 removable blades and a PC with an external hard drive]

Backups

A backup is an exact copy of the system (or part of the system), taken as a deliberate step, so that in the event of a system failure of any type, the backup can be restored to ensure that SP AusNet can conduct its business as usual.

Backups help to maintain the integrity and availability of our information system and assets at all times.

SP AusNet's policies for backups are closely related to the business continuity and disaster recovery plans.

Backups for shared drives are often automated – but you may need to take your own backups of any files stored on your PC's local drive and on your laptop.

Forward button moves to screen 4b

Screen 4b

There are three basic principles that you need to apply to backups.

Click on each of the backup drives in the cabinet to work through these principles.

[Graphic: Close up of a server with 3 removable blades. The user clicks on each of these blades to display the three principles – can also toggle between them]

Principle 1: Make backups regularly

The frequency with which you make backups will depend on the complexity of the work, its criticality, and the degree and frequency of any changes.

In some cases daily backups are necessary. For example, financial information, databases related to clients, marketing and other plans are in daily use and subject to constant change.

Many organisations run a full system backup every 24 hours, running automatically every night.

Principle 2: Use the same or equal controls

Backups should have the same (or equal) controls that the production system uses to protect the data in question.

So backups should always be made in line with data classification labels used by the production system.

Principle 3: Store backups securely

In case of a disaster, the backups must themselves be undamaged and ready to be installed; so SP AusNet keeps one set on-site and another off-site in a secure location. Backups should be kept in a fireproof safe.

You may need to consider the same protocol for your own backups. For all your backup and restore requirements contact the IT-Service Desk.

Forward button moves to screen 5

Screen 5

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for systems integrity

- Never tamper with or make unauthorised changes to SP AusNet's information system or its configuration without authorisation. Discuss the change requirement with your CAB Manager
- Never install or remove software or hardware without the proper authorisation
- Properly document any authorised installations or changes that are made
- Always ask the IT-Service Desk or designated personnel if you have a question about or problem with the system
- Never try to rectify system problems yourself, unless authorised and qualified to do so
- Always make sure you know where and from whom to obtain backups, in the case of a systems failure
- Always backup any files on your own PC or laptop that are not covered by the system's automated backup procedures

- Always make sure that backups are made regularly, stored securely and that they use the same or equal controls that the production system uses

Forward button exits module

Module 2f - Malware

Screen 1

Malware is a generic name for any form of malicious and unwanted computer program. Examples of malware include:

- Viruses
- Trojan horses
- Adware
- Spyware
- Bots

Malware poses a real and constant threat to information security. Consequently, SP AusNet has implemented sophisticated security controls including firewalls, virus and spyware detection, as well as spam and spyware filters.

Although this protection may be running automatically, it is important that you know about malware and can recognise its effects, so that you can help protect against it.

[Graphic: A menacing looking bug pushing against (and trying to get round) a screen being held up by smaller people. (The mesh is a representation of a firewall)]

Forward button moves to screen 2

Screen 2

[Graphic: PC screen]

Viruses and Trojan horses

Computer viruses and destructive code can be hidden behind seemingly innocent programs. These programs are called Trojan horses and they can pose a threat to any information system.

This PC has been infected with a virus. Click on the screen for more information on the effect this virus could have.

- Viruses can corrupt and damage your data *[text on screen changes to read 'data loss']*
- Viruses can make your systems malfunction *[text on screen changes to read 'error']*
- Viruses can destroy entire information systems, rendering them inoperable *[text changes to read 'total failure']*

After clicking instructional text changes to:

Click on the screen again.

Once user has clicked on the screen three times the instructional text changes to:

Click on the forward button to continue.

Forward button moves to screen 3

Screen 3

[Graphic: One PC with modem, with biohazard symbol on monitor]
Imagine that you open your e-mail program, and see an e-mail from what looks to be a good friend. The subject of the e-mail is 'Re: Thanks'. You open the attachment that accompanied the e-mail.

Click on the PC to see what happens.

[Graphic: Additional three PCs are shown, each with modems. The modem on the original PC flashes representing the virus being sent to the three other PCs, biohazard symbols appears on all PC monitors in turn]

This e-mail carried a virus. Without being aware of it, you have now sent the virus to all of those people whose e-mail addresses are saved in your address book – including suppliers and colleagues.

Because your PC is linked to a network, the virus is spread throughout SP AusNet. And this could all happen in a matter of minutes!

Forward button moves to screen 4

Screen 4

Any form of malware is bad news. But where do these malicious programs come from?

Click on each of the four pictures below to identify possible sources.

If virus 1 [Graphic: virus bug on top of an envelope marked with the '@' e-mail symbol]

E-mails can carry malware either in attachments or behind links to websites included in the e-mail itself.

If virus 2 [Graphic: virus bug on top of a piece of fibre-optic cable]

Files downloaded from the Internet may contain viruses or other malicious code, but even just visiting a website could lead to malware being downloaded. It is not unknown for hackers to hide malware on a perfectly legitimate website so that when you connect to it, you unknowingly download the malware.

If virus 3 [Graphic: virus bug on top of a CD]

CDs and other portable data storage devices (USB sticks, external hard drives etc.) can pass on malware infections. Before using them you need to be able to verify the source and integrity of the media. This is why it is important not to use copies and pirated software.

If virus 4 [Graphic: virus bug on top of a 'software' box]

Software from a questionable source, freeware and shareware are all potential carriers of malware. You need to be able to verify the source and integrity of any software before you load it on to your computer.

Forward button moves to screen 5

Screen 5

Although some malware is designed to cause data loss, most of the malicious software distributed has been designed to generate profits for its authors.

In recent years, the majority of widespread viruses and Trojans have been designed to take control of users' computers so that they can be exploited.

Infected computers (known as zombie computers) are used to send spam e-mails to lure people into giving away their personal information, to unknowingly host prohibited data such as illegal images, or to launch attacks to render websites unavailable as a form of extortion.

[Graphic: Several linked computers – a virus starts on one and spreads to others]

Forward button moves to screen 6

Screen 6

Spyware and Adware

Spyware is a computer program that secretly gathers information from your computer. It can log the Internet sites you visit and monitor your keystrokes to discover your passwords and other personal details.

The spyware then forwards this information to someone else without your authorisation or knowledge. The recipient may then be able to access your computer, use your applications, copy your files, steal personal information, and even wipe your hard drive clean.

Adware is similar to spyware but often redirects you to specific Internet sites and causes unwanted pop-up adverts for sites and products to appear on your computer screen.

[Graphic: PC and spyware mesh to illustrate the capturing of financial data]

Forward button moves to screen 7

Screen 7

Spyware and adware can invade your privacy and threaten SP AusNet's security.

Adware and spyware can be installed on your computer because you agreed to install them by:

- Visiting a website
- Accepting terms hidden inside a lengthy user agreement for another program

[Graphic: PC with lengthy user agreement on the screen – at the bottom of the U/A is a check-box to accept the agreement]

Forward button moves to screen 8

Screen 8

A term often associated with malware is 'bot' – from the term robot.

Not all bots are malicious or unwanted - but they can be exploited by criminals and used as remote attack tools. Malicious bots are mostly targeted at home computer users but, as with all malware, they could be aimed at organisations too.

Malicious bots will often take control of a computer, and use it to send out spam e-mails and to infect other computers. In this way a whole network of infected machines – known as a botnet – is created. In one case, law enforcement agencies closed down a botnet of 1.5 million computers!

[Graphic: data robots – a bot]

Forward button moves to screen 9

Screen 9

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for combating malware

- Be cautious about what data you accept, and from whom
- Don't open any unexpected e-mail attachments
- Use any protection or virus scanning software you are provided with for both incoming and outgoing e-mails
- If you suspect your PC or laptop has been affected by any form of malware, stop now and report it immediately
- Don't attempt to fix a virus or remove a malware program yourself – always seek help from qualified personnel
- The best defence against all types of malware is to be wary of any unusual or suspicious behaviour on your computer

Forward button exits module

Module 2g - Electronic communication

Screen 1

[Graphic: Picture of an e-mail subtitled 'E-mail'; picture of a fax subtitled 'Fax'; picture of an IMS message subtitled 'IMS'; picture of a group of three business people subtitled 'Third Parties'; web camera subtitled 'Web Cams'; and a telephone subtitled 'IP Telephony (IPT)']

Electronic communication is now indispensable to every modern organisation. But with speed and convenience comes risk – and the potential for abuse. Faxes, e-mails and instant messaging systems (IMS) all pose information security challenges, so appropriate and acceptable use of electronic communication is an essential part of information security.

A further aim of an information security policy is to prevent abuse of your communications network by third parties or criminals.

Click on each of the six images below to learn more.

If selection = 'e-mail' move to screen 2

If selection = 'IMS' move to screen 8

If selection = 'fax' move to screen 12

If selection = 'third parties' move to screen 14

If selection = 'web cam' move to screen 16

If selection = 'IP Telephony' go to screen 19

Forward button moves to screen 21

Screen 2

[Graphic: The world with e-mails whizzing around – some are being intercepted and read]

It is estimated that up to 62 billion e-mails are sent worldwide each day! Many of those are sent by employees within organisations and whilst some won't be particularly private others will contain confidential or sensitive information.

Organisations therefore take steps to protect their e-mails from being intercepted and read by hackers. Encrypting e-mails means your e-mail data is scrambled and can only be un-encrypted through the use of the correct key.

Note: Currently at SP AusNet we are not providing e-mail encryption to all employees. It will be considered on a case-to-case basis. If you think you need e-mail encryption, contact your Information Security Manager. Encryption technology and its mechanisms are used in the new consolidated Windows domain infrastructure and a few security devices like firewalls and switches. Organisation wide e-mail encryption is being considered and the decision to use it will be communicated to all SP AusNet employees.

Forward button moves to screen 3

Screen 3

[Graphic: Two employees exchanging public keys – on their free hand each is holding their private key. The 'keys' could be tokens with strings of characters on them – to signify encryption]

There are different approaches for encryption and decryption – one widely used method is the Public Key Infrastructure (PKI).

With PKI, each user has two 'keys', which are mathematically related to each other. The first key, the user's private key, is kept confidential at all times. The second key, the public key can be freely given out to all potential correspondents. Within organisations, public keys are printed in freely available directories, rather like a telephone directory.

Both keys must be used to encrypt and decrypt e-mails.

Forward button moves to screen 4

Screen 4

[Graphic: Sally at computer with e-mail and attachment. Can see 'Encrypt' and 'Send' buttons on the e-mail screen. Send button is clickable. After button clicked, add second graphic of Ed at his desk – with e-mail screen]

It works like this – Sally wants to send Ed a copy of the plans for mergers and acquisitions. She creates her e-mail as usual and attaches the Confidential report. She then looks up Ed's public key in the directory and, using the encryption button on her e-mail screen, enters Ed's public key (some systems can do this automatically selecting the appropriate public key for entries in your e-mail address book).

Add instruction text:

Click on the Send option to continue.

Add graphic of Ed at his desk with e-mail on his screen.

When user clicks on 'Send' the following text appears:

The e-mail and attachment are turned into cipher text, so that if someone intercepts them they'll be unreadable.

Ed receives the e-mail, and using his private key (which uniquely will work with his public key) decrypts the message and the report.

Forward button moves to screen 5

Screen 5

[Graphic: An e-mail but the signature 'Bill Bailey, Production Manager.' Is animated to swap between the text and a string of digital characters]

As well as using their private key to decrypt incoming e-mails, an employee can use their private key to 'digitally sign' their outgoing e-mails. The receiver can then use the sender's public key to verify the sender's identity; if the two keys don't work together and authenticate the sender, then the e-mail is a fake.

So, in the previous example, Sally could have used her private key to digitally sign the e-mail. On receiving it, Ed could then have verified it truly was from Sally by validating the signature with Sally's public key.

Only someone possessing the private key could have created the digital signature, and anyone with access to the corresponding public key can verify it.

If you think the information you process or store needs more security, contact your Information Security Manager for details.

Forward button moves to screen 6

Screen 6

[Graphic: Report with four headings – each heading is clickable. Alongside each heading add a checkbox (for initials and tick)]

If click on a heading, display the relevant text on screen. When user clicks on a heading, add text and add a squiggle in the check box as a signature and a tick.

More and more organisations are choosing to use secure e-mail.

Click on each heading of this report to see why.

- Confidentiality
- Authentication
- Integrity
- Non-repudiation

If click Confidentiality:

A secure system means only the intended recipient can read or use the information. Without confidentiality, anyone with access to the information system can use readily available tools to eavesdrop on network traffic and intercept valuable proprietary information. If it is stored as plain text, then once intercepted, it can easily be read. This could be by a hacker or even another authorised system user, but for whom the report was not intended.

However, if the information is encrypted, then even if intercepted, it is useless without the decoding key, known only to the designated recipient.

If click on Authentication:

As you have seen, systems such as PKI can be used for authentication. Digital signatures enable users to trust the e-mail and the information it contains.

If click on Integrity:

Many secure systems enable recipients to verify that the original contents have not been altered or corrupted. For example, an intruder might covertly alter a file, but in doing so they will change the unique digital thumbprint for the file, causing other users to detect the tampering by comparing the changed digital thumbprint with the digital thumbprint for the original contents.

If click on Non-repudiation:

Secure systems can give assurance that the communication (and its contents) cannot, subsequently, be denied.

For example, without non-repudiation, an originator of a particular e-mail might falsely deny being the creator/sender. And similarly without non-repudiation, the recipient of a communication might falsely deny having received the communication.

Forward button moves to screen 7

Screen 7

[Graphic: Someone sat at a PC in an office looking at a clock which says 4.50pm. It is dark and the person looks annoyed, as if they are all too ready to get out of the office]

Work your way through the following scenario to find out whether you know how to use e-mail securely.

It really is time to be leaving the office – but you haven't finished your summary of the financial projections for your manager, and she wants it on her desk first thing tomorrow morning. You plan to work on it this evening and think of e-mailing it to your web mail account, but you know it doesn't support data encryption. What should you do?

A) Send it to your web mail account anyway – after all, hackers are only after corporate e-mails

B) Save it to an encrypted USB stick and lock it in your briefcase

(B = correct answer)

If user selects A

This isn't a good idea – hackers target both corporate and private e-mail systems. So, if you have something confidential, put it on an encrypted CD, USB stick or other storage device – and keep it safe.

If user selects B

Yes, this is the best approach. Hackers target both corporate and private e-mail systems; if you have something confidential, put it on an encrypted CD, USB stick or other storage device – and keep it safe.

Forward button returns to screen 1

Screen 8

[Graphic: A female manager looking angrily over the shoulder of an employee who is using IMS

Imagine the following situation. Your boss has just caught you using an Instant Messaging System to negotiate a deal with a client.

You haven't been saving all of the IMs, but she scrolled back through the thread from the message you were typing when she interrupted you.

It turns out that you and your client contact had been negotiating quite informally – which included making some (quite personal) jokes at the expense of a well-known competitor.

Forward button moves to screen 9

Screen 9

[Graphic: An IMS-style window with the text overlaid. 'Send' option is visible]

The statements below have radio buttons next to them – users select the options they think are correct and then click on the forward button. This takes them to screen 7

Your manager takes you aside and points out what's wrong with what you have been doing.

Click on the radio button next to each comment you think is true. When you are finished, click on the forward button to get some feedback.

- People often use IM very casually – but messages can be used as evidence of libel
- Business deals via IM should always be recorded
- Business deals negotiated via IM are not legally binding
- In the U.S., government regulations require organisations to record financial and healthcare data exchanged by IM

Forward button moves to screen 10

Screen 10

[Graphic: An IMS-style window with the text overlaid]

The statements below have TRUE or FALSE next to them as specified below. A green tick appears next to each option the user correctly selected on the previous screen

As you can see, most of these statements are true - the green ticks show which ones you got right. Hopefully, you weren't too far off the mark!

- People use IM casually – but messages can be used as evidence of libel TRUE
- Business deals via IM should always be recorded TRUE
- Business deals negotiated via IM are not legally binding FALSE
- In the U.S., government regulations require organisations to record financial and healthcare data exchanged by IM TRUE

Forward button moves to screen 11

Screen 11

[Graphic: An image of an IM message. The 'file' dropdown is extended, there is the option 'open' and 'send' but the mouse cursor is selecting the 'save' option underneath]

It's vital to remember that all electronic communication, including IM and e-mails are admissible in court. So never write anything potentially libellous about someone, and never make comments that are negative or offensive about race, gender, sexual orientation, nationality, political or religious beliefs.

If messages are evidence of a business arrangement, you must save copies. In some cases government regulations require you to keep the messages stored safely and accessibly for set periods.

For this reason, increasing numbers of organisations have strict use and retention policies. If you are unsure of the policy or how it should be applied, ask your manager or supervisor.

Forward button returns to screen 1

Screen 12

[Graphic: Fax machine with buttons marked 'start', 'stop' and 'fax'. Whichever button the user clicks on the small character jumps on the button]

Although faxes have been a mainstay of office communications equipment for a long time, they are being less used in favour of e-mail and IMS. However, as they are still used it is worth reminding yourself of the security risks associated with them.

Imagine that you are about to fax a report, classified as Confidential, to one of your project team colleagues.

You have entered their fax number. Press the 'start' button on the fax if you are ready to proceed, or press the 'stop' button if you think there's something else to consider.

If user clicks on 'start', graphic and text as below

Hold it! If you're faxing Confidential information, shouldn't you make sure that the person you are sending it to is there to receive it at the other end? And remember – always double check the number you have keyed in before you hit 'send'.

If user clicks on 'stop', graphic and text as below

You're right to be cautious! If you're faxing Confidential information, then it's important first to make sure that the person you are sending it to is there to receive it at the other end. And remember – always double check the number you have keyed in before you hit 'send'.

Forward button moves to screen 13

Screen 13

What if you have called the recipient of the fax but their voicemail says they're not available? You wisely hold off from sending the fax, but should you leave a message telling them about the report and roughly what it contains?

Click on the figure to leave a message, or on the handset to hang-up if you're not going to leave a message.

[Graphic: Animation as above but with small character standing by telephone handset, if user clicks the handset meaning 'no' they don't want to leave a message the handset gets put down, if user clicks the man meaning 'yes' they want to leave a message, he animates]

If 'yes', feedback as below

Probably not a good idea! Voicemail systems are not totally secure, especially if the recipient has been careless enough to give their password to another person. Think very carefully before leaving voicemail messages.

If 'no', feedback as below

Yes, you need to be careful! Voicemail systems are not totally secure, especially if the recipient has been careless enough to give their password to another person. Think very carefully before leaving messages.

Forward button returns to screen 1

Screen 14

[Graphic: Icon of an office with 'HQ' written on it, with dotted lines extending to four other buildings/clusters of people in 'orbit' around it]

Information systems and assets are often shared with outside organisations – 'third parties'. These could be subsidiaries, vendors, other business partners or key clients. The challenge here is to maintain the confidentiality and integrity of the data while keeping it available to the people who need it.

The information security requirements will vary from party to party according to the risk (based on the sensitivity of the information and SP AusNet's relationship with the third

party). So each situation needs to be carefully thought through before access is granted, and sufficient preparations need to be made.

One common approach is to use a Non-Disclosure Agreement (NDA), in which all parties agree up-front that the information will be treated as though it was their own confidential information.

Forward button moves to screen 15

Screen 15

[Graphic: Four people in a classroom environment (the induction). One is pointing something on a whiteboard out to the others. The board has 'IT procedures' written on it]

Independent contractors are unlikely to automatically obey SP AusNet's information security procedures, in part because they may not be aware of them. So they need to be properly informed and made aware our information security policies and procedures.

For example, if they are using their own computers and connecting it to your network, have they installed adequate anti-virus software to scan incoming and outgoing e-mails?

SP AusNet has set up its system to scan e-mails automatically – but has the third party? Issues like these need to be addressed before they become problems.

Forward button returns to screen 1

Screen 16

[Graphic: Computer on a desk with a web cam on it - and other sophisticated video conferencing system in a conference room]

Web cameras (web cams) are growing ever more popular and can be a great communication tool for organisations but they do bring security risks.

The benefits of using web cameras and other video conferencing systems include a reduction in travel costs for meetings and the easier, and often increased, communication between geographically dispersed offices.

Although systems may vary in cost and complexity, the controls remain the same.

Forward button moves to screen 17

Screen 17

[Graphic: Computer on a desk with a web cam on it - a big eye/spy is leaning out of the camera looking at what is happening on the desk - employee at desk is looking worried]

The risk comes from hackers who gain unauthorised access into our network and activate a computer's camera without the user's knowledge, providing the hacker with a live-feed from the camera and in some cases even control of motorised pan-and-tilt mechanisms.

In a famous case, the means to access over 1,000 unprotected cameras around the world was published on a website! These cameras didn't require a password login, so surfers with access to the 'code' could spy on offices, restaurants and all sorts of other businesses.

It's an uncomfortable feeling knowing a hacker could see whether you are at your desk, details of any confidential and sensitive information on your desk and what is going on in confidential meetings.

Forward button moves to screen 18

Screen 18

[Graphic: Computer on a desk with a web cam on it - a big eye/spy is leaning out of the camera looking at what is happening on the desk - employee at desk is looking worried]

If you or your team uses video or web-conferencing there will be specific procedures for how sessions should be set up and securely ended. Make sure you know what these procedures are.

At all times, whether in a video/web conference room or using a desk-based web cam, bear the following points in mind:

- Know your audience – if possible verify your counterpart(s)
- Shut down any additional sessions you are running on your PC to avoid unintentional display/access to information
- Don't leave the conference or your desk unattended
- Don't allow remote viewers to leave unattended
- Don't allow others to control your PC
- Don't present any confidential or sensitive information (you can't be sure who is watching)

Forward button returns to screen 1

Screen 19

[Graphic: Employee at desk and PC with headset on – (if possible on the screen is some representation of an IP Telephony control panel)]

Voice over Internet Protocol (VoIP), also known as IP Telephony (IPT) is the routing of voice conversations over the Internet or through any other IP-based network.

Benefits of IP Telephony include lower overall costs and seamless integration of voice, data, and video communication platforms.

But, as with all other data sent over an electronic network, it can be open to a range of security threats.

Forward button goes to screen 20

Screen 20

[Graphic: Employee at desk and PC with headset on – as before]

Criminals will target IP Telephony systems for the same reasons they might disrupt traditional telephone and information systems and Internet services. These include:

- Financial benefit
- Toll fraud

- Identity theft
- Information theft
- To disrupt services and inconvenience users

Your call is sent as a 'digital packet of information' to the other party so it could be intercepted and modified and sent on to the recipient; an attacker could connect a rogue IPT phone to a network and, using a stolen user account and password, place calls at the organisation's expense. For all these reasons it is important that you keep your account log on and password details confidential and follow our procedures carefully.

Forward button returns to screen 1

Screen 21

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for electronic communication

E-mail, IMS and web cams or video/web conferencing can get information to people securely and they may make things happen a lot quicker, provided they are used correctly.

DO:

- Be selective about when and how you use e-mail
- Avoid sending documents classified as Sensitive, Private or Confidential via e-mail, unless encrypted or password protected
- Remember your e-mails and IMs are business documents, so use an appropriate style and language
- Immediately report any suspicious or malicious e-mail you receive
- Close down any unrelated work session on your PC and clear your desk of sensitive and confidential information when using a web cam or in a video/web conferencing session

Forward button moves to screen 22

Screen 22

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for electronic communication

DON'T:

- Use SP AusNet's e-mail for casual or non-business purposes
- Put any form of Confidential, Private or Sensitive information into e-mails without using encryption
- Send suspicious e-mails, or fail to report such e-mails when you receive them
- Propagate chain letters and hoax warning messages by forwarding them to your work associates
- Reply to suspicious e-mails asking you to update or confirm your personal details

- Write anything in an e-mail or IM that you might regret later!
- Leave web cameras or videoconferences unattended
- Allow others to control your computer during web/video conference sessions

Forward button moves to screen 23

Screen 23

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for faxing information

- Never fax information that could be classified as Confidential, Private or Sensitive to an unattended fax machine
- Always check the destination fax number before starting your transmission
- Be careful what messages you leave on answering machines and voicemail

Rules for communicating with third parties

- Check that any third party has been granted access before releasing information to them
- Check whether a Non-Disclosure Agreement is appropriate and if so whether it has been signed

Forward button exits module

Module 2h - Internet security and acceptable use

Screen 1

A ‘hacker’ is anyone who attempts any kind of illegal computer-based activity including breaking into someone else’s information system. And the Internet is a hacker’s paradise. It could potentially give hackers open access to any information held on SP AusNet’s information system.

SP AusNet uses a wide range of access controls in order to minimise the risks of this occurring. This is often done ‘behind-the-scenes’ without you even being aware.

[Graphic: Telephone socket on a wall with a cage around it]

Forward button moves to screen 2

Screen 2

How aware of the security risks involved in using the Internet are you? Click on ‘True’ or ‘False’ for each of the statements below.

Internet data is all virus-checked before it is put on the web. *[false]* *[Graphic: Globe that is stamped with the words ‘virus checked]*

Feedback if ‘false’ is selected:

That’s correct – this statement is false. Information viewed over, or downloaded from, the Internet is just as likely to carry viruses as any other form of computer data.

To reduce the risk from Internet viruses, we have set up controls to ensure that all incoming data is virus checked as it downloads. But this doesn't ensure 100% security – new viruses may not be picked up, so it's always best to avoid downloading information via the Internet.

Feedback if ‘true’ is selected:

That’s incorrect – this statement is false. Information viewed over, or downloaded from, the Internet is just as likely to carry viruses as any other form of computer data.

To reduce the risk from Internet viruses, we have set up controls to ensure that all incoming data is virus checked as it downloads. But this doesn't ensure 100% security – new viruses may not be picked up, so it's always best to avoid downloading information via the Internet.

Forward button moves to screen 3

Screen 3

Using the Internet during work hours is permitted as long as I don't abuse it. *[true]* *[Graphic: PC monitor with a warning symbol on it.]*

Feedback if ‘true’ is selected:

That's correct – this statement is true. Even though SP AusNet permits staff to use the Internet for personal use there are strict guidelines that you should follow. As a general rule make sure that you never access sites that offer sexual material or defame race, gender, religion or other protected groups. And keep in mind that, based on SP AusNet's privacy policy, your use of the Internet and e-mail may be monitored. Also, avoid using the Internet excessively. Failure to do so could end up in disciplinary action, or even dismissal.

Feedback if 'false' is selected:

That's incorrect – this statement is true. Even though SP AusNet permits staff to use the Internet for personal use there are strict guidelines that you should follow. As a general rule make sure that you never access sites that offer sexual material or defame race, gender, religion or other protected groups. And keep in mind that, based on SP AusNet's privacy policy, your use of the Internet and e-mail may be monitored. Also, avoid using the Internet excessively. Failure to do so could end up in disciplinary action, or even dismissal.

Forward button moves to screen 4

Screen 4

Posting information to forums, chat rooms and bulletin boards is done anonymously. *[false]*
[Graphic: Notice board with small people blindfolded, suspended on a window cleaner's scaffold. Various notices appear, including ones saying 'Check this out' and 'Notice']

Feedback if 'false' is selected:

That's correct – this statement is false. You are not as anonymous as you think when you participate in a forum, chat room or bulletin board. Your e-mail address may be logged by the forum's administrator and could be intercepted by others and passed on for mailing purposes, which can often lead to unsolicited and nuisance e-mails.

There is also the potential issue of people's 'personal' opinions being misinterpreted as 'corporate' opinions, especially if they take part in forums during working hours.

Make sure you know what the rules for Internet use are and that you follow them in all aspects of your job role.

Feedback if 'true' is selected:

That's incorrect – this statement is false. In fact, you are not as anonymous as you think when you participate in a forum, chat room or bulletin board. Your e-mail address may be logged by the forum's administrator and could be intercepted by others and passed on for mailing purposes, which can often lead to unsolicited and nuisance e-mails.

There is also the potential issue of people's 'personal' opinions being misinterpreted as 'corporate' opinions, especially if they take part in forums during working hours.

Make sure you know what the rules for Internet use are and that you follow them in all aspects of your job role.

Forward button moves to screen 5

Screen 5

Files only download onto your system when you have specifically requested it. *[false]*
[Graphic: A long queue of files being admitted via a security barrier]

Feedback if 'false' selected:

That's correct – this statement is false. Whenever you access a website, information may be downloaded onto *your* system without you knowing it and can therefore impact on SP AusNet's network.

Even though we protect our systems with firewalls and other defences there is always an inherent risk in using the Internet.

Feedback if 'true' selected:

That's incorrect – this statement is false. Whenever you access a website, information may be downloaded onto *your* system without you knowing it and can therefore impact on SP AusNet's network.

Even though we protect our systems with firewalls and other defences there is always an inherent risk in using the Internet.

Forward button moves to screen 6

Screen 6

The issue of both security and intellectual property rights (IPR) is something else to consider.

Just because you can access vast amounts of information, doesn't mean you can take it and use it in any way you please.

If you are posting information to the Internet, remember that you are making the information public, which means that anyone, anywhere in the world, can potentially access it and you have little control over how they might use it.

Information that is classified Confidential, Private or Sensitive or is subject to any kind of restriction should never be posted to the Internet because it could put SP AusNet at risk.

[Graphic: Person about to post information on the Internet considering whether to click 'send'. There's a warning panel asking, 'Do you wish to send?', buttons on the panel 'Yes' and 'No'. The cursor arrow hovers over the no button]

Forward button moves to screen 4

Screen 7

To minimise the risk of sensitive or confidential information being made public through the Internet, we have strict policies about:

- Who can modify or add to our Internet sites
- What subjects can be discussed and how material should be written, reviewed and agreed
- How you can use information you download from external sources

To protect yourself, make sure you know what the policy is and follow the correct procedures at all times.

[Graphic: Small people sitting as if in a theatre, looking at a huge PC screen – 1984 style]

Forward button moves to screen 5

Screen 8

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for Internet security

- Don't post confidential or sensitive information on chat rooms, bulletin boards or forums using SP AusNet's network or your work computer
- Don't post personal opinions on the Internet where they could be misinterpreted as SP AusNet's view
- Don't browse websites that offer sexual material or defame race, gender, religion or other protected groups
- If prompted, never give your permission for any file to be downloaded from the Internet without first verifying or confirming the source and validity of the document for business purposes
- Only use the Internet in accordance with our Acceptable Use Policy

Forward button exits module

Module 2i - Security out of the office

Screen 1

When you're working away from the office, SP AusNet's security procedures continue to apply, but you also face increased risks and need to take extra care to protect against them.

Don't forget that you are a valuable source of information and knowledge, and an important asset to SP AusNet – so it's important that you know how to protect yourself.

By following some very simple rules you can help to protect:

- Yourself
- SP AusNet's equipment
- SP AusNet's information

Click on each of the four images to find out more.

When returning from screen 2, 3 or 4 instructions change to:

Click on any of the images that you have not already selected.

On completion the instructions change to:

You have now clicked on each of the images. Click on an image to review again, or click on the forward button to continue.

[Graphic: 4 images on screen; Small person sitting on a large briefcase, small person sitting on a laptop, small person carrying an envelope which reads 'F.A.O Mr. J. Smith' and 'PRIVATE', a PDA]

If selection = person sitting on briefcase go to screen 2

If selection = person sitting on laptop go to screen 3

If selection = person carrying an envelope go to screen 4

If selection = PDA go to screen 5

Forward button moves to screen 7

Screen 2

Protecting yourself

Click on each of the items below and drag them into the briefcase to see some general rules on how to protect yourself when out of the office.

[Graphic: Image of large open briefcase. A small person can be seen peering from round the side of the case. Also arranged on screen are various items including; an itinerary document, a drivers licence, a package wrapped in brown paper with an address label clearly visible, a wallet containing credit cards, a luggage label, a 'taxi' sign, and a ticket labelled 'Flight tickets']

If selection = Itinerary document

- Do not publicise your travel plans; only inform those who need to know
- Leave a complete hard copy of your itinerary, including contact numbers, with a designated person in the office

If selection = wallet containing credit cards

- Take only the credit cards and money that you need
- If travelling abroad, be aware of the exchange rate to ensure you have enough funds and have a plan for how you will cover unexpected events
- Leave expensive items such as jewellery at home

If selection = drivers licence

- Keep copies of your proof of identification i.e. passport and driver's licence, but do not store them with the originals
- Make sure your passport and visa are up-to-date and have sufficient time before they expire

If selection = package wrapped in brown paper with address label

- Do not transport items for other people and always check any gifts received from business contacts before placing them in your luggage

If selection = luggage label

- Never leave your luggage unattended
- Make sure your luggage tag is completed, so that any lost item can be returned to you

If selection = plane ticket

- If travelling abroad, check the Department of Foreign Affairs and Trade "Smartraveller.gov.au" website or call the Australian consulate in your destination country for up-to-date information and advice on your destination
- Consider registering with your embassy or consulate in your destination country

If selection = taxi sign

- Use registered taxis or travel firms
- If possible, research your intended journey so you know where you are going and how long it should take
- Always ask to be dropped off somewhere you know, at your hotel or in a safe, well-lit area

Forward button returns to screen 1

Screen 3

Protecting equipment

When you are out of the office, equipment such as Blackberries, PDAs, laptops, mobile phones, portable storage devices (USB sticks) and briefcases all need safeguarding.

Click on each of the people below to see how best to do this.

[Graphic: Circles containing images of people as below:

Circle 1 – Small person looking at a briefcase through a car rear window (NOT on roof)

Circle 2 – Small person standing next to an oversized mobile phone

Circle 3 – Small person with briefcase and laptop bag and two other metal cases (containing electronic equipment)

Circle 4 – Small person filling out a luggage tag

Circle 5 – Small person with padlock or key

Circle 6 – Small person with security guard]

When the user clicks each circle, the relevant text appears underneath.

If Circle 1 - rear window selected:

Never leave equipment in view, even if locked in a car.

If Circle 2 - mobile is selected:

If possible, always lock your mobile phone so that a PIN (personal identification number) is required before use.

If Circle 3 – many cases is selected:

Only take the equipment you need for your trip or meeting.

If Circle 4 – luggage tag is selected:

Make sure all your equipment is labelled with an office telephone number – but do not include SP AusNet's name.

If Circle 5 – padlock/key is selected:

If you have a lock on your briefcase or any other equipment – use it!

If Circle 6 – security guard is selected:

Be wary of mishaps, like someone bumping into you or spilling a drink... they may be staged to set you up for a robbery.

Forward button returns to screen 1

Screen 4

Protecting information

Information comes in many forms; as hardcopy documents, data on laptops and other electronic storage devices, numbers stored on your mobile phone, conversations in public places etc…

Click on each of the envelopes below to find out how to help protect this information when out of the office:

[Graphic: 3 small people.

Person 1 is putting an oversized envelope into a small bag.

Person 2 is looking up at image of envelope on laptop screen

Person 3 is looking up at an opened envelope, with content visible, but is aware that someone is standing behind them]

When person 1 is selected text below is shown on right of screen

- When travelling, carry any sensitive information in your hand luggage – do not place it in a suitcase
- Use the lock on your mobile phone when it's not in use

When person 2 is selected text below is shown on right of screen

- Regularly erase any old files from your laptop and other electronic storage devices

- Password protect files that are of a sensitive or confidential nature, whether at rest or in transit
- And just in case the unexpected happens, always make regular backups of data

When person 3 is selected text below is shown on right of screen

- Beware of 'shoulder surfers' – people who watch over you when you are working, for example, inputting passwords, or reading work documents
- Never discuss confidential or sensitive issues in public places – anyone could be listening in
- Dispose of any hardcopy documents correctly – remember your office procedures
- Do not leave confidential information in vehicles, for example test records, schematic diagrams, internal documents, memos etc

Forward button returns to screen 1

Screen 5

Protecting data and networks

Wireless networking means flexibility and freedom, and is increasingly popular – the majority of all laptops are now built with wireless functionality. After all, who wouldn't want to be able to log on to their e-mails from a café, or their hotel? But working this way is potentially risky.

On the next screen you can see a representation of a wireless enabled café, where you can explore some of the information security risks.

[Graphic: A businessman working on a PDA in the lounge of an hotel]

Forward button moves to screen 6

Screen 6

Look around this wireless enabled café and click on three items that represent a potential security threat to someone working using a public wireless network.

[Graphic: When user clicks on item, the appropriate text is displayed. As each item is selected a tick appears next to them. 'Café' scene with a businesswoman working on a laptop, wireless router (with antenna) next to a person working on a modern (touch-screen type) cash register/till, businessman working on a PDA]

When selection = businesswoman, text as below

To be secure, wireless devices need to be set up so that access to them is properly controlled. But as a still-new technology, many businesses do not yet configure all wireless equipment to be used securely. And if this hasn't happened, the competitor sitting next to you could be browsing through your Inbox…

When selection = businessman, text as below

Unless you are adequately protected (e.g. with password-only access), using a wireless network could leave you wide open to attack – for example from hackers who could access SP AusNet's network via a back door.

When selection = PC sitting on a shelf, text as below

You are particularly vulnerable if you use a 'leaky' network – one that does not prevent other users from attempting to access your device. And without being an IT expert, how would you know whether the network was secure or not?

When user has clicked on all items, message appears as follows:

You have now selected all options. Please click on the forward button at the bottom of the screen to continue.

Forward button returns to screen 1

Screen 7

These are just some of the steps you should take to safeguard yourself, your equipment and your information when you are out of the office. But above all, remember to be vigilant at all times – and never do anything that would put yourself at risk.

[Graphic: Montage image - Car from screen 3 can be seen driving off down road with the boot open. Briefcase from screen 2, envelopes from screen 4, small person and PDA being tossed about almost falling out].

Forward button moves to screen 8

Screen 8

Rules for security out of the office

To protect yourself:

- Don't publicise your travel plans; just leave a hard copy itinerary with a designated person
- Only take the credit cards and money that you need
- Take only one original proof of identification, and a photocopy
- Don't transport items for others and check any business gifts thoroughly
- Never leave your luggage unattended – and if you see any unattended bags contact security immediately
- Only use registered taxis and get dropped off in a safe, well-lit place

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Forward button moves to screen 9

Screen 9

Rules for security out of the office

To protect equipment:

- Never leave equipment in view
- Only take the equipment you need
- Use locks on briefcases/luggage if supplied, and secure your mobile phone
- Label your equipment, but do not display SP AusNet's name

- Be wary of mishaps

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Forward button moves to screen 10

Screen 10

Rules for security out of the office

To protect information:

- Carry sensitive information in your hand luggage
- Erase any old files from your laptop
- Password protect all sensitive or confidential files
- Make regular backups of data
- Beware of 'shoulder surfers'
- Never discuss sensitive or confidential issues in public places

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Forward button exits module

Module 2j - Social engineering

Screen 1

Social engineering is the term for describing an intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineering can take place face-to-face, over the phone and on-line, or any combination thereof.

So a *social engineer* is a criminal who uses highly developed social skills including manipulation, ingratiation, impersonation, psychological tricks and a wide variety of tools to persuade you to reveal information to which they have no right or authorised access.

[Graphic: Villain-like character standing to the side of a pile of documents. On top of the pile is a box file labelled "passwords"]

Forward button moves to screen 2

Screen 2

In general we are quite careful about giving out our personal details verbally. For example, if someone called you and said they were from the bank and needed to check your credit card PIN number, you wouldn't give it out would you? No – you would be suspicious and would want to check this person's identity first.

Well, the same principles apply at work and to non-verbal requests.

If anyone asks you for potentially sensitive information, such as your password, you should ALWAYS be suspicious. If they are a social engineer and manage to obtain the information they need, SP AusNet could be put at serious risk.

[Graphic: 2 small people - person 1 is holding an ID card, person 2 is holding out their hand requesting to see it. The ID card shows a photograph and signature of Person 1]

Forward button moves to screen 3

Screen 3

Social engineers may try to obtain a range of information depending on their specific intent. For example, bank account or credit card details and PINs, social security numbers, your computer log on and password details.

And as you will see, they might use a range of tactics, including the telephone, e-mails and fake websites to extract this information from you. The best way to defend yourself is to ensure that you can recognise potential attacks when they are happening and know how to deal with them.

[Graphic: Image of a villain-like character standing behind a large innocent looking mask making a sneak approach to an innocent person]

Forward button moves to screen 4

Screen 4

Click on the two images below to learn about the two common types of social engineering.

[Graphic: Two images to left of screen:

Image 1 (labelled "Human Based") - villain-like character from screen 1 standing to the side of a pile of documents. On top of the pile is a box file labelled "passwords".

Image 2 (labelled "Computer Based") - Computer monitor with an image similar to a change password pop-up on it.]

If user selects human-based graphic go to screen 5

If user selects computer-based graphic go to screen 7

Forward button moves to screen 9

Screen 5

Human-based social engineering

This is when a hacker uses interpersonal skills via the telephone or face-to-face, to try to extract sensitive information.

Click on each of the three items below to see some common examples of human-based social engineering.

[Graphics: 3 separate image hotspots arranged on screen:

Image 1 - Comedy glasses, nose and moustache disguise as you might find in a joke shop. Small villain-like character from screen 1 standing beside.

Image 2 - villain-like character from screen 1 standing on top of calculator

Image 3 – villain-like character from screen 1 hiding behind a sign that reads "Technical Support"]

If user selects image 1 go to screen 5a

If user selects image 2 go to screen 5b

If user selects image 3 go to screen 5c

Once user has selected all 3 images show the following text:

In all of these human-based examples the social engineer easily obtained the information they needed – but ONLY because the employees co-operated!

Forward button moves to screen 6

Screen 5a

[Graphic: Zoom of Image 1 from screen 5 - Comedy glasses, nose and moustache disguise as you might find in a joke shop. Small villain-like character from screen 1 standing beside]

Situation: The IT-Service Desk receives an incoming call from an embarrassed employee who has forgotten his password. The employee asks if they could reset his password, or give him the old one over the phone. The IT-Service Desk cooperatively reset the password right away.

Result: The caller was a social engineer impersonating a member of staff. He now has a password that will give him access to SP AusNet's network.

If user selects forward return to screen 5

Screen 5b

[Graphic: Zoom of Image 2 from screen 5 - villain-like character from screen 1 standing on top of calculator]

Situation: An accounts administrator receives a call from a frustrated secretary. She says that she only has ten minutes to get the pricing details for a new product over to the Finance Director for an important meeting. She says she is having problems with her computer and wants the accounts administrator to fax the information immediately.

When the employee hesitates, the secretary both reassures him the information will be secure as she is standing right by the fax, and threatens to report him to his supervisor if he doesn't help. Under pressure, the employee faxes the details to the number given.

Result: This person turns out to be a social engineer who is impersonating the Finance Director's secretary. She now has a hard copy of our intended pricing for the new product – very sensitive information and something our competitors would dearly like!

If user selects forward return to screen 5

Screen 5c

[Graphic: Zoom of Image 3 from screen 5- villain-like character from screen 1 hiding behind a sign that reads 'Technical Support']

Situation: An employee receives a call from the IT-Service Desk. They say they are calling to check on an intermittent network problem that, if it hasn't already affected their data, potentially could.

The IT-Service Desk representative says that to fix the problem and save the employee from losing their files they need the employee's User ID and password.

Wanting to be helpful and visualising the consequences of their files being corrupted or lost, the employee gives out her User ID and password thinking that the computer problems will be resolved.

Result: The caller was in fact a social engineer, who, having gained access to the telephone system, found it easy to impersonate someone from the IT-Service Desk. They now have a password that will give them access to potentially sensitive information.

If user selects forward return to screen 5

Screen 6

Now take a look at the following scenario:

[Graphic: Small person standing on keyboard looking up at PC. Stick-on note can be seen stuck to the side of the monitor with the word "password" written on it. Behind the small person is a slightly larger person dressed as villain from screen 1)]

You are working on a project when you notice someone behind you looking over your shoulder. As you turn around you discover that the person is writing down your password, that you had scribbled on a piece of paper by your desk. As you go to question him, he says:

"Sorry to interrupt you… I need to upload a new version of the e-mail software that you have on your PC. If I can just take your password, I'll come back later and do it."

What do you do?

A. Let him finish writing down the password and get on with your work – if he's in the building he must have authorisation

B. Ask to see his identification and then let him have the password

C. Ask to see his ID and tell him you are just going to call and check this with the IT-Service Desk before you give any information out

(C = correct answer)

If user selects A

First of all, you should never write down any password – it should only be committed to memory. In addition you should have verified the person's identity and then checked this with the IT Service-Desk.

This person is a social engineer who has gained access to the building and used their interpersonal skills to manipulate you into revealing your password. You should change your password immediately.

If user selects B

First of all, you should never write down any password – it should only be committed to memory. You were right to be suspicious and to ask for their ID, however this ID is false and you should have double-checked with the IT-Service Desk.

This person is a social engineer who has gained access to the building and used their interpersonal skills to manipulate you into revealing your password. You should change your password immediately.

If user selects c

First of all, you should never write down any password – it should only be committed to memory. But, you were right to check with the IT-Service Desk.

This person is unknown to them and could be a social engineer trying to manipulate you into revealing your password. The IT-Service Desk has called security and they are on their way to question the man. You should change your password immediately.

Forward button returns to screen 4

Screen 7

Computer-based social engineering

This type of social engineering involves a hacker using computer software in their attempts to get sensitive information. They use various electronic tools, including e-mail, pop-up windows and fake websites. They may even combine these with human-based techniques, for example voicemails.

Click on each of the three items below and drag them over the computer monitor to see some common examples of computer-based social engineering.

[Graphic: Image of a PC on right of screen. Next to PC are three items: Item 1 – key on a key ring containing a password, Item 2 – e-mail envelope, Item 3 – miniature car]

If user drags key to monitor show following text to left of screen:

Pop-up windows

Situation: An employee is working on a PC. A pop-up window suddenly appears on screen telling the user that there has been a security breach and that they must renew their password immediately. The employee carries out the request and inserts their old password followed by the confirmation of a new password.

Result: The pop-up window does not update the password, but instead sends the current password back to a social engineer at a remote site. This could give them further access to SP AusNet's systems.

[Graphic: Image of a change password pop-up window is shown on the monitor screen]

If user drags e-mail envelope to monitor show following text to left of screen:

Mail attachments

Situation: An e-mail comes into an employee's inbox, seemingly from the technical services department of their bank. The e-mail, presented graphically with the bank's logo and website address, explains that the bank is undertaking a 'scheduled software upgrade, to improve the quality of service for all customers'.

The e-mail urges the recipient to go to the link specified to confirm their bank details. The link seems genuine.

The employee recognises the bank's logo and style and, almost without thinking, follows the link to the website and enters all the details requested.

Result: The e-mail was from a social engineer trying to trick people into revealing their personal account details. The website was a fake and the criminal now has the employee's account details including their security password/number.

[Graphic: Image of scam e-mail from 'Your Bank']

If user drags car to monitor, an e-mail appears. Large letters "Win a Car" are visible. Show the following text to left of screen.

Internet

Situation: An employee is searching the web when a pop-up window invites them to click to be in with a chance of winning a car. The employee clicks on the pop-up and is taken to a very smart looking website where they must enter an e-mail address and a password.

Result: There is no car to win – but as soon as the employee clicked on the pop-up spyware was downloaded on to their PC. This spyware can now track which Internet sites are visited and record all future keystrokes – so the criminal can potentially capture User IDs, passwords, confidential details, in fact anything typed in to the computer.

This could enable the social engineer to steal the employee's work or personal identity.

[Graphic: Image of "win a car" website is shown on monitor screen]

Forward button moves to screen 8

Screen 8

Now take a look at the following scenario:

[Graphic: Image of small person scratching head looking up at monitor. On the monitor there is an e-mail. Large letters "Register now and enter a prize draw for a trip to Hawaii" are visible]

You are doing some research on the Internet when a pop-up window appears saying: "Register now and enter a prize draw for a trip to Hawaii". What do you do?

A) Register your details quickly and carry on with your research

B) Ignore it and close down the pop-up window

C) Keep it minimised for later when you will fill it out in your own time

(if user selects A or C]

This is a bad idea! Pop-ups can be deceptive, and it could be software created by a social engineer – you should always ignore and close down pop-ups such as this and report them to the IT-Service Desk or security department.

[If user selects B]

A wise choice! You should always ignore pop-ups such as this and report them to the IT-Service Desk or security department – it could be software created by a social engineer.

Forward button returns to screen 4

Screen 9

[Graphic: Criminal with many fishing lines and a fishing net, on the hooks of each line and in the net are scraps of paper with account details or User IDs and passwords written on them]

People who use e-mail are increasingly at risk from 'phishing'. This involves a criminal (a social engineer) sending out fake e-mails to trick unsuspecting people into revealing personal information like user names and passwords.

This scam always involves two parts:

- The initial phishing e-mail; a common tactic is to say the victim's account will be closed if they don't update or re-confirm their financial details before a specific date, and
- A fake website, designed to mimic the victim's bank, Internet service provider, payment agency or even the government

The target is instructed to click on a link provided in the e-mail and then, having been taken to the fake website, they are asked to enter their details into a specially designed form. The criminal can now use them fraudulently.

Forward button moves to screen 10

Screen 10

[Graphic: Many people at computers receiving the same phishing e-mail]

Phishing scams work because websites and e-mails are easy to copy and the fakes look good. Added to this, we all want to avoid the hassle of possibly having to set up our bank, e-mail or Internet accounts again, so when we receive something from an official source, seemingly directed to us, we act on it.

But the e-mail isn't specifically directed to any particular recipient; the social engineer sends the very same e-mail to thousands, perhaps even hundreds of thousands of e-mail addresses.

The criminal knows that if just a small percentage of targets have accounts with that bank they might respond and his scam will have been a success.

Forward button moves to screen 11

Screen 11

[Graphic: Villain character sat perched on a ledge above a victim sat at their computer. The phisher is lowering a fishing line down towards the PC]

Although media coverage focuses on the threat to consumers, organisations are also at risk from phishing.

When targeting organisations, phishers could be looking to capture an employee's log on details so that they can gain access to the information system and all the restricted information it contains.

Alternatively, they could be looking for a 'back door' way into the organisation's information system. Their objective here is to release a Trojan to corrupt or disable some part of the system, often the e-mail server.

So how does phishing for organisational details work?

Forward button moves to screen 12

Screen 12

[Graphic: Villain character is bent over and beckoning welcomingly with both hands towards a giant computer screen, urging/inviting the victim towards it]

The phishing e-mail will appear to be from a trusted source such as senior management, or our IT-Service Desk.

Using SP AusNet's standard e-mail layout and design, the e-mail will typically ask you to follow a link to update your User ID and password details to deal with some kind of IT problem that threatens to disrupt your e-mail account or network access.

E-mail styles and websites are easy to copy and the fakes look good. Added to this, most employees will automatically follow any 'official' instruction without question – and who wouldn't want to help avoid a situation that could lock you out of your files and disrupt your work?

Forward button moves to screen 13

Screen 13

[Graphic: Villain character has opened a padlocked door on the side of a computer – they are holding a key in one hand - and is in mid-action of withdrawing a bag of money through the now open door with the other hand].

IT security systems, such as firewalls, are powerless if attackers have a key in the form of a bona fide electronic ID. And as soon as they are inside SP AusNet's networks, fraudsters can download malware, or can steal or corrupt confidential data, such as financial records, at will.

Consequences can include:

- Malicious software installations

- Industrial espionage
- System sabotage
- Billing and invoice fraud
- Corporate credit card fraud
- Theft from client accounts
- Theft of HR or personnel information

Forward button moves to screen 14

Screen 14

[Graphic: Victim character standing up to the phisher assertively with hands on hips – villain character slinking away]

A leading industry survey showed that on average almost a third of the fake e-mails sent by phishers are misidentified as being legitimate, and another survey that one in every 250 e-mail messages contains a virus that helps trigger an attack. So you need to remain alert – particularly if e-mails ask you to 'confirm' details that SP AusNet already has.

If you do receive any suspicious e-mails, make sure that you report them promptly, as others in SP AusNet may not have been so vigilant.

Closely related to phishing, pharming attacks operate at the server level – you type in a legitimate website address but the hacker's software redirects you, without your knowledge, to a fake website where the scam takes place.

It's a sobering thought – but unauthorised access to information systems is the second largest cause of financial loss for organisations.

Forward button moves to screen 15

Screen 15

Attacks from outside usually involve remote attempts to access confidential data. But some illicit activities, such as industrial espionage, involve a more personal touch using a range of everyday devices collectively known as 'sneakers'.

A sneaker is any kind of mass storage device that can be easily concealed. Common examples include mobile phones, USB sticks, PDAs, digital cameras, web cams, digital voice recorders, smart card and magnetic stripe burners.

Click on each of the five items below to illustrate what organisations might be concerned about in this regard.

[Graphic: Mobile phone with camera, USB stick, digital voice recorder, PDA, web camera - user is able to toggle between answers]

[If user clicks on mobile phone with camera]

The majority of mobile phones have in-built cameras. This provides a new means for sensitive data to leak, exposing sensitive data to greater risk from both inside and outside an organisation.

Bans are hard to enforce, so most organisations will have restricted secure zones with guidelines for camera use elsewhere. If you have a camera phone, ensure you know what

the rules for use are in SP AusNet. This very specifically applies to zonal sub station and terminal stations. If you are in doubt contact your corporate security co-ordinator.

[If user clicks on USB stick]

USB sticks, DVD/CD burners, magnetic stripe recorders and external hard drives are all easily connected to most PCs, enabling the user to take data away with them very quickly.

[If user clicks on digital voice recorder]

Digital voice recorders have a legitimate place in business but they can also be used for clandestine recordings. Many mobile phones, too, have a recording facility, which means almost anyone close by could potentially record your conversation.

[If user clicks on PDA]

PDAs (Personal Digital Assistants) are sophisticated pieces of equipment, combining a variety of functions including a mobile phone, an e-mailer, digital camera and voice recorder, and mass storage in an all-in-one device. A PDA could easily be used to record and steal information.

[If user clicks on Web Camera]

Web cameras (web cams) are growing ever more popular but they do bring security risks. They can be hacked into, providing an unprotected way into the organisation's information system and enabling the hacker to see your workspace and possibly details of confidential and sensitive information on your desk.

It's an uncomfortable feeling knowing a hacker could see when employees are at, or away, from their desks and what is going on in confidential meetings.

Forward button moves to screen 16

Screen 16

In this topic you have looked at some of the most common methods used by social engineers and others parties seeking to illegally access confidential data. As you have seen, social engineers have highly developed skills and will use their interpersonal skills alone or in combination with electronic methods to set up sophisticated scams.

You should now recognise how YOU can help protect SP AusNet against these attacks by being vigilant and alert.

Whenever you are asked to disclose potentially sensitive information, either person-to-person or via computer or a combination or both, be cautious. Never give this information to anyone unless you are absolutely sure of his or her identity and authority. Furthermore, don't put yourself and SP AusNet at risk by disclosing your own personal data to an unknown source.

[Graphic: Image of small person standing on top of a pile of personal items, including; a 3D "password", a box file labelled "confidential", and a credit card labelled "banking card" The person has their arms folded in a protective manner, and is looking down at a small villain-like character - from screen 2]

Forward button moves to screen 17

Screen 17

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for preventing social engineering

- Never disclose potentially sensitive information to an unknown source, and never give out more information than seems necessary
- Be wary of e-mails or websites that ask you to confirm sensitive information the organisation already has
- If you have any suspicions don't be afraid to ask questions
- When dealing with telephone calls – be vigilant
- When asked for potentially sensitive data by someone you don't recognise, always ask to see their identification
- If you are being cajoled, harassed or feel manipulated, don't just give information out – always make the appropriate checks first
- Watch out for 'shoulder surfers' – people who may be reading sensitive information on your computer screen/desk

Forward button moves to screen 18

Screen 18

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for preventing social engineering

- Never leave passwords or sensitive information lying around
- If you are suspicious at any time, seek advice from your manager before handing information over
- Always shred sensitive documents, such as financial reports, before you throw them away
- Report any incidents immediately to your manager

AND finally…

If in doubt – DON'T!

Forward button exits module

Module 2k - Incident reporting

Screen 1

[Graphic: Small person dressed as villain, e.g. trench coat with collar turned up, sneaking into a giant computer through a side door with 'authorised access only' written over the top of it]

An information security incident takes place when SP AusNet's computer network is subject to unauthorised use that violates our security policy. This could involve an attack from outside, or intentional or unintentional internal misuse.

Examples could include:

- Unauthorised system access
- Viruses
- Website defacement
- Sabotage
- Disruption or denial of service
- Unauthorised data storage (images, music files, etc.)
- Unauthorised changes to hardware or software

Forward button moves to screen 2

Screen 2

[Graphic: PC – onscreen is a window with a red cross on it, reminiscent of the Microsoft error message window]

How do you know if an incident is taking place?

Sometimes there will be telltale signs, such as:

- The network or your own PC has slowed or is unstable
- The mouse cursor moves by itself
- You see notices of failed sign-ons, at times when you weren't accessing the system
- You notice that file properties such as date or file size have suddenly changed

Small incidents like these, when taken together, point to unauthorised individuals accessing the system, resulting in the possible theft of confidential data.

Forward button moves to screen 3

Screen 3

[Graphic: User sat at their PC looking quizzical, hand on chin, brow furrowed, hand resting on phone].

Work through the following scenario to learn more about how you should handle information security incidents.

You are working at your PC on some financial files when you realise that they were 'last accessed' over the weekend – when you were not at work. They contain sensitive information and are password protected and you're sure no one else should have had access to them. What should you do?

A) Report the incident immediately

B) Get on with your work

C) Discuss it with your manager after lunch and get their advice on whether to report it

(correct answer = A)

If user selects A

Yes. Even if it seems trivial to you, reporting incidents enables SP AusNet to learn more about the violators, link up apparently isolated incidents and reveal any underlying problems. Any delays could help those responsible to cover their tracks.

Security incidents can create bad publicity and incur serious financial losses – so you must report them immediately.

If user selects B

No. Even if it seems trivial to you, reporting incidents enables SP AusNet to learn more about the violators, link up apparently isolated incidents and reveal any underlying problems. Any delays could help those responsible to cover their tracks.

Security incidents can create bad publicity and incur serious financial losses – so you must report them immediately.

If user selects C

No. Even if it seems trivial to you, reporting incidents enables SP AusNet to learn more about the violators, link up apparently isolated incidents and reveal any underlying problems. Any delays could help those responsible to cover their tracks.

Security incidents can create bad publicity and incur serious financial losses – so you must report them immediately.

Forward button moves to screen 4

Screen 4

[Graphic: E-mail form onscreen with 'Incident Report' in 'subject' field. Mouse cursor hovering over 'To' field]

You are writing an e-mail to report the incident that has just taken place. Who should you include in the address list?

A) Your line manager

B) BS&S (the IT-Service Desk)

C) BS&S (the IT-Service Desk) and your line manager

(correct answer =C)

If user selects A

Incorrect – management will always need to be informed, but BS&S (the IT-Service Desk) may need to know as well. Also, some incidents may need to be reported to the authorities because they may involve certain illegal actions.

Your report should be as detailed as possible, describing any system vulnerabilities or modifications made. The more that is known about the causes and consequences of each incident, the more security can be improved.

If user selects B

Incorrect – BS&S (the IT-Service Desk) will need to be informed, but management must also be told. In addition, some incidents may need to be reported to the authorities because they may involve certain illegal actions.

Your report should be as detailed as possible, describing any system vulnerabilities or modifications made. The more that is known about the causes and consequences of each incident, the more security can be improved.

If user selects C

Correct. Both BS&S (the IT-Service Desk) and management will need to be informed. Also, some incidents may need to be reported to the authorities because they may involve certain illegal actions.

Your report should be as detailed as possible, describing any system vulnerabilities or modifications made. The more that is known about the causes and consequences of each incident, the more security can be improved.

Forward button moves to screen 5

Screen 5

[Graphic: Person pulling the plug from their PC]

You've reported the incident in as much detail as possible. What else should you do before you get back to work?

A) Delete the files in question, as they may now contain viruses

B) Nothing – just wait for further instruction

C) Turn off your PC and reboot it to make sure any unauthorised link with the outside is broken

(correct answer = B)

If user selects A

That's incorrect. It's vital that you don't do anything to taint the evidence. Don't delete or turn off anything until you have received further instruction. If the problem involves obscene onscreen images you can't get rid of, just turn off your monitor and wait for further assistance.

If user selects B

That's right. It's vital that you don't do anything to taint the evidence. Don't delete or turn off anything until you have received further instruction. If the problem involves obscene onscreen images you can't get rid of, just turn off your monitor and wait for further assistance.

If user selects C

That's incorrect. It's vital that you don't do anything to taint the evidence. Don't delete or turn off anything until you have received further instruction. If the problem involves

obscene onscreen images you can't get rid of, just turn off your monitor and wait for further assistance.

Forward button moves to screen 6

Screen 6

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

Rules for incident reporting

DO:

- Report all incidents immediately
- Be as detailed as possible
- Try to keep the evidence as it is and wait for further instruction
- Check SP AusNet's existing procedures and follow them carefully

DON'T:

- Delete files or taint the evidence

Forward button exits module

Module 3 – Information security in action

Screen 1

[Graphic: Office scene, comprising desk with phone and computer, two drawer filing unit. On computer screen is a screen saver]

In this module you should imagine you are a new employee at the fictitious organisation, Salford Secure Holdings. You have just attended an induction seminar at which you were given an induction pack that has all the essential information you need to get started at your desk.

You're now in your office, following the instructions in the pack on how to log on to the organisation's information system.

Forward button moves to screen 2

Screen 2

*[Graphic: Computer screen with dialog box entitled: 'Change Password' in the box are spaces for user to 'Enter New Password: **********' and 'Confirm New Password: **********'. Underneath the box is a message with smaller illegible content]*

You have entered your User ID and the initial password given to you. The system immediately prompts you to choose a new password. A message on the screen reminds you to choose a 'strong password'. How would you define a strong password?

A) One that contains only letters and no numbers

B) One that includes your initials or date of birth

C) One that is easy for someone to guess but difficult to remember

D) One that is easy to remember but difficult for someone else to guess

Correct = D

If selection = A, B or C

That's incorrect. A strong password is one that is easy to remember but difficult to guess. To ensure that your password is strong you should follow some key rules.

A password should be at least eight characters long, and should include a mix of upper and lower case letters, numbers and special characters, and shouldn't be based on words taken straight from a dictionary.

A good approach is to use the 'pass-phrase' or 'first-character' basis. You think of a phrase (ideally including a number) that you can remember easily. You then take the first letter of each word to make your password, ensuring that the rules for length and mix of letters, numbers and special characters is followed.

If selection = D

You're right. The rules are that a password should be at least eight characters long, and should include a mix of upper and lower case letters, numbers and special characters, and shouldn't be based on words taken straight from a dictionary.

A good approach is to use the ‘pass-phrase’ or ‘first-character’ basis. You think of a phrase (ideally including a number) that you can remember easily. You then take the first letter of each word to make your password, ensuring that the rules for length and mix of letters, numbers and special characters is followed.

Forward button moves to screen 3

Screen 3

[Graphic: As in Screen 2 but with an Emperor Penguin on the desk]

Recalling a documentary you recently watched, your first thought for a password is to use ‘Emp3rorp3nguin’.

How would you rate this password?

A) Strong

B) Medium

C) Weak

Correct = C

If selection = A

No, although it has more than eight characters and does include a mix of upper and lower case letters and numbers, it is actually quite weak.

It is based on a term straight from the dictionary – Emperor Penguin – with each lower case ‘e’ replaced by a ‘3’. A better one could be based on the pass-phrase ‘My number one favourite animal is the Emperor Penguin’ - M#1faitEP.

If selection = B

Well, even though it has more than eight characters and does include a mix of upper and lower case letters and numbers, it is actually quite weak.

It is based on a term straight from the dictionary – Emperor Penguin – with each lower case ‘e’ replaced by a ‘3’. A better one could be based on the pass-phrase ‘My number one favourite animal is the Emperor Penguin’ - M#1faitEP.

If selection = C

Yes, although it meets some of the rules, it is actually quite weak.

It is based on a term straight from the dictionary – Emperor Penguin – with each lower case ‘e’ replaced by a ‘3’. A better one could be based on the pass-phrase ‘My number one favourite animal is the Emperor Penguin’ - M#1faitEP.

Forward button moves to screen 4

Screen 4

[Graphic: Rubik’s cube]

You change your mind and after a little more deliberation you come up with a password that you are happy with.

You enter your new password and the system responds with a message informing you that you will be reminded when your password needs changing but that you can change it at any time if you feel it has been compromised.

Forward button moves to screen 5

Screen 5

[Graphic: Chalkboard with possible passwords listed, all except one is in strike-through text as though discarded. Final one – just shown by 10 asterisks has a big tick beside it. Discarded passwords are 'Mmaws1', 'Rhythm&blues', 'Awsz123']

Peter, another new employee who you met in the induction seminar, comes into your office. He says he is having trouble logging on to the system and can't get through to the IT-Service Desk, so asks for your help.

What should you do?

A) Explain the rules and suggest he creates his own from them

B) Explain the rules and give him a few examples to choose from

C) Explain the rules and use your new password as an example

Correct = A

If selection = A

You're right, having explained the rules to him, Peter will need to create his own password.

You should never share your password or use it as an example – this would compromise them and they would have to be changed immediately.

If selection = B

The best option is to explain the rules and suggest he creates his own password. If you do give examples, make sure you don't use your own password or suggest that Peter uses one of the examples for his own password. Doing so would compromise them and they would have to be changed immediately.

If selection = C

This would compromise your password and you would have to change it immediately. Once the rules have been explained to him, Peter will need to create his own secret password.

Forward button moves to screen 6

Screen 6

[Graphic: An e-mail screen with toolbar shown. Two buttons are clearly visible, 'Yes' and 'No']

Following the steps in your induction pack you successfully access the e-mail system. Your inbox already contains a few e-mails including one from your own line manager suggesting a meeting later today.

You decide to send a quick e-mail to a friend to let her know how you are getting on at your new job, so you open your Internet browser and type in the address of your personal web-based e-mail account.

When you arrive at your inbox there are a number of personal e-mails waiting for you. Should you open them?

A) Yes

B) No

Correct = B

If selection = B

You're right. You shouldn't open these e-mails. In fact, you shouldn't use your company's computer to access personal e-mail accounts at all.

These web-based accounts may not be protected by the level of security required to safeguard the network from attack – so e-mails containing malicious software could get through. If you open any of these infected e-mails on your work computer, malicious software could infiltrate and spread across the organisation's network.

If selection = A

That's not the right answer. You shouldn't open these e-mails. In fact, you should not use your company's computer to access personal e-mail accounts at all.

These web-based accounts may not be protected by the level of security required to safeguard the network from attack – so e-mails containing malicious software could get through. If you open any of these infected e-mails on your work computer, malicious software could infiltrate and spread across the organisation's network.

Forward button moves to screen 7

Screen 7

[Graphic: Picture of an e-mail subtitled 'E-mail'; picture of an Internet website subtitled 'Internet']

Looking through your induction pack you see that the organisation has a clear policy on acceptable use of the information systems.

The policy explains that the organisation owns the information systems and any information that resides on them. It explains that any use of the information systems or any other organisational asset for on-line shopping, gaming, personal profit, or other is strictly prohibited.

Your attention is drawn to two specific sections. Click on each of the images for a summary.

If click on E-mail

- The e-mail system is primarily provided for business use but limited and reasonable personal use is permitted where it does not impact on an employee's workload
- The organisation monitors all e-mail traffic and will take action to ensure no inappropriate material is received or sent
- E-mail is not a secure method of communication and employees are reminded to consider this before sending e-mails
- E-mail communication is admissible in court and employees should apply the same high standards to e-mail as they would for other communication channels

If click on Internet

- Internet access is provided for business use but limited and reasonable personal use is permitted where the use is considered acceptable and does not impact on an employee's workload

- The organisation monitors all Internet usage and will take action to prevent infringement of its usage policy
- Access to certain material is strictly prohibited and the organisation will block access to sites known to host such material

Forward button moves to screen 8

Screen 8

[Graphic: Picture of an e-mail screen and an envelope with a padlock attached to it]

Looking through the induction pack, you notice that the organisation has a policy that e-mails containing anything other than Public information should be encrypted. This is more stringent than your previous employer's policy, and you wonder if the organisation is being over cautious.

You start to think about this and all the different types of Sensitive, Private and Confidential information that is used within an organisation. You soon realise that the value of this information to the organisation, and the privacy laws it may have to conform to, mean security and confidentiality is a major issue.

Forward button moves to screen 9

Screen 9

[Graphic: An Internet site for 'Fishing Equipment', and alongside, small dingy and a box of 'Food']

In the induction pack, you read the warnings about responding to e-mails that could be phishing scams. It reminds you that you want to order some supplies and equipment for your family's forthcoming weekend fishing trip to the lake.

You have Internet access on your computer; can you use it for this purpose?

A) Yes, this is considered acceptable use

B) No, this is never acceptable use

C) Only if the organisation's policy allows it

Correct = C

If selection = A

Some organisations do allow Internet shopping as 'limited and reasonable' use, although they may restrict it (either by policy or software) to lunch times only. Other organisations prohibit it altogether.

You should always check your organisation's Acceptable Use Policy. If personal use is allowed, you should ensure you don't impact on your work by keeping all personal Internet use to your break or lunch times.

If selection = B

While some organisations prohibit Internet shopping, others allow do allow it within the terms of 'limited and reasonable' personal use, although they may restrict it (either by policy or software) to lunch times only.

You should always check your organisation's Acceptable Use Policy. If personal use is allowed, you should ensure you don't impact on your work by keeping all personal Internet use to your break or lunch times.

If selection = C

Like many organisations, Salford Secure Holdings does include Internet shopping within the terms of 'limited and reasonable' personal Internet use. However, its policy and software limits such use to lunch times only.

You should always check your organisation's Acceptable Use Policy. If personal use is allowed, you should ensure you don't impact on your work by keeping all personal Internet use to your break or lunch times.

Forward button moves to screen 10

Screen 10

[Graphic: A plain brown, A4 sized envelope; a printer; an e-mail screen and a USB stick]

You have just come back from your first project meeting and have details of the documents you need to read to familiarise yourself with progress to date. You think you will have more time to read them at home, and are wondering how best to maintain security.

Which of the following is the best option?

A) Print the documents and take them home in an un-marked envelope

B) E-mail them to your home e-mail account

C) Save them on to a USB stick

If selection = A

This is not very secure at all. Hard copies are immediately accessible to anyone who has possession of them. E-mailing them to your home account is not acceptable because 'home systems' are unlikely to have sophisticated security controls, which means e-mails can be easily intercepted.

A better option would be to save the documents to a USB stick, ideally with some form of encryption or password security, which you can then lock in your briefcase or secure on your person.

Before you do anything, however, you must check your organisation's policy. You may find that certain classifications of information cannot be taken from the building at all.

If selection = B

Many organisations strictly prohibit e-mailing documents to your home e-mail address. This is because 'home systems' are unlikely to have sophisticated security controls, which means e-mails can be easily intercepted.

A better option would be to save the documents to a USB stick, ideally with some form of encryption or password protection, which you can then lock in your briefcase or secure on your person.

Before you do anything, however, you must check your organisation's policy. You may find that certain classifications of information cannot be taken from the building at all.

If selection = C

You're right; this is the best option. Ideally, you should encrypt or password protect the files, then lock the USB stick in your briefcase or secure it on your person.

Before you do anything, however, you must check your organisation's policy. You may find that certain classifications of information cannot be taken from the building at all.

Forward button moves to screen 11

Screen 11

You are reading some of the project documentation when Peter comes over and suggests you go and get a coffee. You readily agree, but what should you do before leaving your desk?

Click on any item that you think you should tidy up before you go.

You have 5 items to find.

[When user clicks on item, the appropriate text is displayed, the item is erased from screen or animates and the number of items left to find counts down]

[Graphics: Report stamped 'Confidential' left lying on desk; USB stick; desk drawers are open with file in it, key in lock; computer screen is active, showing a spreadsheet of figures; mobile phone on the desk]

Number of items remaining counts down as user clicks each one

When selection = Report, text as below

Remember that not all people in the organisation will have the same access rights as you – so never leave Confidential, Sensitive or Private information on show.

When selection = USB stick, text as below

Removable storage devices are easy to steal, so always lock them away or take them with you when you leave your desk.

When selection = desk drawer, text as below

If your desk has lockable drawers use them for portable electronic equipment and files requiring any degree of confidentiality.

When selection = computer, text as below

You should always lock your screen or log off, even if leaving your computer for just a few minutes.

When selection = mobile phone, text as below

Portable equipment such as mobile phones or laptops are valuable in themselves and for the information they contain, so always take them with you or lock them away when leaving your desk.

When learner has clicked all items

Good, now that your desk meets the organisation's clear desk policy you can go and enjoy your break!

Forward button moves to screen 12

Screen 12

[Graphic: Head office building, with lots of employees walking towards it. A security guard is by the entrance doors]

The purpose of information security policies and procedures is to ensure that everyone within SP AusNet, including you, takes the precautions needed in order to keep information, information assets and information systems as secure as possible.

And as you have seen in this module, you are required to play your part from the moment you become an employee.

Forward button exits the module

Module 4 - Management and IT responsibilities

Screen 1

As a manager or IT representative you have additional responsibilities for information security.

Click on each of the five pendulums below for more information.

[Graphic: Five balls on a Newton's Cradle. Brass plaque on side has 'Management and IT responsibilities' written on it. When a ball is hovered over, the base shows the title. When a ball is selected, the balls with swing one way and then back]

Information security management

Staff training and supervision

Responsibility for assets

Incident reporting

Business continuity

If selection = 'information security management' go to screen 2
If selection = 'staff training & supervision' go to screen 3
If selection = 'responsibility for assets' go to screen 4
If selection = 'incident reporting' go to screen 6
If selection = 'business continuity' go to screen 8

Forward button moves to screen 12

Screen 2

Information security management

Responsibility for the management of information security is shared between SP AusNet's managers and its security department and BS&S Division.

Examine the device to find out more.

[Graphic: Safe-type combination lock labelled 'Managers', 'BS&S' and 'Security department'. Text that appears to the side of lock when clicked on, with small people standing at the edge]

If selection = 'managers', text as below

Managers provide an expert knowledge and understanding of our business needs.

Managers know what information is required by whom, and will work with BS&S and the security department to ensure this can be provided in a timely and secure way.

If selection = 'BS&S', text as below

BS&S contributes a specialist understanding of systems design and the skills needed to build IT security controls into the IT system as an integral part of its design.

They will work with management and security specialists to ensure the system performs the functions required, is reliable and robust and that backups are available if needed.

If selection = 'Security department', text as below

Security brings specialist knowledge of security matters, including likely risks and the effectiveness of different types of control in minimising these risks.

They will work with management and BS&S to ensure security aspects are relevant and appropriate for the system and the information it holds.

[When one item has been selected, the following text appears 'Click on the device again to find out more.']

[When all items have been selected, the following text appears 'Click on the forward button to move on.']

Forward button moves to screen 2a

Screen 2a

The contribution of managers and IT staff is a vital one in the day-to-day management of information security.

You need to be aware of the risks to information security and be committed in your efforts to lead by example in your own adherence to information security best practice.

Forward button returns to screen 1

Screen 3

Staff training and supervision

[Graphic: Scales with group of small people on one side and one larger manager on the other]

Explore the picture by clicking on each side of the scales.

If selection = left hand side of scale with small people

Your staff should be:

- Aware of the risks of not following good information security procedures
- Aware of which procedures apply to their job role
- Competent in using the appropriate security controls
- Diligent in following SP AusNet's policies and procedures

If selection = right hand side of scale with manager

If you are a manager, it's your responsibility to:

- Promote information security in your department
- Encourage best practice by ensuring your staff are aware of, and comply with, the rules
- Monitor workplace practice
- Deal firmly with incidences of non-compliance

Forward button returns to screen 1

Screen 4

Responsibility for assets

You may have had certain information assets assigned to you. You are the nominated 'owner' of these assets – which means that you are ultimately accountable for taking proper precautions to protect them from loss, damage, destruction, misuse or theft.

Click on the four assets to find out what they may include.

[Graphic: Montage of graphics on side of screen, when graphic is clicked text appears on the other side]

Information assets *[Graphic: A file pulled from a filing cabinet]*

Include all forms of data, whether in soft or hardcopy format; for example, databases and data files, system documentation, user manuals, training materials, operational or support procedures and continuity plans.

Software assets *[Graphic: Software]*

Include application software, system software, development tools and utilities.

Physical assets *[Graphic: Computer monitor]*

Include computer equipment, communications equipment, storage media, other technical equipment, furniture and accommodation.

Services *[Graphic: Plug and desk light]*

Include information systems and communications services and general utilities such as heating, lighting and power.

Once all the interactions are complete, instructional text changes to:

Click on the forward button to move on.

Forward button moves to screen 5

Screen 5

Make sure you know which information assets are *your* responsibility.

If you're not sure, take time now to check with your manager or supervisor.

Once these assets have been identified, you need to take steps to ensure that they are adequately protected. This may include:

[Graphic: Small person looking up at mobile phone and laptop]

…making sure that a log exists showing the key users and the whereabouts of any portable items such as laptops or mobile phones…

[Graphic: Small person looking up at CDs representing backups, tape says 'Backup']

…making sure that backup routines are correctly followed for any information systems for which you are responsible…

[Graphic: Small people holding a pen which is being used to mark an item, such as a base unit]

…making sure that equipment is marked clearly according to your SP AusNet's policy, so it can be easily identified and tracked…

[Graphic: Small character placing a tick onto a box on a 'procedures' list]

…making sure that staff follow the policies and procedures and do not expose information assets to unnecessary risk…

Forward button returns to screen 1

Screen 6

Incident reporting

If a potential security risk is exposed, then it's vital to report the incident immediately.

[Graphic: Small person standing next to handset with cable running off (no phone base), her hands around her mouth to form a megaphone – shouting into the handset]

Any staff for which you are responsible must report any incidents that they are aware of, in the first instance, to you. So they must know the procedures for reporting incidents and for not corrupting evidence.

Your responsibility, as a manager, is then to decide what to do about the incident and, if necessary, to enlist the help of security experts in helping to resolve it as quickly as possible.

Where information security is concerned, any delay can lead to serious complications; so make sure that your staff are aware of this and the need to report incidents in a prompt, timely fashion.

Forward button returns to screen 1

Screen 8

Business continuity

Business continuity describes the processes and procedures an organisation puts in place to ensure that essential functions can continue during and after a disaster. Business continuity planning seeks to prevent interruption of mission-critical services, and to re-establish full functioning as swiftly and smoothly as possible after any interruption.

No organisation wants to suffer a breach of its information security defences. But even the best defences are not always failsafe. It therefore needs a 'Business Continuity Plan' (BCP) which sets out the actions to be taken to restore business as usual after a critical incident.

However, it is better if the breach can be avoided, so organisations put in place pro-active controls to help minimise and manage risks.

[Graphic: Security guard protecting the cordoned off area, with all three items contained within]

Forward button moves to screen 9

Screen 9

[Graphic: Lever like on an automatic gear shift with four notches – the first notch is the starting point and is labelled "neutral" (faded down so as not to look like a hotspot), second is labelled "preventative", third is labelled "detective", and fourth is labelled "recovery". Pulling the lever into each notch will bring the bullets up alongside]

SP AusNet uses a range of 'preventive', 'detective' and 'recovery' controls to manage the risks to information security.

Click on each of the three words next to the gear lever to explore these different types of control.

If selection = preventative, text as below

Preventive controls help prevent security breaches from occurring. They include:

- Passwords and/or data encryption (to prevent unauthorised access)
- Security education (to raise staff awareness of the risks)

- Change control procedures (to prevent unauthorised changes to systems or data)

If selection = detective, text as below

Detective controls are designed to alert you to a security breach when it has happened. They include:

- Systems audits (to check for and anticipate potential problems)
- Input data validation (to check the integrity of any data entered into the system)
- Virus scanning (to check for the presence of viruses)
- Event logging (to detect and keep track of irregular transactions across the system)

If selection = recovery, text as below

Recovery controls are there to help you get up and running again after an unexpected incident. They include:

- Robust backup procedures to fill the gaps left by an incident – from repairing a single database through to bringing on-line an exact replica of the complete information system
- Upgrades and 'fixes' to repair any damage caused by malware in the system (these will be applied to both the main and the backup system)
- An auxiliary power supply (to keep things running, should the power fail)
- A business continuity plan (so everyone knows what to do in the event of a crisis)

Forward button moves to screen 10

Screen 10

For a business to recover quickly (and minimise its losses) from an incident, all staff will need to be aware of, and trained on, SP AusNet's BCP (Business Continuity Planning) and DR (Disaster Recovery) procedures.

If a major incident does affect your area, then as a manager or IT representative, you will have a key role to play in ensuring that this plan is promptly activated and correctly followed.

To fulfil this role, you need to be fully conversant with the BCP – find out where you can obtain a copy and make the time to read through it carefully to see how and where it applies to your area of the business.

[Graphic: Hotspot of a closed business continuity plan document. Two small people looking up at document which is labelled 'business continuity plan']

Forward button moves to screen 11

Screen 11

The headings on this BCP are indicative of those you might find on your own divisional plan.

Browse through the plan on screen, so you know what sorts of things to look for in your own divisional plan.

[Graphic: As screen 10. The user sees all four headings which remain on the book at all times which, when clicked on, brings up the heading and description on right hand side of screen].

If click on: emergency procedures

EMERGENCY PROCEDURES

These describe the immediate actions to be taken in the event of a major incident.

If click on: fallback procedures

FALLBACK PROCEDURES

These describe the actions to be taken to move essential business activities or support services to alternative temporary locations.

If click on: resumption procedures

RESUMPTION PROCEDURES

These describe the actions to be taken to return to normal full business operations as quickly as possible.

If click on: test schedule

TEST SCHEDULE

This specifies how and when the plan will be tested. Testing the plan is vital, so that problems and oversights can be corrected under test, rather than crisis, conditions.

Forward button returns to screen 1

Screen 12

Management and IT responsibilities

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

In your role as a manager or IT representative you should be aware of the additional responsibilities you have, which include the following:

- Be aware that the responsibility for information security is shared between managers, BS&S and security
- Ensure that your staff are informed about the risks relating to information security, and are aware of the appropriate security controls
- Monitor compliance with information security policies and procedures

Forward button moves to screen 12

Screen 12

Management and IT responsibilities

[Graphic: Small person placing the 's' on to the end of the word 'Rule']

- Find out which assets you are responsible for, and protect them from loss, damage, destruction, misuse and theft
- Encourage your staff report any information security incidents to you – then take appropriate action and inform those who need to know

- Familiarise yourself with the range of preventive, detective and recovery controls that SP AusNet uses
- Keep yourself up-to-date with the business continuity plan

Forward button exits module

Help screen:

Left and right arrows…

Follow any instructions you are given on the screen. When you are ready to move on, click on the right-hand arrow to move forward to the next screen. The left-hand arrow will return you to the previous screen.

Exit…

Click here to exit the course.

Glossary…

Click here to access a Glossary of terms used within the course.

Instructions…

Click or press any key to return to the last screen.

Glossary:

Access, Permission or right to obtain information.

Access control, Prevents individuals from obtaining information for which they do not have permission or authorisation.

Accountability, Determines who is ultimately responsible, i.e. the person who is answerable for any problems or incidents that may occur.

Assets, The property or possessions that give an organisation its bottom line value. Information, hardware, software, buildings, expertise, skills, etc., are all examples of assets that give a real value to the organisation.

Audit, Formal process for reviewing and verifying the effectiveness of an organisation's controls and procedures.

Authorised, Officially recognised and endorsed by the organisation or owner.

Auxiliary power supply, Emergency power backup that kicks in automatically, if the main power supply is cut or interrupted.

Availability, Relates to the business need to ensure that information is available to authorised users when it is required.

Bcc, Used when creating e-mails to provide a space for you to type in the e-mail addresses of people who should receive the message, but should be hidden from other recipients.

Backup, Copies of computer files, documents, applications, databases, spreadsheets, etc., that are regularly updated, held in reserve and used to restore systems and information that have been lost, damaged or corrupted.

Backup cycle, Refers to the frequency with which backups are made, and the number of backup versions that are held in reserve. For example, a seven-day backup cycle would mean that backups are made daily, and that copies of the last seven-day's backups are held in reserve.

Bot, A term (derived from robot) for a software agent that carries out a particular task it has been programmed to follow.

Botnet, A network of computers infected with the same bot, remotely controlled by the bot originator.

Business continuity plan, Plan detailing how critical business processes will be maintained or recovered, in the event of a major failure or disaster.

Business continuity planning, The process of planning how to protect critical business processes from the effects of major failures or disasters, so that the organisation is able to continue functioning.

Change control procedures, Affect any changes that are made to software applications, hardware, computer systems, operating procedures, security controls or business continuity plans. The idea is that all changes are formally agreed, authorised and documented before being implemented.

Classification, The process whereby an organisation identifies and 'labels' information and other assets, according to their value or sensitivity. The level of classification determines the level of security that needs to be applied, in protecting that asset. The more valuable the asset, the greater the security required to protect it.

Classified, Not in the public domain, i.e. information that has some degree of confidentiality attached to it and that is therefore available only to those who are authorised to have it.

Compliance, Refers to the legal and contractual obligation on individuals to follow the organisation's specified information security policy and procedures.

Confidentiality, Relates to the business need to ensure that information is accessible only to those authorised to have access.

Connection, Electronic link-up between one computer device and another; point of access into a computer system.

Controls, The various procedures or devices that an organisation might use to regulate access to information, software and hardware assets, the way in which these are used and by whom.

Controlled-circulation, Restriction of access to a limited audience, to information that is not in the public domain.

Crash, Failure of computer systems or applications.

Database, A large body of information that can be processed, managed and stored electronically, on a computer.

Detection, Identification of information security problems or incidents.

Disclosure, Where information is revealed; unauthorised or improper disclosure is where information is revealed to someone who is not entitled to have it.

Download, To copy files or data from a host computer, usually a mainframe computer, to another.

Encryption, A process whereby confidential information can be stored and transmitted in a scrambled or encoded format, such that the original information cannot be obtained without knowledge of a secret key.

Event logging, A record held in the system, showing events; for example, all requests/accesses made to an organisation's computer systems.

Fixes, Technical solutions that can be applied to technical problems such as viruses, incompatibilities, etc.

Hacker, Anyone who gains or attempts to gain unauthorised access to computer systems and computer-held information.

Hard disk, The permanent disk drive inside a PC on which software applications, data files, etc., may be stored.

Hardware, Includes any physical computing device or equipment, e.g. monitors, keyboards, cables, modems, printers, etc.

Identity theft, Someone posing as you by using your personal information without permission, in order to commit fraud.

Impact, The business implications and costs incurred in the event of a security breach or systems failure.

Incident reporting, Formal reporting and recording of all incidents that may have information security implications.

Information security incident, Any kind of incident or event in which the security of information or systems may have been breached or put at risk.

Input data validation, Controls designed to check for inputting errors such as out-of-range values, invalid characters in data fields, etc.

Instant Messaging System, (IMS), A communications mechanism, using IP technology, that exchanges user messages in real time.

Integrity, Relates to the business need to safeguard the accuracy and completeness of information and to protect the systems used to process it.

Inventory, A formal, written listing or catalogue of all the assets held or owned by the organisation.

IP Telephony, the software and systems by which voice telephone calls are made and routed and over the Internet. (Voice over IP – VoIP).

ISO 27002, A suite of internationally recognised standards for information security best practice. ISO 27002 replaces ISO17799.

IT disaster, Serious failure or interruption in the normal operations and services provided by an organisation's computing systems.

.jpg file extension, This is a well known type of graphics file.

LAN, Local Area Network, a communications network linking PCs, servers, printers etc. within a limited geographic area – usually a building.

LAN administrator, The person responsible for the day-to-day management and maintenance of the Local Area Network.

Laptop, Portable computer.

Licensed software, i.e. software that is subject to copyright restrictions.

Mainframe, A single, centralised data processing and data storage unit that may be accessed and used simultaneously, by individuals working from terminals at different locations around a building.

Malware, Generic name for any form of malicious and unwanted program on your information system. Malware includes, but is not limited to, computer viruses, Trojan horses (viruses and destructive code hidden behind a seemingly innocent program), adware, freeware, shareware, spyware and spam.

Mini-computer, A smaller scale version of a mainframe computer.

Modem, This is computer hardware. The modem is what enables a telecommunications link to be established between computers, so that information can be transferred directly between them.

Network, i.e. where any number of separate computer systems, including PCs and mainframes, are linked together to form part of a single system, enabling transfer and sharing of information and resources. Networks are fast becoming the norm for most organisations in how they set up and manage their computer systems.

Non-compliance, Where an individual either ignores or acts in breach of the organisation's specified information security policy and procedures.

Owner, The person with designated responsibility for a particular asset.

Password, A secret code that is used to verify an individual's identity before granting them access to a system or information source.

Penetration testing, Involves periodically testing a computer system's security for weak spots, i.e. ways in which an unauthorised hacker might be able to break through the system's defences.

Personal information, Any information that is of a personal nature and specific to a particular individual, e.g. date of birth, address, phone number. It also relates to employee, vendor and customer information.

Pharming, The process by which criminals intercept you when you enter a website address, and take you to a fake website to activate a scam or malware.

Phishing, The process where criminals send fake e-mails that trick you into revealing personal information like user names and passwords.

Policy, Statement of principle that defines organisational beliefs and procedures.

Prevention, Minimisation of risks and threats to the security of information, hardware and software assets.

Procedural control, Specified procedure designed to minimise the risks to security of information, hardware and software assets.

Procedure, Specified method or approach.

Public domain, Information that has no particular importance or confidentiality attached to it, is unrestricted and therefore generally available, i.e. in the public domain.

Remote access technologies, Any kind of communications technology that enables you to access information from a distance, using a modem connection.

Risk, The likelihood of a potential threat affecting the security of information, hardware and software assets.

Risk assessment, The process of identifying and evaluating the various risks to which information, hardware and software assets may be exposed.

Risk management, The process of putting in place procedures and controls to minimise and manage the potential impact of security risks.

Screensaver, A piece of software that can be set to activate automatically, running continuous pictures and images across the screen, so that it does not hold any single image for too long a period of time, in order to prolong the lifetime of the screen. A password can be attached to a screensaver so that access is restricted while the screensaver is active.

Security breach, Any incident or event in which security controls and procedures are bypassed, thereby introducing a potential threat to security.

Security education, The process of informing people about an organisation's security policy, and enabling them in the use of agreed security procedures and controls.

Server, A central or primary computer in a network, that drives the applications and operational software used by other computers in the network. It may be a file server for central storage of user files, or it may be a print server that provides printing facilities.

'Shoulder surfers', Those who either purposely overhear conversations or look over shoulders for information.

Sneakers, A collective terms describing any kind of mass storage device that can be easily concealed. Common examples include mobile phone, PDA, USB stick, web cams, etc.

Social engineering, The process of getting sensitive information, such as passwords and access rights, from employees inside an organisation using manipulation and/or intimidation**.**

Software, Any computer program or application.

Spoofing, When an individual masquerades as another person, or pretends to represent another organisation, in order to obtain unauthorised access to information on the Internet.

Spreadsheet, A particular type of software, used generally for processing figures and calculations.

Swipe card, An electronic card that, when 'swiped' through a card reader, identifies the cardholder. Swipe cards are typically used to regulate access to restricted areas of an organisation's premises.

Systems, An overall term used to describe an organisation's computing and information technology facilities.

Tape streamer, A device that can be used to make backups of computer-held information and data.

Technical control, A control that is built into an organisation's computing system, and which is designed to regulate access to information held on the system.

Terminal, A single computer linked into a wider network of computers; point of access to an organisation's network or computing systems.

Trojan Horse, A virus or destructive code hidden behind a seemingly innocent program.

USB stick, A small removable data storage device that uses flash memory and a USB connector. Also known as USB key/memory key, USB drive/flash drive, USB/flash device, keychain drive, micro hard drive, pen drive, pocket drive, thumb drive, jump drive.

User ID, Known in some organisations as the log on ID; this is the name that is used to identify any user gaining access to a computer system, or making transactions within that system.

Virus, Computer viruses are self-replicating programs that can infect other programs or computer files, interfering with their correct functioning.

Virus checking, The process by which incoming data is screened for computer viruses; may also be referred to as virus scanning.

Virus scanning, The process by which incoming data is screened for computer viruses; may also be referred to as virus checking.

Web cam, A small digital camera attached to a PC and that, via software, streams a video signal to the recipient's computer.

Exit screen:

Are you sure you wish to exit?

Yes

No

If user selects 'yes' they exit the course. If user selects 'no' they are returned to the last screen they visited

Game chooser introduction:

This module contains a game designed to test how much you have learned about information security. You can choose to complete a simple, text-based presentation of questions, or take the interactive assessment to add an element of fun.

Please make your selection below.

[Graphic: Two animated examples of the different games, each labelled as below]

Text-Based Assessment

The Golf Game

Text Based Assessment Introduction:

Welcome to The Security Challenge.

This test is designed to challenge your knowledge of information security.

Work your way through all 20 questions, selecting one of the multiple choice answers for each question. When you are ready to start, click the forward button to begin.

You'll receive 1 point for each question answered correctly. If you don't answer at least 14 questions correctly, you'll need to re-take the test. Good Luck!

Golf Game Introduction:

Welcome to The Security Challenge.

After studying hard to improve your knowledge of information security, what better way to relax than a quick game of golf! If you're not really a golf fan, don't worry – as you'll soon find out, if you've been concentrating during the program you will be more than a match for even a professional golfer!

The aim of the game is to play a round of golf and reach the clubhouse. However, you'll be accompanied by your Information Security Manager who will ask you a question to test your knowledge before you tee off at each hole. You need to answer correctly to get the ball in the hole.

Each correct question will earn you bonus points. Clicking on one of the three golf balls will determine how much each question is worth. The points you have earned are shown on your scorecard.

If you're ready to begin, click here. Good luck.

Question bank:

MODULE 1:

What is information security and why does it matter?

Question 1

Classified information is information that has some confidentiality attached to it. Access to this type of information should be strictly controlled. Is this true or false?

A) True

B) False

[answer = A]

[if selection = A]

That's correct, any information that is classified has a security classification attached to it and should not be disclosed to an unauthorised person.

[if selection = B]

Sorry, your choice is incorrect. Any information that is classified has a security classification attached to it and should not be released to an unauthorised person.

Question 2

Which of the following statements best describes the purpose of information security?

A) Making sure that information, information equipment and systems are kept secure and available for use by the proper authorised people

B) Protecting information, information equipment and systems by 'keeping people out', i.e. preventing access

C) Ensuring that information systems are not subject to unauthorised access from hackers

[answer = A]

[if selection = A]

Yes. Information security is concerned with the security of information, equipment and systems (computerised or otherwise) by which information is processed, managed and stored.

[if selection = B]

Your choice is incorrect. The idea of information security is to 'control' access to information and information systems. It allows 'authorised' people in, but keeps 'unauthorised' people out. It also prevents unauthorised changes to and use of information and systems.

[if selection = C]

No, it is much wider than this. The idea of information security is to 'control' access to information and information systems. It allows 'authorised' people in, but keeps 'unauthorised' people out. It also prevents unauthorised changes to, and use of, information and systems.

Question 3

What are the three main objectives of any information security strategy?

A) To protect confidentiality, maintain secrecy and prevent access

B) To protect confidentiality, protect integrity and maintain availability

C) To damage systems, destroy data and make confidential information generally available

[answer = B]

[if selection = B]

That's correct. The main objectives are to keep information confidential, protect the integrity of information and information systems and make sure that information can be made available to those who are authorised to have it.

[if selection = A]

Sorry, your choice is incorrect. The main objectives are to keep information confidential, protect the integrity of information and information systems and make sure that information can be made available to those who are authorised to have it.

[if selection = C]

Sorry, your choice is incorrect. The three main objectives are to keep information confidential, protect the integrity of information and information systems and make sure that information can be made available to those who are authorised to have it.

Question 4

On average, how long can an organisation survive a failure in its computer facilities and systems?

A) 3-4 hours

B) 3-4 days

C) 3-4 weeks

[answer = B]

[if selection = B]

Yes. About 10% of organisations are in serious trouble if their systems are down for just 3-4 hours. A major systems failure can put an organisation out of business in a very short amount of time. However, the loss for SP AusNet should be very minimal because of the nature of our business.

Script note: Source - 2001 Cost of Downtime Survey Results, 2001.

[if selection ≠ B]

Sorry, your choice is incorrect. The average is around 3-4 days. About 10% of organisations are in serious trouble if their systems are down for just 3-4 hours. A major systems failure can put an organisation out of business in a very short amount of time. However, the loss for SP AusNet should be very minimal because of the nature of our business.

Script note: Source - 2001 Cost of Downtime Survey Results, 2001.

Question 5

What is the average cost of a single information security breach for a large organisation?

A) $5,000

B) $80,000

C) $150,000

D) $350,000

[if answer = A or B]

Sorry, your choice is a little low. The average cost is a little over $150,000. But this is only an average – the costs can be much higher. A breach can not only have a high financial cost, it can impact on an organisation's reputation too.

Script note: Source - The CSI/FBI 2006 Computer Crime and Security Survey

[if answer = C]

Yes, you're correct. The average cost is a little over $150,000. But this is only an average – the costs can be much higher. A breach can not only have a high financial cost, it can impact on an organisation's reputation too.

Script note: Source - The CSI/FBI 2006 Computer Crime and Security Survey

[if answer = D]

Your choice is a little high; the average cost is a little over $150,000. But this is only an average – the costs can be much higher. One of the reasons for the costs being lower than you might have expected is because of the massive increase in spending in information security measures.

Script note: Source - The CSI/FBI 2006 Computer Crime and Security Survey

MODULE 3:

How does Information Security affect me?

Entry control

Question 6

Most staff members are given an ID badge by their organisation. What is the purpose of this badge? A) To enable staff members to recognise one another, B) To provide identification for customers, C) To enable security staff to identify immediately any intruders.

A) A and B

B) B and C

C) A and C

D) A, B and C

[answer =D]

[if selection =D]

That's correct, ID badges serve all three of the purposes listed. They *do* have a very important security function, however – which means that you must wear your badge at all times, while at work.

[if selection ≠ D]

Your choice is incorrect. The correct answer was D. ID badges serve all three of the purposes listed. ID badges *do* have a very important security function – which means that you must wear your badge at all times, while at work.

Question 7

Being a permanent member of staff means that you have automatic security clearance to visit any part of your organisation's premises and operations. Is this true or false?

A) True

B) False

[answer = B]

[if selection = B]

You're correct, this statement is false. No one, not even the Chairperson or CEO has universal security clearance. There are some parts of any organisation – for example, the file server storage area, the production line, or the maintenance areas – to which access needs to be strictly controlled. There are security reasons – and in some cases personal safety reasons – for such entry controls.

[if selection = A]

Your selection is incorrect. This statement is false. No one, not even the Chairperson or CEO has universal security clearance. There are some parts of any organisation – for example, the file server storage area, the production line, or the maintenance areas – to which access needs to be strictly controlled. There are security reasons – and in some cases personal safety reasons – for such entry controls.

Question 8

Electronic 'passes' enable an organisation to specify access rights on an individual basis to each member of staff, according to the responsibilities and requirements of their job. Is this true or false?

A) True

B) False

[answer = A]

[if selection = A]

Yes, it's true. The use of this kind of entry control is good information security practice, since it minimises the traffic in 'high risk' areas of the organisation's premises.

[if selection = B]

Your choice is incorrect. It is in fact true. The use of this kind of entry control is good information security practice, since it minimises the traffic in 'high risk' areas of the organisation's premises.

Question 9

A colleague whom you know well has left her electronic pass at home. She needs to get into the file storage – which she can't do without her pass. You know she has access rights to the file storage. Is it okay to lend her *your* pass?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct, it's not okay to lend your pass to anyone, however well you know them and their access rights.

[if selection = A]

Sorry, your choice is incorrect. It's not okay to lend your pass to anyone, however well you know them and their access rights.

Question 10

You're returning to work from your lunch break, and have opened the door using your electronic pass. As the door is swinging shut behind you, you see that someone else is rushing towards it, trying to get in before it closes again. Is it OK to hold the door open for them?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct. Holding secure doors open for people you don't know can result in unauthorised entry to the premises – this is called 'piggybacking'.

[if selection = A]

Sorry, your choice is incorrect. Holding secure doors open for people you don't know can result in unauthorised entry to the premises – this is called 'piggybacking'.

Clear desk and secure disposal policies

Question 11

In which one of the following places would you keep a filing cabinet key?

A) In your desk drawer

B) In a lockable key cabinet

C) In a safe

D) With your department manager

[answer = B]

[if selection = B]

Yes. The filing cabinet should be kept locked when not in use and the key kept securely, but readily available, in a lockable key cabinet.

[if selection ≠ B]

Your selection is incorrect. The filing cabinet should be kept locked when not in use and the key kept securely but readily available, in a lockable key cabinet. B is the correct answer.

Question 12

Which of the following are good reasons for having a clear desk policy? A) It helps to ensure that sensitive information and materials are never left unattended, B) If information is put away at the

end of each day, it's much easier to find it again next time, C) Excess paper waste could become a fire hazard.

A) A only

B) B only

C) A and B only

D) A, B and C

[answer = D]

[if answer = D]

That's correct. All of these are very good reasons for having a clear desk policy.

[if answer ≠ D]

Your choice is incorrect. All three of the reasons given are good reasons for having a clear desk policy. D is the correct answer.

Question 13

How should paper-based information, classified as Confidential, be stored?

A) You shouldn't keep Confidential information in a paper-based form. All Confidential information should be stored on a computer system, so controls such as passwords can be used to restrict access to it

B) It should be kept in locked storage units or restricted access storage areas

C) Provided you don't take it off-site, there's no problem about where you store it on-site

[answer = B]

[if selection = A]

Your selection is incorrect. You can't keep all your Confidential information on your computer system. Paper-based copies often exist, even when there are electronic versions. You should keep any Confidential paper-based information in locked storage units or restricted access storage areas.

[if selection = B]

Yes, that's correct. You certainly shouldn't leave documents containing Confidential information lying around unsecured.

[if selection = C]

Your selection is incorrect. It matters very much where you keep Confidential information. You should keep any paper-based information classified as Confidential in locked storage units or restricted access storage areas.

Question 14

It obviously makes sense from a security point of view, to 'lock' your computer terminal whenever you are going to be away from your desk for a meeting. Is locking your terminal also necessary when all you want to do is go to the coffee machine for two minutes?

A) Yes – I should lock my terminal whenever I am away from my desk

B) No – provided the terminal is within my view

C) No – two minutes isn't really long enough for a serious security breach to take place

[answer = A]

[if selection = A]

Yes, you're correct. You should never leave an unattended terminal open – even if it's only for a couple of minutes.

[if selection = B]

Your selection is incorrect. You should never leave an unattended terminal open – even if it's within your view.

[if selection = C]

Your selection is incorrect. You should never leave an unattended terminal open – even if it's only for a couple of minutes.

Question 15

The primary purpose of a 'clear desk policy' is to minimise the risks to information security in the workplace. Is this true or false?

A) True

B) False

[answer = A]

[if selection = A]

You're correct, it's true. And a clear desk policy also has the added benefit of minimising fire hazards, by ensuring that 'combustible' items such as paper are properly stored and/or disposed of.

[if selection = B]

Your choice is incorrect. This is actually true. And a clear desk policy also has the added benefit of minimising fire hazards, by ensuring that 'combustible' items such as paper are properly stored and/or disposed of.

Question 16

All paper documents for which you no longer have a use can be disposed of in the waste paper bin. Is this correct?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct, this isn't correct at all! Paper documents containing any sort of restricted information should be destroyed, for example by shredding, or disposed of in locked recycle bins.

[if selection = A]

Sorry, your choice is incorrect. Paper documents containing any sort of restricted information should be destroyed, for example by shredding, or disposed of in locked recycle bins.

Question 17

Which of the following precautions are advisable, before disposing of old computer equipment? A) Make backups of files from the hard disk, B) Wipe files from the hard disk, C) Wipe software from the hard disk, D) Remove the hard disk and destroy it.

A) A only

B) A and B only

C) A, B and C

D) A, B, C and D

[answer = C]

[if selection = C]

Yes. Your own files might contain information that needs to be kept confidential, so these should certainly be removed from the computer's hard drive – after they have been backed up, of course! Any software should also be wiped to prevent unauthorised copies from entering into circulation.

[if selection = A]

Your selection is incorrect. Files should be backed up, but they may contain confidential or sensitive information that needs to then be wiped from the computer's hard drive. Any software should also be wiped to prevent unauthorised copies from entering into circulation.

[if selection = B]

Your selection is incorrect. Some of these files could contain confidential or sensitive information, so it's important to remove them before the computer is disposed of. Any software must also be wiped to prevent unauthorised copies from entering into circulation.

[if selection = D]

Your selection is incorrect. All of these precautions are necessary, except for removing or destroying the hard disk! Most computers are 'reconditioned' and sold again. We don't want to destroy the computer – but we *do* need to wipe its hard drive of any data or software specific to our organisation!

Password management

Question 18

How many people need to know your password?

A) I need to know it, and my manager needs to know it – for when I'm out of the office

B) Only I should know my password

C) It doesn't matter who knows it

[answer = B]

[if selection = B]

Yes, that's correct. Giving your password to other people constitutes a threat to information security and is not good information security practice. You are the only person who needs to know your password.

[if selection ≠ B]

Your selection is incorrect. The only person who needs to know your password is *you*. You should keep your password secret. Giving your password to other people constitutes a threat to information security and is not good information security practice.

Question 19

How often should you change your password?

A) It doesn't really matter – a couple of times a year, perhaps

B) You should never change it – if you keep changing passwords you are likely to forget them

C) Regularly - at least once every 90 days

[answer = C]

[if selection = C]

Yes, that's correct. Changing your password about once every 4 to 6 weeks is best (and never leave it longer than 90 days). These regular changes reduce the risks of someone else obtaining your password and having an opportunity to use it.

[if selection ≠ C]

Your choice is incorrect. You could run into serious problems if that's your approach to passwords! You should change your password about once every 4 to 6 weeks (and never leave it longer than 90 days). These regular changes reduce the risks of someone else obtaining your password and having an opportunity to use it.

Question 20

The best way to remember your password is to write it down and stick it under your keyboard. True or false?

A) True

B) False

[answer = B]

[if selection =B]

You're correct. This would be very risky. Passwords should, ideally, be committed to memory. They should certainly never be left written down in a place that is accessible to other people.

[if selection = A]

Your selection is incorrect. This would be very risky. Passwords should, ideally, be committed to memory. They should certainly never be left written down in a place that is accessible to other people.

Question 21

Passwords should, ideally, use a mix of numbers, special characters, upper and lower case letters and be at least eight characters in length. Do you agree with this advice?

A) Yes

B) No

[answer = A]

[if selection = A]

You're correct, this is good information security advice. The idea is to make the password something that others won't easily 'guess'. It's also important to avoid using obvious words, dates or numbers, especially those that have personal associations such as birthdays or family names.

[if selection = B]

Your selection is incorrect. Following this advice will help to make the password something that others won't easily 'guess'. It's also important to avoid using obvious words, dates or numbers, especially those with personal associations such as birthdays or family names.

Question 22

Ann failed to follow her organisation's rules on password security and her password fell into the wrong hands. Unknown to her, an unauthorised person used Ann's password to access confidential files. Some of this confidential information has since been leaked to people outside the organisation. Who is most likely to be held responsible for the leak?

A) Both Ann and the person who used her password

B) Only the person who used Ann's password

C) Ann – and only Ann

[answer = A]

[if selection = A]

That's correct. Both Ann and the person who used her password can be held accountable for this leak. Your password is linked to your User ID, so access can be traced back to you. The best protection against this kind of incident is to make sure that you never give your password to anyone.

[if selection ≠ A]

Your choice is incorrect. Both Ann and the person who used her password can be held accountable for this leak. Your password is linked to your User ID, so access can be traced back to you. The best protection against this kind of incident is to make sure that you never give your password to anyone.

Question 23

Which of the following passwords conforms to the best practice rules for creating a password?

A) HACKER

B) paul@organisationname

C) Hi9h&abm

D) GH0973

[answer = C]

[If selection = A]
This is a really bad password – it breaks all the rules. It is less than 8 characters, it is a word straight from the dictionary, and it uses all upper case letters. A good password should be at least

8 characters long, include a mix of upper and lower case letters, numbers and special characters. A much better password would be Hi9h&abm.

[If selection = B]
You should never include your own or your organisation's name in your password. A good password should be at least 8 characters long, include a mix of upper and lower case letters, numbers and special characters. A much better password would be Hi9h&abm.

[If selection = C]
Yes this password meets all the rules. It is more than 8 characters long, it includes a mix of upper and lower case letters, and it contains a number and a special character.

[If selection = D]
This is not a good password – especially if the user was Gerald Hopper, born in September 1973! You should never include your own name, initials and date of birth in your password. A good password should be at least 8 characters long, it should not be a word straight from the dictionary, it should include a mix of upper and lower case letters, numbers and special characters. A much better password would be Hi9h&abm.

Source note: The password is from a pass-phrase – a quotation (Happiness is good health and a bad memory – Ingrid Bergman), which is then amended to include a number and special character

Classifying information

Question 24

Confidential information is:

A) Highly restricted information with a very limited circulation that, if inappropriately disclosed, could severely damage SP AusNet's business interests

B) Restricted information that, if inappropriately disclosed, could expose SP AusNet to risk

C) Information that has been authorised for release into the public domain

[answer = A]

[if selection = A]

That's correct. Confidential information is highly restricted information with a very limited circulation that, if inappropriately disclosed, could severely damage SP AusNet's business interests.

[if selection ≠ B]

Sorry, your choice is incorrect. Confidential information is highly restricted information with a very limited circulation that, if inappropriately disclosed, could severely damage SP AusNet's business interests.

Question 25

You have to leave your office for a few minutes and you have been working on a Confidential document. Should you:

A) Turn the papers face down on your desk and close the office door

B) Put the papers in lockable storage and take the key with you

C) Not take any special precautions; you will only be gone for moments and you trust all of your colleagues

[answer = B]

[if selection = B]

You're correct. This is highly restricted information that, if inappropriately disclosed, could severely damage SP AusNet's business interests and professional reputation, seriously undermine customer confidence, or help the competition. Confidential documents should always be locked away – even if you are leaving them unattended for a few minutes only.

[if selection ≠ B]

Sorry, your selection is incorrect. This is highly restricted information that, if inappropriately disclosed, could severely damage SP AusNet's business interests and professional reputation, seriously undermine customer confidence, or help the competition. Confidential documents should always be locked away – even if you are leaving them unattended for a few minutes only.

Question 26

You have been working on a Confidential document that needs to be sent to several colleagues. E-mail is the safest method for sending the document.

A) True

B) False

[answer = B]

[if selection = B]

That's correct. E-mails can get 'lost' and can be intercepted and, unless the recipient knows in advance to expect the e-mail, they won't know that it has gone missing. However, you can protect your e-mails from being read by unauthorised users by encrypting them.

[if selection = A]

Sorry, that is incorrect. E-mails can get 'lost' and can be intercepted and unless the recipient knows in advance to expect the e-mail, they won't know that it has gone missing. However, you can protect your e-mails from being read by unauthorised users by encrypting them.

Systems integrity

Question 27

The network administrator often backs up information on shared drives automatically. But who is responsible for backing up the files stored on your local PC hard disk?

A) My manager

B) The network administrator

C) Me

[answer = C]

[if selection = C]

That's correct. Automated backups will cover any files on the networked or shared drives, but not the files on your own PC hard disk. It's your responsibility to make sure that regular backups are made of these.

[if selection ≠ C]

Your selection is incorrect. You're the one responsible. Automated backups will cover any files on the networked or shared drives, but not the files on your own PC hard disk. It's your responsibility to make sure that regular backups are made of these.

Question 28

You have just acquired a new piece of software, and you want to try it out. You install it onto your local PC. Is this likely to have any damaging consequences?

A) Yes

B) No

[answer = A]

[if selection = A]

Yes, you have to assume that *any* change or installation, however small, will have an impact on the overall system and could actually interfere with how some parts of the system operate. You must never install software or hardware unless you are qualified and authorised to do so.

[if selection = B]

Sorry, your selection is incorrect. You should assume that *any* change or installation, however small, will have an impact on the overall system and could actually interfere with how some parts of the system operate. You must never install software or hardware unless you are qualified and authorised to do so.

Question 29

Jack regularly uses a laptop at work. To take advantage of the laptop's wireless capability he's planning to add a wireless router to a network connection in his office. Is this acceptable?

A) Yes

B) No

[answer = B]

[if selection = B]

That's right - this isn't acceptable. By installing an unauthorised wireless router, Jack could leave the network vulnerable to unauthorised access. Systems are designed and connected very carefully to make sure that services and information are continuously maintained and protected. You should never tamper with, disconnect or make any unauthorised changes to any device on the network, however minor they might be.

[if selection = A]

Your selection is incorrect. By installing an unauthorised wireless router, Jack could leave the network vulnerable to unauthorised access. Systems are designed and connected very carefully to make sure that services and information are continuously maintained and protected. You should never tamper with, disconnect or make any unauthorised changes to any device on the network, however minor they might be.

Question 30

Crisis! Something has gone wrong and a number of important files have been corrupted so they cannot be opened. Which particular information security procedure is designed to cope with this kind of problem?

A) Password controls

B) Backup routines

C) Installation procedures

[answer = B]

[if selection = B]

That's correct. Backup routines are designed to ensure that regular backup copies are made of important data. These backups can be used to retrieve any data that is lost or corrupted.

[if selection ≠ B]

Your choice is incorrect. The correct answer is backup routines. Backup routines are designed to ensure that regular backup copies are made of important data. These backups can be used to retrieve any data that is lost or corrupted.

Question 31

You should make backups of *all* your computer data, every day, without fail. True or false?

A) True

B) False

[answer = B]

[if selection = A]

That's incorrect. The frequency with which you should make backups depends on the complexity of the data, its criticality and the degree and frequency of any changes made to it. While some data will need to be backed up every day, e.g., customer databases, invoicing information, and so on, other data can be backed up less frequently.

[if selection = B]

You're correct. While some data does need to be backed up every day, other data can be backed up less frequently. The frequency with which you do it depends on the complexity of the data, its criticality and the degree and frequency of any changes made to it.

Question 32

It is important, as part of your information security practice, that you use only authorised software. So what *is* 'authorised' software? Choose from the definitions below and click on the one that you think is correct.

A) Authorised software is any kind of licensed software, produced and distributed by a reputable software vendor

B) Authorised software is any software that has been formally evaluated, tested and installed by our organisation

[answer = B]

[if selection = B]

Yes, you have chosen the correct definition. SP AusNet has certain procedures in place for ensuring that all software is formally evaluated before installation. It is important that you follow these procedures.

[if selection ≠ B]

Your choice isn't correct. If you install your own licensed software without passing it through the proper channels for evaluation and testing, then you may run into compatibility problems. For software to be authorised, it must first go through a formal authorisation procedure.

Question 33

Which of the following dangers could result from the use of unauthorised software or unauthorised copies of software? A) It may be illegal, B) It may be carrying malware, C) It could clash with other systems or software.

A) A, B and C only

B) A only

C) A and B only

[answer = A]

[if answer = A]

That's correct. All of these options are dangers that could result from the use of unauthorised software.

[if answer ≠ A]

Your selection is incorrect. A is the correct answer. All of these options are dangers resulting from the use of unauthorised software.

Question 34

Which of the following dangers could result from the use of unapproved hardware and connections? A) It could cause your existing hardware or software to fail, B) It could invalidate warranties on your equipment, C) It could undermine your system's security controls by exploiting internal or external routes into the system.

A) A

B) A and B

C) B and C

D) All of the above

[answer = D]

[if answer = D]

That's correct. These are all potential dangers from the use of unapproved hardware and connections. From the security point of view, therefore, it is important that you follow SP AusNet's approved procedures for evaluating, installing and maintaining new hardware.

[if answer ≠ D]

Your choice is incorrect. In fact, these are all potential dangers from the use of unapproved hardware and connections. From the security point of view, therefore, it is important that you follow SP AusNet's approved procedures for evaluating, installing and maintaining new hardware.

Malware

Question 35

Which of the following might indicate that you had a virus in your system?

A) Problems with your printer

B) Very slow processing speed

C) Strange things happening to the data on your screen

D) Documents saving without being prompted

E) Documents spontaneously changing their names

F) All of the above

[answer = F]

[if selection = F]

Yes you're correct, a virus could cause all or any of the symptoms listed.

[if selection ≠ F]

Your selection is incorrect. A virus could cause all or any of the symptoms listed. The answer you should have chosen was F.

Question 36

Virus scanning software has an unlimited life span. Once you install it, you never need worry about viruses again. Is this true or false?

A) True

B) False

[answer = B]

[if selection = B]

You're correct. New viruses are constantly finding their way into computer systems. Virus scanning software can only search for *known* viruses, which means that it has a *limited* life span. Organisations need to update their virus scanning software regularly.

[if selection = A]

Sorry, your choice is incorrect. New viruses are constantly finding their way into computer systems. Virus scanning software can only search for *known* viruses, which means that it has a *limited* life span. Organisations need to update their virus scanning software regularly.

Question 37

Everyone knows that you should virus check incoming data. But should you also virus check outgoing data?

A) Yes

B) No

[answer = A]

[if selection = A]

You're correct, it's good practice – and responsible – to virus check outgoing as well as incoming data. The reason? Well, it helps to ensure that *you* are not responsible for passing on a virus to someone else's system. Even if you think your own system is clean, it's worth taking this simple precaution. It could be quite damaging to the reputation of *any* organisation to be blamed for passing on a computer virus.

[if selection = B]

Sorry, your selection is incorrect. It's good practice – and responsible – to virus check outgoing as well as incoming data. The reason? Well, it helps to ensure that *you* are not responsible for passing on a virus to someone else's system. Even if you think your own system is clean, it's

worth taking this simple precaution. It could be quite damaging to the reputation of *any* organisation to be blamed for passing on a computer virus.

Question 38

What should you do if you suspect that a virus has 'slipped through' and infected your system?

A) Just accept it – there's nothing you can do about it

B) Continue working, keeping a log of any 'telltale' problems that you encounter

C) Try to track the virus down and fix it

D) Stop using the system and report your suspicions immediately

[answer = D]

[if selection = D]

Yes, that's exactly what you should do. It's particularly important that you do not delay, or try to fix the virus yourself. Always leave virus fixing to the proper, qualified personnel.

[if selection = A]

Your selection is incorrect. You must do something about it! Don't delay, and don't try to fix the problem yourself. Stop using the system (to minimise any virus damage) and report your suspicions immediately to the proper, qualified personnel.

[if selection = B]

Your selection is incorrect. This just gives the virus a chance to spread and do damage – this is exactly what you must not do! To minimise the potential damage you should stop using the system and report your suspicions immediately to the proper, qualified personnel.

[if selection = C]

Your selection is incorrect. Trying to fix the virus yourself may only make matters worse – and also wastes valuable time. Don't delay – report your suspicions immediately to the proper, qualified personnel.

Question 39

You work mostly on a laptop computer, at home or out and about. This isn't connected to your organisation's network. The chances that you could infect the network with a virus are therefore virtually none. Is this true?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct, this isn't true at all. If you use e-mail, or the Internet, or removable drives (a USB stick) and CDs, and if you send data from any of these sources to the network, then there's a significant risk that you could be transmitting viruses along with the data. You must never be complacent about viruses or the risk of infection spreading remotely, via e-mail and other means.

[if selection = A]

Sorry, your choice is incorrect. If you use e-mail, or the Internet, or removable drives (a USB stick) and CDs, and if you send data from any of these sources to the network, then there's a significant

risk that you could be transmitting viruses along with the data. You must never be complacent about viruses or the risk of infection spreading remotely, via e-mail and other means.

Question 40

Which of the following is a good definition of 'malware'?

A) Any form of malicious and unwanted program on your information system

B) A program illegally installed to corrupt your system

C) A software agent that polices your information system

D) Offensive spam

[answer = A]

[if selection = A]

Yes, malware is a generic name for any form of malicious and unwanted program on your information system. Malware includes, but is not limited to, computer viruses, Trojan horses, adware, spyware and spam.

[if selection ≠ A]

That's incorrect. Malware is a generic name for any form of malicious and unwanted program on your information system. Malware includes, but is not limited to, computer viruses, Trojan horses, adware, spyware and spam.

Question 41

This example of malware is a computer program that secretly gathers information from your computer. It can log the Internet sites you visit and monitor your keystrokes enabling it to discover your passwords and other personal details.

What form of malware is being described?

A) A virus

B) A Trojan Horse

C) A bot

D) Spyware

[answer = D]

[if selection = D]

Yes, spyware secretly gathers information from your computer. The spyware then forwards this information to someone else without your authorisation or knowledge. The recipient may then be able to access your computer, use your applications, copy your files and even wipe your hard drive clean and use your personal details for fraud.

[If selection ≠ D]
That's incorrect. It is spyware that secretly gathers information from your computer. The spyware then forwards this information to someone else without your authorisation or knowledge. The recipient may then be able to access your computer, use your applications, copy your files and even wipe your hard drive clean and use your personal details for fraud.

Question 42

What is the primary aim of those who create and distribute malware?

A) To amuse the recipients

B) To generate profit for themselves

C) To slow down the organisation's computers but do no real harm

D) To corrupt data and cause financial loss to the organisations affected

[answer = B]

[if selection = A]

No, this rarely their primary aim. Although some malware is designed to cause data loss, most of the malicious software distributed nowadays has been designed to generate profits for its authors.

[if selection = B]

Yes, although some malware is designed to cause data loss, most of the malicious software distributed nowadays has been designed to generate profits for its authors.

[if selection = C or D]

This is rarely their primary aim. Although some malware is designed to slow down or deny a service to its users and other examples to cause data loss, most of the malicious software distributed nowadays has been designed to generate profits for its authors.

Question 43

All bots are software agents with malicious intent, created by criminals. Is this true or false?

A) True

B) False

[answer = B]

[if selection = B]

That's correct. Not all bots are malicious or unwanted. For example, certain bots have been developed to lurk in the background of electronic communication channels (IMS and chat rooms) to spot and act on certain phrases – either to offer help (for example to new users) or to offer mild censorship when required. Other legitimate and useful applications of bots include automatic data testing, and web automation.

[if selection = A]

That's incorrect. Not all bots are malicious or unwanted. For example, certain bots have been developed to lurk in the background of electronic communication channels (IMS and chat rooms) to spot and act on certain phrases – either to offer help (for example to new users) or to offer mild censorship when required. Other legitimate and useful applications of bots include automatic data testing, and web automation.

Electronic communication

Question 44

Read through the statements below about e-mail. Which is the true one?

A) E-mail is a very secure medium for transmitting messages

B) The only person who has access to my personal e-mailbox is me

C) E-mails can carry computer viruses

[answer = C]

[if selection = C]

Well done, you chose the correct answer. The other two statements about e-mail are completely false.

[if selection ≠ C]

Your selection is incorrect. E-mail is not a secure medium – external e-mail certainly isn't. On the other hand, e-mail *can* carry computer viruses. The answer you should have chosen is C.

Question 45

Is the following a good or bad example of how e-mail should be used: ''This is to remind everyone that there will be a sale of ladies and gentlemen's watches in the staff room at lunch time.''

A) Good

B) Bad

[answer = B]

[if selection ≠ B]
Your selection is incorrect. SP AusNet's e-mail facility should be used for business purposes only. You should reserve e-mail for important, meaningful messages, rather than for casual communications of the kind shown here.

[if selection = B]

You're correct. SP AusNet's e-mail facility should be used for business purposes only. You should reserve e-mail for important, meaningful messages, rather than for casual communications of the kind shown here.

Question 46

E-mail is one of the safest ways to send messages that require confidentiality. Is this true or false?

A) True

B) False

[answer = B]

[if selection = B]

You're correct. E-mail is not totally confidential, whatever people may think. External e-mail in particular is prone to risk, because once the information has been transmitted beyond the security parameters of our organisation, there is little our organisation can do to protect it. To enhance security, many organisations encrypt documents before they are e-mailed, particularly if they are being sent externally.

[if selection = A]

Sorry, your choice is incorrect. E-mail is not as confidential as you may think. External e-mail in particular is prone to risk, because once the information has been transmitted beyond the security parameters of our organisation, there is little our organisation can do to protect it. To enhance security, many organisations encrypt documents before they are e-mailed, particularly if they are being sent externally.

Question 47

Access to your e-mailbox is password-protected. Provided you have been careful with your password, the only person who can access your e-mailbox will be you. Is this correct?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct, this isn't true. In most cases, your e-mail administrator can access your e-mail. In addition, skilled hackers can get into most e-mailboxes if they put their mind to it. Don't assume e-mail systems are 100% secure; they can be breached.

[if selection = A]

The statements weren't correct. In most cases, your e-mail administrator can access your e-mail. In addition, skilled hackers can get into most e-mailboxes if they put their mind to it. Don't assume e-mail systems are 100% secure; they can be breached.

Question 48

You work for an organisation that uses PKI for its e-mail encryption. You want to send an encrypted e-mail to your colleague Noel.

What do you need in order to do this?

A) Noel's private key

B) Noel's public key

C) Your private key

[answer = B]

[if selection = B]

That's correct. You would encrypt it using Noel's public key, safe in the knowledge that only Noel, by using his private key, can decrypt it.

[if selection ≠ B]

That's incorrect. You would encrypt it using Noel's public key and only Noel will be able to decrypt it, using his private key.

Question 49

Your organisation uses PKI for its e-mail encryption. What is the purpose of your private key?

A) To encrypt and decrypt e-mails

B) To decrypt and digitally sign e-mails

C) To encrypt and digitally sign e-mails

D) To encrypt, decrypt and digitally sign e-mails

[answer = B]

[if selection = B]

That's not correct. A private key is used for decrypting e-mails and can also be used to digitally sign e-mails.

[if selection ≠ B]

That's correct. A private key is used for decrypting e-mails and can also be used to digitally sign e-mails.

Question 50

Unlike e-mails, messages sent via IMS generally have no legal status, so are not admissible in court – nor do they count as evidence of business agreements. True or False?

A) True

B) False

[answer = B]

[if selection = B]

You're correct. You can libel someone using IMS just as easily as you can with e-mail. And if messages are evidence of a business agreement, you must save copies.

[if selection = A]

Your selection is incorrect. You can libel someone using IMS just as easily as you can with e-mail. And if messages are evidence of a business agreement, you must save copies.

Question 51

You are about to fax a Confidential report. What key precaution should you take before starting your transmission?

A) Put a Confidential cover page at the front of the document

B) Phone the recipient to make sure they will be standing by to retrieve the document as it comes through the fax

C) Leave a message on the recipient's answering machine, explaining why you are faxing the document and roughly what it contains

[answer = b]

[if selection = b]

Yes, that's correct. If you're faxing Confidential information it's important first to make sure that the person you are sending it to is there to receive it at the other end. Do not fax Confidential information to an unsecured or unattended fax machine.

[if selection = a]

Your selection is incorrect. This won't prevent 'unauthorised' people from reading the document as it comes through the fax! You need to make sure that the person receiving the fax at the other end is the person for whom the fax is intended. Do not fax Confidential information to an unsecured or unattended fax machine.

[if selection = c]

Your selection is incorrect. Firstly, you should not leave Confidential information on answering machines. Secondly, you should not send Confidential information to an unsecured or unattended fax machine. You should phone to make sure that the person you are sending the fax to is there to receive it.

Question 52

Answering machine messages can be accessed by anyone who plays the messages back. The information security implications are that you should not give confidential or sensitive information, when leaving messages on an answering machine. Should you apply this same rule to voicemail messages?

A) Yes

B) No

[answer = A]

[if selection = A]

You're correct. Voicemail systems *are* more secure than answering machines. But they're still not foolproof – especially if the recipient has been careless enough to give their voicemail pass code to another person. You should think very carefully about any messages you leave on both answering machines *and* voicemail.

[if selection = B]

Your choice is incorrect. Voicemail systems *are* more secure than answering machines. But they're still not foolproof – especially if the recipient has been careless enough to give their voicemail pass code to another person. You should think very carefully about any messages you leave on both answering machines *and* voicemail.

Question 53

You should always confirm or check the number you are sending to, before transmitting any form of confidential document via fax. Is this true or false?

A) True

B) False

[answer = A]

[if selection = A]

Yes, of course you should! You may have taken the fax number down incorrectly, or you may have keyed it in incorrectly. Phoning to confirm the number and checking on the fax machine that you have entered the correct number before you start transmitting are both very sensible security precautions.

[if selection = B]

Your choice is incorrect. Of course you should check the number! You may have taken the fax number down incorrectly, or you may have keyed it in incorrectly. Phoning to confirm the number and checking on the fax machine that you have entered the correct number before you start transmitting are both very sensible security precautions.

Question 54

Jim is hiring a third party to act as a consultant on an IT project he is managing. Does he need to ask the consultant to sign a Non-Disclosure Agreement before starting work on the project?

A) Yes

B) No

[answer = A]

[if selection = A]

You're correct. Third parties must always sign NDAs to agree to treat your information as carefully as they would their own confidential information. And without an NDA, our organisation may have no legal means of redress against them if they misuse confidential information.

[if selection = B]

Your choice is incorrect. Third parties must always sign NDAs to agree to treat your information as carefully as they would their own confidential information. And without an NDA, our organisation may have no legal means of redress against them if they misuse confidential information.

Question 55

Which of the following could be reasons why a criminal might target IP Telephony systems?

A) Financial benefit

B) Identity theft

C) Information theft

D) All of the above

[answer = D]

[if selection = D]

Yes, all of these are reasons why criminals target IP Telephony systems. Calls are sent as 'digital packets of information' to the other party so they can be intercepted and modified and sent on to the recipient; an attacker could connect a rogue IPT phone to a network and, using a stolen user account and password, place calls at the organisation's expense. For all these reasons it is important that you keep your account log on and password details confidential and follow our procedures carefully.

[if selection ≠ D]

This is one explanation, but in fact all of these are reasons why criminals target IP Telephony systems. Calls are sent as 'digital packets of information' to the other party so they can be intercepted and modified and sent on to the recipient; an attacker could connect a rogue IPT phone to a network and, using a stolen user account and password, place calls at the organisation's expense. For all these reasons it is important that you keep your account log on and password details confidential and follow our procedures carefully.

Internet security and acceptable use

Question 56

As a representative of SP AusNet, you have automatic authorisation to put information onto our website. Is this true or false?

A) True

B) False

[answer = B]

[if selection = B]

Correct. Information put onto SP AusNet's website is in the public domain. It is part of the public face that our organisation presents to the world outside it. You should never put any information onto our website unless you are clearly authorised to do so.

[if selection = A]

Sorry, your choice is incorrect. Information put onto SP AusNet's website is in the public domain. It is part of the public face that our organisation presents to the world outside it. You should never put any information onto our website unless you are clearly authorised to do so.

Question 57

You can assume a code name when chatting on-line. This enables you to post information to chat rooms and bulletin boards anonymously, i.e. without anyone being able to identify who you are, or from which organisation. Is this a true statement?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct, this isn't true at all. You're not as anonymous as you think when you visit a chat room or bulletin board. Your e-mail address may be logged by the forum's administrator and could be intercepted by others and passed on for mailing purposes, which can lead to unsolicited and nuisance e-mails, so beware! There's also the potential issue of people's 'personal' opinions being misinterpreted as 'corporate' opinions, if they visit chat rooms during working hours.

[if selection = A]

Your selection is incorrect. This isn't true at all. You're not as anonymous as you think when you visit a chat room or bulletin board. Your e-mail address may be logged by the forum's administrator and could be intercepted by others and passed on for mailing purposes, which can lead to unsolicited and nuisance e-mails, so beware! There's also the potential issue of people's 'personal' opinions being misinterpreted as 'corporate' opinions, if they visit chat rooms during working hours.

Question 58

You like to 'surf' the Internet, and you enjoy a good on-line 'chat' once the official working day is over. There's nothing wrong with this at all. But does it matter where you 'chat' and 'surf' from, i.e. does it make a difference whether you use the organisation's Internet facilities, or your own Internet facilities at home? (Remember – this is 'after hours', so it's not as if you're doing your 'surfing' on the organisation's time!)

A) Yes

B) No

[answer = A]

[if selection = A]

You're correct, it *does* matter. Okay, so it's after hours, you're not doing it on the organisation's time. But you should not be doing it on the organisation's systems either! Casual Internet use exposes the organisation's system to unnecessary risk from hackers and viruses. You should only use the Internet in accordance with our Acceptable Use Policy.

[if selection = B]

Sorry, your choice is incorrect. Okay, so it's after hours, you're not doing it on the organisation's time. But you should not be doing it on the organisation's systems either! Casual Internet use exposes the organisation's system to unnecessary risk from hackers and viruses. You should only use the Internet in accordance with our Acceptable Use Policy.

Question 59

When you're using the Internet, files only download onto your system when you have specifically requested it – for example, when buying a piece of software on-line. Is this true or false?

A) True

B) False

[answer = B]

[if selection = B]

You're correct, this statement is false. Whenever you access a website, the reason you can see the site is because it has downloaded onto *your* system. In other words, files are downloaded from the Internet every time you visit a new website page. This is a feature of the Internet that cannot be avoided – and means that your system is potentially exposed to viruses, every time you browse a website.

[if selection = A]

Your selection is incorrect. This statement is false. Whenever you access a website, the reason you can see the site is because it has downloaded on to *your* system. In other words, files are downloaded from the Internet every time you visit a new website page. This is a feature of the Internet that cannot be avoided – and means that your system is potentially exposed to viruses, every time you browse a website.

Security out of the office

Question 60

If you were visiting a customer's premises, and they operated an excellent security system, would it be safe to leave your PC or briefcase containing customer information in one of their offices while you went to lunch?

A) Yes, as long as the office is secured

B) No, you must never leave your PC or briefcase unattended

[answer = B]

[if selection = B]

That's correct.

[if selection ≠ B]

Your choice is incorrect. The correct answer is B.

Question 61

Which of the following precautions would help to prevent loss or theft of portable equipment when you are out of the office? A) Never leaving equipment unattended in a public place, B) Never

leaving it in view, e.g. in the back seat of your car, C) Never carrying equipment around with you unless you need to use it, D) Always checking that you have all your equipment with you.

A) A, B and C only

B) A, B and D only

C) All of the above

D) None of the above

[if answer = C]

That's correct. These are all sensible precautions to take.

[if answer ≠ C]

Your selection is incorrect. In fact these are all sensible precautions to take.

Question 62

Lots of organisations these days have a stock of laptop computers that they can 'lend out' to staff, as required. Whose responsibility is it to keep up-to-date backups of any files or documents generated on these laptops?

A) The IT-Service Desk

B) The staff member using the laptop

[answer = B]

[if selection = B]

You're correct. It's the responsibility of the staff member who generated the documents in the first place! It's their responsibility also to make sure that the laptop is kept safe, and that neither it nor any of the information it contains are exposed to unnecessary risk while in their care.

[if selection ≠ B]

Your choice is incorrect. Keeping the laptop in good working order is the responsibility of the IT-Service Desk. But each staff member using the laptop should make sure that they backup any important documents, and that the laptop is kept safe, and not exposed to unnecessary risk.

Question 63

What is a 'leaky network'?

A) A computer network from which files frequently 'leak' through accidental deletions

B) A wireless network that leaves you vulnerable to attack

C) A wireless network that does not support standard e-mail protocols – and from which e-mails regularly 'leak out'

[answer = B]

[if selection = B]

That's right. You are particularly vulnerable if you use a 'leaky' wireless network – one that does not prevent other users from attempting to access your device.

[if selection = C]

Your choice is incorrect. You are particularly vulnerable if you use a 'leaky' wireless network – one that does not prevent other users from attempting to access your device.

[if selection = A]

Your choice is incorrect. You are particularly vulnerable if you use a 'leaky' wireless network – one that does not prevent other users from attempting to access your device.

Question 64

On your way back to the office after a meeting you called in to a café for lunch and your laptop was stolen. What is the greatest loss arising from the theft?

A) The cost of the laptop – it was a brand new 'state-of-the-art' model

B) The loss of the notes from your meeting

C) The chance the someone could find out your User ID and password

D) The loss of the organisation's data on the hard drive

[answer = D]

[if selection = A]

This is of course serious, but the loss of the organisation's data on your computer poses a far greater risk to the organisation. A criminal may be able to extract your User ID and password and so gain access to the organisation's main information system, and depending on your job, you may have all kinds of Sensitive, Private and Confidential information stored on the laptop. Its release could impact on the organisation's finances and reputation.

[if selection = B]

This may be your initial reaction, but the loss of the organisation's data on your computer poses a far greater risk to the organisation. A criminal may be able to extract your User ID and password and so gain access to the organisation's main information system, and depending on your job, you may have all kinds of Sensitive, Private and Confidential information stored on the laptop. Its release could impact on the organisation's finances and reputation.

[if selection = C]

This certainly is a risk, but even greater than this is the potential cost of the loss of any Sensitive, Private or Confidential organisational data on your computer. Its release could impact on the organisation's finances and reputation.

[if selection = D]

Yes, this is the biggest potential loss for the organisation. Depending on your job, you may have had all kinds of Sensitive, Private and Confidential organisational data stored on the laptop and its release could impact on the organisation's finances and reputation.

Social engineering

Question 65

Which of the following definitions describes social engineering?

A) The process of getting sensitive information, for example passwords and access rights, from employees inside an organisation using techniques such as manipulation and/or intimidation

B) The method of passing on sensitive organisational information to corrupt sources for monetary gain

C) A system to protect your organisation from outside security threats by controlling the use of passwords and e-mail

[answer = A]

[if selection = A]

Well done – this correctly defines the process of social engineering.

[if selection ≠ A]

Your choice is incorrect. Social engineering is the process of getting sensitive information, for example passwords and access rights, from employees inside an organisation using techniques such as manipulation and/or intimidation.

Question 66

Which of the following is an example of human-based social engineering?

A) A bogus pop-up window appears on your computer screen asking you to supply your User ID and password

B) You receive a call from someone pretending to be from the IT-Service Desk – they ask for your User ID and password in order to check that your computer is working OK

C) You take a call from an external number – the person asks you to confirm your telephone and fax number

[answer = B]

[if selection = A]

Sorry, this option is incorrect. This is an example of computer-based social engineering. The correct answer was in fact B.

[if selection = B]

Yes – this is correct.

[if selection = C]

Sorry, this option is incorrect. There is nothing suspicious about someone asking for a telephone or fax number. The correct answer was B.

Question 67

You receive an e-mail from an unknown source with the subject line 'funny attachment – take a look' – what should you do?

A) Delete the e-mail right away without opening the e-mail or the attachment

B) Go ahead and open the e-mail and attachment, you want to see what's so funny

C) Run anti-virus software on the attachment first – if it appears to be clean then you'll go ahead and open it

[answer = a]

[if selection = A]

Yes – well done. This is always the best thing to do when you receive e-mails with attachments from an unknown source.

[if selection = C]

Sorry, this selection is incorrect. You were right to be cautious and run the anti-virus software first… but this e-mail isn't work related or important, so why waste the time? The correct thing to do would be to delete the e-mail right away.

[if selection = B]

Sorry, this selection is incorrect. This e-mail is from an unknown source and the attachment could be a virus. You should have deleted it immediately!

Question 68

You are busy working on your PC when a pop-up window appears telling you that you have lost your network connection. The message says that in order to restore the connection you must insert your User ID and password. What should you do?

A) Insert your User ID and password – you really need to get on with your work

B) You ask around the office to see if other people have received this message – they say yes and tell you that they gave their details, so you insert your User ID and password

C) You decide to call the IT-Service Desk to ask for guidance

[answer = c]

[if selection = A]

Sorry, this option is incorrect. A social engineer had illegally gained access to your office the night before and loaded this pop-up software onto a number of PCs. You have done exactly what they wanted you to do. Without realising it, you have sent your User ID and password back to the social engineer giving them access to your computer systems, putting SP AusNet at serious risk. What you should always do when receiving pop-up windows like this is check with the IT-Service Desk before inputting any information.

[if selection = B]

Sorry, this option is incorrect. You were right to be suspicious and ask questions. However, a social engineer had illegally gained access to your office the night before and loaded this pop-up software onto a number of PCs. You have done exactly what they wanted you to do. Without realising it, you have sent your User ID and password back to the social engineer giving them access to your computer systems, putting SP AusNet at serious risk. What you should always do when receiving pop-up windows like this is check with IT-Service Desk before inputting any information.

[if selection = C]

Well done – that is always the best thing to do! A social engineer had illegally gained access to your office the night before and loaded this pop-up software onto a number of PCs. They wanted you to reply because the pop-up window was set-up to send your User ID and password back to them. This would have given them access to your computer systems and put SP AusNet at

serious risk. The IT-Service Desk is now aware of this and can alert all staff, remove the software from all PCs, and minimise risk.

Question 69

Which of the following statements best describes phishing?

A) Criminals sending fake e-mails that trick you into revealing personal information like user names and passwords

B) Criminals who send mass e-mails promoting products and services you don't want

[answer = A]

[if selection = A]

That's right. This enables the fraudster to take on your on-line identity, which they can then abuse for a range of criminal purposes.

[if selection ≠ A]

Your choice is incorrect. Phishers are criminals who use e-mail to attempt to steal your on-line identity, which they can then abuse for a range of criminal purposes.

Question 70

Your organisation's on-line sales website has been affected by a scam in which visitors to the site are automatically redirected to a fake website where their orders are not placed and their money is stolen.

This type of attack is known as:

A) Trawling

B) Spawning

C) Pharming

D) Phishing

[answer = C]

[if selection = C]

Yes, pharming attacks operate at the server level – you type in a legitimate website address but the hacker's software redirects you, without your knowledge, to a fake website where the scam takes place.

[answer ≠ C]

That's incorrect. Attacks like this are known as pharming attacks. The malicious software operates at the server level of the computer. The unsuspecting user doesn't have the malware on their machine and they can't avoid being redirected.

Question 71

What is the generic term for mobile storage devices that can be easily concealed and used to steal information?

A) Stealers

B) Sneakers

C) Creepers

D) Leakers

[answer = B]

[if selection = B]

That's right. A sneaker is any kind of mass storage device that can be easily concealed. Common examples include mobile phones, USB sticks, PDAs, digital cameras, web cams, digital voice recorders, smart card and magnetic stripe burners.

[answer ≠ B]

That's incorrect, a sneaker is the term for a mass storage device that can be easily concealed. Common examples include mobile phones, USB sticks, PDAs, digital cameras, web cams, digital voice recorders, smart card and magnetic stripe burners.

Incident reporting

Question 72

What should you do if you detect the unauthorised storage of inappropriate images on your organisation's network?

A) Report it

B) Try and fix the problem yourself

C) Both of the above

[answer = A]

[if selection = A]

That's right. All computer security incidents should be promptly reported. Once you have done that, you should await further instructions. Attempting to fix the problem yourself could create further problems – and could obscure vital evidence.

[if selection = B]

Sorry, this option is incorrect. All computer security incidents should be promptly reported. Once you have done that, you should await further instructions. Attempting to fix the problem yourself could create further problems – and could obscure vital evidence.

[if selection = C]

Sorry, this option is incorrect. All computer security incidents should be promptly reported. Once you have done that, you should await further instructions. Attempting to fix the problem yourself could create further problems – and could obscure vital evidence.

Question 73

Computer security incidents like data theft are usually very hard to detect for normal network users. True or false?

A) True

B) False

[answer = B]

[if selection = A]

Your choice is incorrect. System instability, mouse cursors moving by themselves or files whose properties suddenly change can, when taken together, reveal the existence of further, underlying security problems.

[if selection = B]

That's right. System instability, mouse cursors moving by themselves or files whose properties suddenly change can, when taken together, reveal the existence of further, underlying security problems.

Management and IT responsibilities

Question 74

Who's responsible for the overall management of information security within your organisation? A) BS&S Division, B) Security department, C) Managers.

A) A and B

B) B and C

C) A, B and C

[answer = C]

[if selection = C]

That's correct. Responsibility for information security management is shared between the organisation's managers, security and the BS&S Division. All three groups have specific roles to play.

[if selection ≠ C]

Sorry, this selection is incorrect. In fact all three groups – managers, security and the BS&S Division – have a shared responsibility for information security management. They all have specific, complementary roles to play.

Question 75

If you come across an incident that you suspect may have put SP AusNet's information security at risk, should you report it, and if so, to whom?

A) It's not my responsibility to report incidents. There's no obligation for me to do this

B) I should report any incident immediately, to the police

C) I should report any incident at the earliest possible opportunity to my manager, or to the security department

[answer = C]

[if selection = C]

Yes. You should certainly report any incident as soon as possible, either to your manager, or to the security department, or to any other designated person who needs to know about it.

[if selection ≠ C]

Sorry, this selection is incorrect. You should report any incident as soon as possible, either to your manager, or to the security department, or to any other designated person who needs to know about it.

Question 76

You have received a report from one of your staff that they saw another staff member going through a colleague's desk and filing cabinets, after hours. In particular they took one file and put it in their briefcase. The member of staff making the report has a history of making complaints against colleagues. What should you do?

A) Cross-question the 'guilty' colleague immediately, to find out what they were up to

B) Point out to the staff member who has made the report that they shouldn't report colleagues unless they're absolutely sure of their facts

C) Investigate the matter for yourself, interviewing all the parties involved before forming a view as to whether or not a security incident has taken place

D) Refer the matter to the security department – it's a security issue, not a management issue

[answer = C]

[if selection = C]

Yes. If a security incident *has* taken place then you must take action. Making sure that staff are aware of their information security responsibilities and that they comply with the rules is a key part of any manager's job.

[if selection = A]

Sorry, this selection is incorrect. If a security incident *has* taken place then you must take action. Making sure that staff are aware of their information security responsibilities and that they comply with the rules is a key part of any manager's job.

[if selection = B]

Sorry, this selection is incorrect. If a security incident has taken place then you must take action. Check your facts before you start making accusations. Making sure staff are aware of their information security responsibilities and that they comply with the rules is a key part of any manager's job.

[if selection = D]

Sorry, this selection is incorrect. You should check the facts out for yourself before approaching security.

Question 77

The purpose of information security management is to completely eliminate all security risks. Is this an accurate statement – yes or no?

A) Yes

B) No

[answer = B]

[if selection = B]

You're correct, this is not an accurate statement at all. Eliminating risks completely is virtually impossible and would be extremely costly. The purpose of information security is to minimise the risks to security, keeping them under control and at a manageable level.

[if selection = A]

Sorry, this selection is incorrect. This is not an accurate statement at all. Eliminating risks completely is virtually impossible. The purpose of information security is to minimise the risks to security, keeping them under control and at a manageable level.

Question 78

Where should business continuity plans be kept?

A) In a locked filing cabinet in the basement

B) In a secure place on-site, where those who may need it can have easy access to it

C) At the homes of the various people who will be responsible for implementing the plan, should it need to be used

D) Both B and C

[answer = D]

[if selection = D]

Yes. At least one copy of the plan should be stored on-site, where those responsible for its implementation can gain access to it. Further copies stored off-site, at the homes of those charged with the plan's implementation in the event of an emergency.

[if selection ≠ D]

Sorry, this option is incorrect. At least one copy of the plan should be stored on-site, where those responsible for its implementation can gain access to it. Further copies should be stored off-site, at the homes of those charged with the plan's implementation in the event of an emergency.

Game feedback:

Mastery score = 80%

[If user scores above the mastery score they will see feedbacks depending on how much their score was over the mastery score, e.g. if mastery score is set to 70% and they score 90%, they will be 67% over the remainder of the mastery score (at 70% there will be 30% left and they have scored an extra 20%, which is 67% more).]

[50-100% questions correctly answered above the mastery score]

Excellent! You obviously have a clear understanding of the principles of information security. Remember to use your knowledge and skills every day, and be on the lookout for potential risks.

[0-49% questions correctly answered above the mastery score]

Well done! This is a good score and you have a good grasp of information security, but remember, there is always room for improvement. Make information security an important part of your job every day.

[If user achieves the pass mark they will be presented with the opportunity to print a certificate of their results]

[If user scores below the mastery score they will see feedbacks depending on how close they got to mastery score, e.g. if mastery score is set to 70% and they score 60%, they will have scored 87% of the mastery score]

This is not a bad score, but you should still make the effort to ensure you know all the important information security messages and put these into practice every day.

[34-66% questions answered correctly of the mastery score]

You still have room for improving your information security knowledge. Make sure you understand all the important information security messages.

[0-33% questions answered correctly of the mastery score]

You didn't do very well. You must make sure that you understand the important information security messages in this course.

Certificate of Achievement:

Record of Achievement

presented by

SAI Global Compliance Division

[insert name of user]
Achieved a score of [insert score] out of 20
on the subject of information security by completing the training program For Your Eyes Only

Award Date: [insert date when test taken – e.g. format 31 October 2004]

Game help screens:

The Text Based Assessment:

Option Buttons…

Click here to answer the questions.

Feedback…

Your feedback will appear here.

Exit…

Click here to exit the assessment test.

Help…

Click here for help.

Forward Button…

Click here to move to the next screen.

Instructions…

Click on the forward button to remove this screen.

The Golf Game:

Instructional text

The aim of the game is to play a round of golf and reach the clubhouse. You are accompanied by your Information Security Manager who will ask you a question to test your knowledge before you tee off at each hole. You need to answer correctly to get the ball in the hole.

To begin, click on one of the three golf balls. The number displayed indicates the bonus value of a question that will then be presented. Click on your answer from the options shown. Each correct question will earn you bonus points and these will be shown on your scorecard.

Additional messages:

Text in English	*Alternative/translation*
Loading…	
Please wait…	
Name	
Exit	
Help	
Would you like to see the introduction to the game?	
Are you sure you wish to exit?	
For Your Eyes Only	
An information security awareness program	
Golf	
Press the Help button for the rules	
No *(as in abbreviation of 'number')*	
Scr *(as in abbreviation of 'score')*	
Bonus	
Club 1	
Admit one	
This voucher entitles the bearer to a free game of golf	
The Security Challenge	
Good luck!	
Next	
Help Score	

Date *(e.g. format 31 October 2004)*	
Time	
Score	
out of *(as in '14 out of 20')*	
Continue	
Start	
Glossary	
Top *(as in back to top of glossary)*	
Please do not close this window while running a training course.	
You may now close this window.	
Introduction	
Would you like to return to the last page you visited or start the module again?	
Restart	
Click to move on	
You Scored	
Click here to exit the assessment test	
Would you like to print a certificate of your results?	
January	
February	
March	
April	
May	
June	
July	
August	
September	
October	
November	
December	
[Alt: Help*]*	
[Alt: Exit*]*	
[Alt: Glossary*]*	

OCCAM Course Descriptions:

Title to appear	SCO description	Course description	Manifest description
For Your Eyes Only International		A program to raise awareness and measure understanding of information security issues.	A program to raise awareness and measure understanding of information security issues
Introduction	Welcomes you to For Your Eyes Only and gives a brief overview of the content of each module.		
What is information security and why does it matter?	Explains what is meant by information security and demonstrates why security should be taken seriously. Looks at what policies and procedures are designed to protect and highlights the possible consequences if these are not implemented effectively.		
How does information security affect me?	Shows the practical steps that should be taken to help protect the security of information within SP AusNet.		
Entry control	Guides you on how to follow SP AusNet's entry control procedures for the security and protection of the workforce and the protection of the organisation's information and other assets.		
Clear desk and secure disposal policies	Highlights the importance of keeping desks tidy and information secure to ensure that items aren't left around for non-authorised people to view. Also offers guidance on how to dispose of various types of data and equipment		

	securely.		
Password management	Explains the correct usage of passwords, challenges how people use their password, and how to select an effective password.		
Classifying Information	Describes and explains the significance of different types of data classification.		
Systems integrity	Shows why it is important to use approved software and hardware, and the role backups play in recovering data.		
Malware	Raises awareness of the problems malware can cause an organisation.		
Electronic communication	Tests your knowledge of, and suggests ideal practice for, e-mail security, Instant Messaging Systems, faxing information, and dealing with third parties. Also looks at ways of preventing abuse of SP AusNet's communications network.		
Internet security and acceptable use	Looks at the security risks involved in using the Internet, including connections, viruses and chat rooms.		
Security out of the office	Focuses on the increased risks employees face while out of the office, and the extra care needed to protect themselves and any equipment they may have against these risks.		
Social engineering	Looks at both computer and human-based social engineering, reinforcing the message that not everyone who requests information is genuinely entitled to it.		

Incident reporting	Gives examples of incidents that require reporting and describes the procedures that must be followed.		
Information security in action	Shows information security measures in action in the context of a work-based scenario.		
Management and IT responsibilities	Highlights the additional responsibilities you may have as a manager or IT specialist for information security management, staff training and supervision, responsibility for assets, incident reporting and business continuity.		
The security challenge	A challenging and entertaining assessment game, designed to test your knowledge and understanding of the learning material presented.		