OCR
Oxford Cambridge and RSA

Unit Title:	**IT security for users**
OCR unit number:	180
Unit reference number:	D/502/4258
Level:	3
Credit value:	3
Guided learning hours:	20

Unit purpose and aim

This is the ability to protect hardware, software and the data within an IT system against theft, malfunction and unauthorised access.

This unit is about the skills and knowledge needed by the IT User to monitor potential risks and take steps to protect own and others' systems, data and software (e.g. from unauthorised remote access, disaster recovery or contingency planning).

Learning Outcomes	Assessment Criteria	Examples
The learner will: 1 Select, use and develop appropriate procedures to monitor and minimise security risk to IT systems and data	**The learner can:** 1.1. Evaluate the security issues that may threaten system performance 1.2. Select, use and evaluate a range of security precautions to protect IT systems and monitor security 1.3. Evaluate the threats to system and information security and integrity 1.4. Manage access to information sources securely to maintain confidentiality, integrity and availability of information 1.5. Explain why and how to minimise security risks to hardware, software and data for different users 1.6. Apply, maintain and develop guidelines and procedures for the secure use of IT	• Threats to system performance: Unwanted e-mail (often referred to as "spam"), malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers) and hackers; hoaxes; vulnerability • Security precautions: Configure anti-virus software, adjust firewall settings, adjust internet security settings; carry out security checks, report security threats or breaches; backup; store personal data and software safely; treat messages, files, software and attachments from unknown sources with caution; proxy servers; download security software patches and updates; effectiveness of security measures

Learning Outcomes	Assessment Criteria	Examples
	1.7. Select and use effective backup and archiving procedures for systems and data	• Threats to information security: From theft, unauthorised access, accidental file deletion, use of removable storage media, corruption; malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers), hackers, phishing and identity theft • Keep information secure: Username and password/PIN selection and management, password strength; how and when to change passwords; Respect confidentiality, avoid inappropriate disclosure of information; digital signatures; data encryption; security classification, preserve availability • Minimise risk: Access controls: Physical controls, locks, passwords, access levels, data protection, data retention. Security measures: anti-virus software, firewalls, security software and settings. Risk assessment: anti-spam software, software updates; risk management; user profiles, operating system settings, user authentication (ID cards, smart cards, biometrics); risks associated with widespread use of technology

Learning Outcomes	Assessment Criteria	Examples
		• Guidelines and procedures: Set by: employer or organisation, privacy, laws and regulations, disaster recovery plans, contingency systems, dealing with security breaches, backup procedures; administrative procedures and controls

Assessment

All ITQ units may be assessed using any method, or combination of methods, which clearly demonstrates that the learning outcomes and assessment criteria have been met. Assessments must also take into account the additional information provided in the unit Purpose and Aims relating to the level of demand of:

- the activity, task, problem or question and the context in which it is set;
- the information input and output type and structure involved; and
- the IT tools, techniques or functions to be used.

See the Assessment and postal moderation section of the ITQ Centre Handbook.

Guidance on assessment

Candidates must complete the Evidence Checklist for this unit without any gaps. Individual unit checklists are available to download from the qualification webpage (see forms).

In the Evidence Checklists, the examples given are indicative of the learning context at each level and are not intended to form a prescriptive list for the purpose of assessment.

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 .