Unit Title:	**Principles of ICT systems and data security**
OCR unit number:	25
Unit reference number:	L/601/3508
Level:	2
Credit value:	6
Guided learning hours:	45

Unit aim

The aim of this unit is that learners will:

- Know the common types of threat to ICT systems and data
- Know how to protect ICT systems
- Be aware of the applications of cryptography to ICT systems and data

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
The Learner will: 1 Know the common types of threat to ICT systems and data	**The Learner can:** 1.1 Identify common types of physical threats to ICT systems and data (hardware damage, loss and theft) 1.2 Identify common types of electronic threats to ICT systems and data (e.g. denial of service, data theft or damage, unauthorised use) 1.3 List the security vulnerabilities associated with remote access technologies (including wireless)	• potential weaknesses in the external security of LANs e.g. firewall, web server, mail server, wireless LAN vulnerabilities, weaknesses in VPN etc • the ways systems can be accessed without authorisation without damaging data • the dangers associated with poorly protected passwords • the different risks to data due to unauthorised access e.g. removal/copying of data or code; damage or destruction of data or code internally or externally to the system • the risks associated with malware and the different types and associated risks • how to protect hardware and media against loss or theft • file permissions, password levels on files and data and file attributes

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
		• the risks associated with corrupted or infected email attachments, software and/or images downloaded from the Internet; access to malicious websites. They should know about the risks associated with internal and external hackers • the following legislation: - Data Protections Act 1998 - The Privacy and Electronic Communications (EC Directive) Regulations 2003 - Computer Misuse Act 1990
2 Know how to protect ICT systems	2.1 Identify methods of providing physical access control and security for ICT systems (locks, biometric controls, CCTV, shielding, fire detection and control) 2.2 State methods of providing electronic access control and security for ICT systems (firewalls, virtual networks, secure connection/transfer protocols, secure wireless connection) 2.3 Identify common types of malicious code: • Virus • Trojan • Logic Bomb • Worm • Spyware 2.4 Identify the characteristics of strong passwords	• how to protect IT systems using: - physical security - access control - limited visibility of data - data security software - encryption - backing up and restoring data • the comparison of different methods for providing physical and electronic access and how to select the most appropriate method(s)

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
3 Be aware of the applications of cryptography to ICT systems and data	3.1 State how cryptography can be applied to ICT system and data security 3.2 State how Public Key Infrastructure (PKI) operates	• how to create a security plan for a small business or home network to include: - implementing a password policy - locking down user accounts - security administrator's permissions - installing or updating security software/updates • security policies such as: - backup and recovery schemes - installing/upgrading software - file and folder monitoring (monitoring use of data) - anti-virus protection - setting up files and folder permissions

Assessment

The qualification has been designed to develop knowledge, understanding and skills in the full range of functions involved in the planning and control, hardware, software and systems installation, software solutions and the production of customer support materials. It also provides opportunities for learners to study towards system and network management, to specialise in one or more specific programming languages in addition to being able to take units that are vendor specific.

Each unit within the specification is designed around the principle that candidates will build a portfolio of evidence relating to progression towards meeting the unit assessment objectives.

The unit assessment objectives reflect the demands of the learning outcomes for each unit.

In order for candidates to be able to effectively progress towards meeting the requirements of each assessment objective, tutors must make sure that the supporting knowledge, understanding and skills requirements for each objective are fully addressed. The identified knowledge, understanding and skills are not exhaustive and may be expanded upon or tailored to particular contexts to which the unit is being taught and the assessment objective applied.

We recommend that teaching and development of subject content and associated skills be referenced to real vocational situations, through the utilisation of appropriate industrial contact, vocationally experienced delivery personnel, and real life case studies.

All the learning outcomes and assessment criteria must be clearly evidenced in the submitted work, which is externally moderated by OCR.

Results will be Pass or Fail.

Guidance on assessment and evidence requirements

Candidates do not have to achieve units in any particular order and tutors should tailor learning programmes to meet individual candidate needs. It is recommended that, wherever possible, centres adopt a holistic approach to the delivery of the qualification and identify opportunities to link the units.

Centres are free to deliver this qualification using any mode of delivery that meets the needs of their candidates. Whatever mode of delivery is used, centres must ensure that learners have appropriate access to appropriate resources and consider the candidates' complete learning experience when designing learning programmes. This is particularly important in relation to candidates studying part time alongside real work commitments where candidates may bring with them a wealth of experience that should be utilised to maximum effect by tutors and assessors.

It is difficult to give a detailed answer to how much evidence is required as it depends on the type of evidence collected and the judgement of assessors. The main principles, however, are as follows: for a candidate to be judged competent in a unit, the evidence presented must satisfy:

- all the items listed, in the section 'Learning Outcomes'
- all the areas in the section 'Assessment Criteria'

Questioning the candidate is normally an ongoing part of the assessment process, and is necessary to:

- test a candidate's knowledge of facts and procedures
- check if a candidate understands principles and theories *and*
- collect information on the type and purpose of the processes a candidate has gone through
- candidate responses must be recorded

The quality and breadth of evidence provided should determine whether an assessor is confident that a candidate is competent or not. Assessors must be convinced that candidates working on their own can work independently to the required standard.

Additional information

For further information regarding administration for this qualification, please refer to the OCR document *'Admin Guide: Vocational Qualifications'* on the OCR website www.ocr.org.uk .