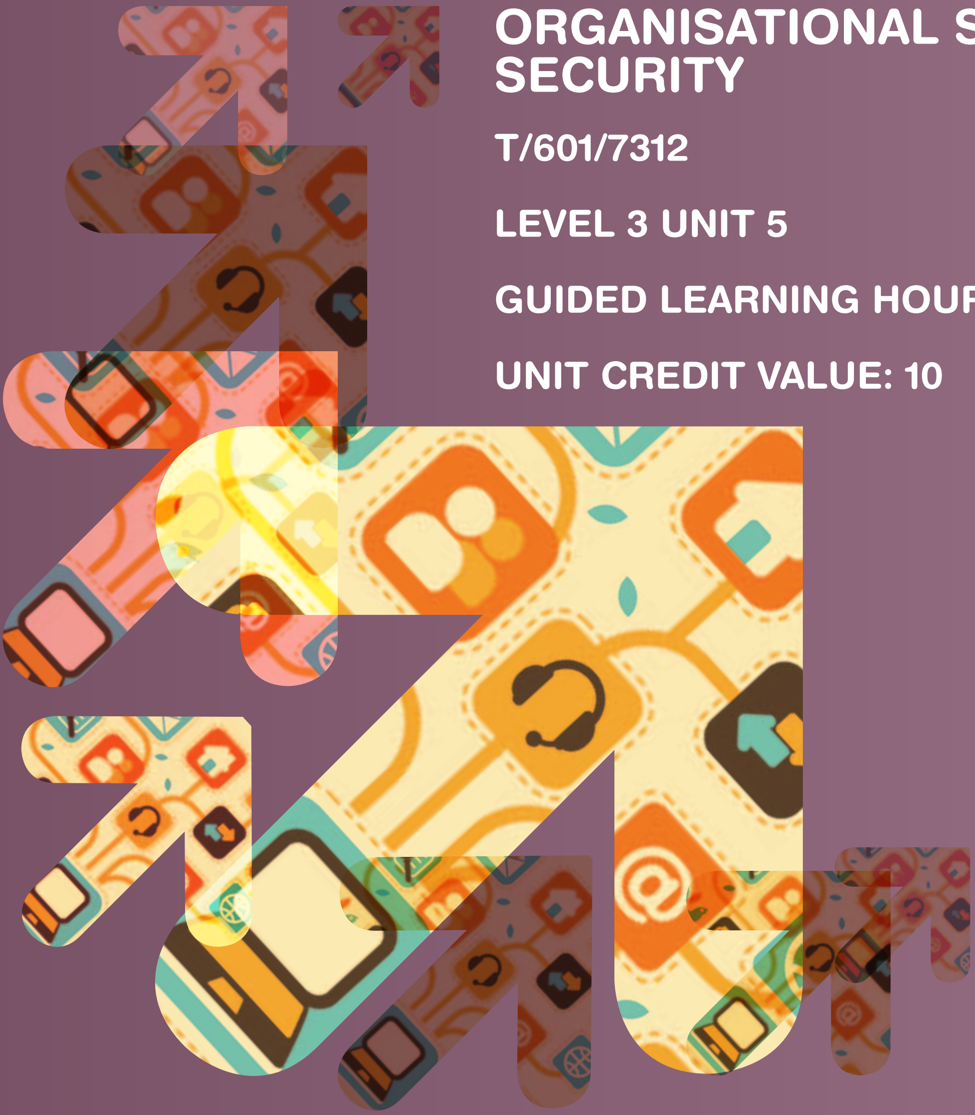
Accredited

OCR LEVEL 3 CAMBRIDGE TECHNICAL

CERTIFICATE/DIPLOMA IN

IT



ORGANISATIONAL SYSTEMS SECURITY

T/601/7312

LEVEL 3 UNIT 5

GUIDED LEARNING HOURS: 60

UNIT CREDIT VALUE: 10

ORGANISATIONAL SYSTEMS SECURITY

T/601/7312

LEVEL 3 UNIT 5

AIM OF THE UNIT

Organisations collect, create and manipulate a wide range of data and information; the cost of these activities is often much higher than the organisation realises until they are lost or stolen. Everyone who works with an information system should understand their responsibility to protect the system against theft or loss and all IT professionals need to understand how to support the organisation in protecting its digital assets and hardware. This unit will enable the learner to recognise the importance of protecting systems against any security issues or failures when working with the hardware and software and providing guidance to customers on the security of their systems. Additionally, it will also ensure that learners keep the importance of security at the forefront of their activities in order to identify threats and protect the organisation and its assets as they work with the information system while working towards the qualification as well as in the work place.

The aim of this unit is to provide the learner with an understanding of the importance of securing organisational IT systems, the impact of the law on the application of security policies and the range of security threats which must be protected against with an organisation and the tools which are used to provide protection. The learner will be able to apply this knowledge to any organisation through reviewing and making recommendations for improvements.

ASSESSMENT AND GRADING CRITERIA

Learning Outcome (LO) The learner will:	**Pass** The assessment criteria are the pass requirements for this unit. The learner can:	**Merit** To achieve a merit the evidence must show that, in addition to the pass criteria, the learner is able to:	**Distinction** To achieve a distinction the evidence must show that, in addition to the pass and merit criteria, the learner is able to:
1 Understand the impact of potential threats to IT systems	P1 explain the impact of different types of threat on an organisation	M1 compare and contrast the impact of different types of threat to different organisation types	
2 Know how organisations can keep systems and data secure	P2 describe how physical security measures can aid in keeping systems secure	M2 discuss the effectiveness of physical security measures used in an identified organisation	
	P3 describe how software and network security can keep systems and data secure	M3 discuss the effectiveness of software security measures used in an identified organisation	
3 Understand the organisational issues affecting the security of IT systems	P4 explain the policies and guidelines for managing organisational IT security issues		D1 recommend modifications to policies and guidelines for managing organisational IT security issues
	P5 explain how employment contracts can affect security		D2 review contracts of employment in an organisation and their impact on security
	P6 assess the laws related to security and privacy of data		

TEACHING CONTENT

The unit content describes what has to be taught to ensure that learners are able to access the highest grade.

Anything which follows an i.e. details what must be taught as part of that area of content.

Anything which follows an e.g. is illustrative, it should be noted that where e.g. is used , learners must know and be able to apply relevant examples to their work though these do not need to be the same ones specified in the unit content.

LO1 Understand the impact of potential threats to IT systems

Threats

- physical
  - environmental
    - temperature
    - humidity
    - natural disasters:
      - earthquakes
      - flooding.
  - malicious
    - causing system crashes through manipulating software
    - wilful damage to monitors, hard discs
    - physical theft.
- technological
  - malicious codes:
    - viruses, code which attaches to other software, or emails causing damage
    - worms:
      - Internet
      - email
    - spyware: tracking activity such as key strokes on a keyboard.
  - hacking:
    - internal, employee accessing areas outside of their area
    - external, non-employee accessing from external location
  - theft of data
- accidental damage (e.g. spilling drinks on key boards, deleting programs or files).

Impacts

- financial (e.g. loss of business, pricing data, invoicing information)
- loss of reputation
- loss of service and access
- loss of security of confidential information (e.g. national security, payroll information, business strategies).

LO2 Know how organisations can keep systems and data secure

Physical protection

- locks (e.g. doors, computer screens, filing cabinets)
- placing computers above known flood levels
- back up systems in other locations
- keypads and biometrics
- security staff.

Network and software protection

- access levels
- software firewalls
- anti-malware software
- backup utilities
- encryption of files and folders
- password protected documents
- encryption of entire discs
- wireless security.

LO3 Understand the organisational issues affecting the security of IT systems

- policies, procedures and guidelines (e.g. password and username, email usage, cyberbullying, access privileges, backup and disaster recovery, network security, physical controls, asset management, network security policy, user responsibilities, issue reporting).

Legislation

- Computer Misuse Act (2000)
- Data Protection Act (1998).

DELIVERY GUIDANCE

It should be noted that this unit can be taught and assessed entirely as a theoretical unit. However, learners will find it far more interesting if they are encouraged to undertake some practical activities. For example, a walk around the computing facilities of their work place or learning centre would enable them to identify any physical security which is in place and discuss whether there is sufficient range and depth to ensure the systems and data are secure. Similarly, with software and network security, learners could be given the opportunity to produce a real public/private key encryption arrangement using free software, check that software patches are up to date, create passwords on files. For the training laboratory they could create and implement access levels linked to usernames. Additionally, software packages such as VM and CAM studio can be used capture evidence of a threat or attempt at illegal access.

Understand the impact of potential threats to IT systems

The internet, journals or newspaper articles and books on IT security are full of interesting and relevant cases: many are humorous, in a macabre way, and others reflect things that learners will have seen in films, this approach makes the subject more alive and relevant to the learner.

Learners should be encouraged to work as groups to find examples of these cases and should then as part of a small or wider group discuss the impacts to organisations and what steps could or were taken to secure against the identified threats. Learners should be encouraged to maintain their research for the latest IT security failure on the news and should be encouraged to investigate different approaches to IT security and examples of successes and failures across an increasingly wide spectrum of organisations.

Learners should take their general findings and apply them to an organisation they are familiar with wither through work experience, workshop or their training facility. Alternatively learners may carry out research on an organisation of their choice to identify how these historical security failures would realistically impact on that organisation.

Know how organisations can keep systems and data secure

This learning outcome is best taught holistically as this would be more appropriate to the sector and will encourage learners to widen their scope and considerations.

Learners should use what they have learned in Learning Outcome 1 to consider in more detail the options for protecting systems. An opportunity for group work arises here as the learners could be asked to find specific examples for a range of physical and software security which would help to protect the computer system from the various risks that they have already identified.

The learner should use their general findings and again apply them to an organisation with which they are familiar or have been given within a scenario by their tutor. The precise number of protection methods cannot be given as it will depend upon the precise nature of the organisation which has been identified but for supplied scenarios learners should be encouraged to consider a wide range and if they have chosen an organisation they have worked with and opportunities for implementing security measures is limited, they could identify what has been implemented already, potential improvements to it and the reasons for the implementation.

Understand the organisational issues affecting the security of IT systems

The internet has samples of model security policies which are actually in use and the centre will have one too. Learners should research these and obtain copies of one or two comparing their ideas for policies and procedures with those from a real organisation such as the learning centre or an identified organisation. The learner will develop their reasoning so that they are able to move from general discussion to evaluating policies and guidelines which have been designed for a specific used within an organisation.

The learner should have a clear understanding of the type of organisation they are working with such as its functions, locations(s) and types of data it uses and then be able to review current policies and procedures for the organisation making recommendations for improvements. The learners should also consider how an organisations policies and procedures are linked to an individual's contract of employment and the responsibilities and liabilities these place on the employee.

With regards to legislation learners should focus on what each of the Acts means, the purpose of the act and the implications for an organisation or individual. With constantly changing legislation learners should review and consider new or outline legislation or revisions that may affect an organisation in this way.

The Computer Misuse Act (2000)

The Computer Misuse Act clearly states that the individual must know that they are carrying out an unauthorised action, if not they may not be found guilty even if the result is serious for the company concerned. For non-employees it is obvious that they will not have authorisation but for employees and contractors it has to be spelt out and it is the limits of rights and responsibilities of access and activities carried out which ensures that the employee can be held responsible.

Key elements include

a) access any computer system without permission, even if you do nothing more than look at the content or just reach the log in page.

b) access with the intention to commit another crime

c) access to carry out unauthorised actions with the intention of damaging the computer.

This is a very short law most of which was written by IT specialists rather than lawyers and thus it is relatively easy to understand. This law is particularly relevant to learners because it requires that the anyone prosecuted under the Act, knows that they were not to carry out whatever actions have resulted in their being in court, and it is the clarity of the employee's contract of employment (explored by the learners earlier) which is used to identify whether they have been explicitly told that they may NOT carryout particular tasks.

The Data Protection Act 1998

For the Data Protection Act, even in organisations, individuals can be held personally responsible for failing to comply with the principles if it can be proved that a director, manager, secretary or similar officer was negligent or knew or helped in the committing of an offence.

Relates to the responsibilities of organisations and individuals who collect and manipulate data on living individuals and the processing personal data fairly and lawfully.

Learners should discuss what is meant by fairly? what is lawful? (The Information Commissioner's Office website has useful leaflets on interpreting the principles into layman's English). No in depth study is required just the areas which are important to anyone working with computers. It is not appropriate for learners to merely list the eight precepts, what is required is an understanding of what they mean in terms of protecting individuals and also to understand what is required by the organisation in order to be compliant with the Law. This will be most effective through discussion as a group.

Copyright could also be discussed in terms of an employees responsibilities and liabilities in terms of downloading images, illegal downloads of music and copying software illegally.

SUGGESTED ASSESSMENT SCENARIOS AND TASK PLUS GUIDANCE ON ASSESSING THE SUGGESTED TASKS

Assessment Criteria P1, M1

P1: Learners could prepare a presentation explaining the impact of different types of threat to an IT system of an organisation. They should include a minimum of five threats as per the teaching content, including physical and technological threats that are realistically applicable to modern organisations and their IT systems.

For merit criterion M1 Learners should compare and contrast the impact of threats (ideally those they have explained in P1) and what this would mean for two different types of organisation, including their own organisation if applicable, and why. The learner must provide a complete set of speaker notes which contain detailed information for the bullets or data on their slides. In a workplace, this could be evidenced with the learner taking part in a security audit within a group or individually. Where the evidence has been used is a group activity then the learner must identify their own contribution and have a witness testimony from their supervisor or manager, confirming that they have undertaken the specific tasks identified in the documentation which is being offered as evidence of having achieved the assessment criteria.

Assessment Criteria P2, P3, M2, M3

P2 and P3: Learners should produce documentation for new colleagues describing the different types of physical security methods which are available to a selected organisation and the software and network security methods. This could be in the form of two leaflets or one larger report. The chosen format must not simply contain a set of bullet points but must include sufficient text so that a new starter would understand what the security measure is and when it is relevant. In order to achieve a pass the learner should discuss at least five different methods of protection against physical threats and five different methods of software and network security protection again technological data security threats.

For merit criteria M2 and M3, the learner should ensure that they clearly extend their leaflets or documentation to discuss the effectiveness of the methods. M2 refers to the physical security and M3 the technological. The learners must also include information on which of these methods are most relevant to their organisation and why they believe this to be the case.

In the case of learners who are on work placement, this assessment may use evidence from the development of new policies, procedures and guidelines carried out by the learner. A witness testimony should be sought from the manager to support the evidence produced by the learner, confirming that the work produced is that of the learner and that it meets the standards required for the organisation. This may require additional discussions or a brief report by the learner to ensure that they have completely met the assessment criteria.

Assessment Criteria P4, P5, P6, D1, D2

P4 The learner should explain at least three different policies and guidelines for managing organisational IT security and give details of the purpose and scope for these. This could be in the form of a report.

P5 The learner should evidence at least three different types of employment contract for junior, middle management and senior management and explain how their generic roles and responsibilities and the wording of the contracts might be used to implement the security procedures within an organisation. This could be evidenced as a report with copies of the contracts to support explanations.

P6 The learner should assess the laws relating to security and privacy which are relevant to the United Kingdom and consider how they affect institutions. They could relate this to identified organisations to support their work. This could be presented as a report.

For distinction criterion D1 the learner must use policies and guidelines relating to information security used within an identified organisation potentially using those reviewed in P4. The learner should describe and comment on the policies and procedures and recommend modifications to them identifying how these recommendations would improve the policies and guidelines. This could be evidenced in the form of a report.

For distinction criterion D2 The learner must have the opportunity to review contracts of employment and the components that will enable an organisation to protect themselves. As this is an extension of P5, learners should extend their explanations to review how organisations can further improve their security by including policies *within contracts of employment and how this may impact on the organisation as a whole. This could be evidenced through a report or presentation but must include sufficient details to support their review.*

MAPPING WITHIN THE QUALIFICATION TO THE OTHER UNITS

Unit 3	Computer systems
Unit 6	e-commerce
Unit 12	Website production

LINKS TO NOS

6.2 IT Security Management

CONTACT US

Staff at the OCR Customer Contact Centre are available to take your call between 8am and 5.30pm, Monday to Friday.

We're always delighted to answer questions and give advice.

Telephone 02476 851509
Email cambridgetechnicals@ocr.org.uk
www.ocr.org.uk