OCR
Oxford Cambridge and RSA

Unit 242: IT Security for Users Level 2

Level: 2
Credit value: 2
Guided learning hours: 15

Learning Outcomes	Assessment Criteria	Examples
The learner will: 1. Select and use appropriate methods to minimise security risk to IT systems and data	The learner can: 1.1 Describe the security issues that may threaten system performance 1.2 Apply a range of security precautions to protect IT systems and data 1.3 Describe the threats to system and information security and integrity 1.4 Keep information secure and manage personal access to information sources securely 1.5 Describe ways to protect hardware, software and data and minimise security risk 1.6 Apply guidelines and procedures for the secure use of IT 1.7 Describe why it is important to backup data and how to do so securely 1.8 Select and use effective backup procedures for systems and data	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 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;* 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; *unsecured and public networks, Bluetooth, portable and USB devices* 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 Protect systems and data: Access controls: Physical controls, locks, passwords, access levels. Security measures: anti-virus software, firewalls, security software and settings. *Risk assessment; anti-spam software, software updates* Guidelines and procedures: Set by: employer or organisation; privacy, *legal requirements; how to use products to ensure information security within organisations*

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 avoid common security risks and control access to software and data; and use a wider range of methods to protect software and data (eg from exchanging information by e-mail or when downloading software from the Internet).

Details of relationship between the unit and national occupational standards

This unit maps fully to competences outlined in IT User National Occupational Standards version 3 (2009).

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 Recommended Assessment Methods in the ITQ Centre Handbook.

Evidence requirements

An evidence checklist must be completed without gaps.

Guidance on assessment and evidence requirements

Please refer to the centre handbook for ITQ 2009.