SVQ for IT Users (ITQ) — level 2 (SCQF level 5)

F99T 04: IT Security for Users 2

2 SCQF credit points at SCQF level 5

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

Outcome **On completion of this Unit the candidate should be able to:**	Skills and Techniques	Knowledge and Understanding
1 Select and use appropriate methods to minimise security risk to IT systems and data.	1 Apply a range of **security precautions to protect IT systems and data**. 2 **Keep information secure** and manage personal access to information sources securely. 3 Apply **guidelines and procedures** for the secure use of IT. 4 Select and use effective backup procedures for systems and data.	1 Describe the security issues that may **threaten system performance**. 2 Describe the **threats to system and information security** and integrity. 3 Describe ways to p**rotect hardware, software and data** and minimise security risk. 4 Describe why it is important to backup data and how to do so securely.

Note: The **emboldened** items are exemplified in the Support Notes.

Evidence Requirements

Completion of a portfolio (manual, electronic or combination) to cover all of the Skills and Techniques and Knowledge and Understanding points stated above. The evidence generated should adhere to the Assessment Strategy for this award and encompass a range of evidence types.

General information

This Unit equates to NOS (National Occupational Standards for IT Users 2009) ITS: IT Security for Users level 2. It has a stated number of SCQF credit points = 2 at SCQF level 5.

Note: aspects of personal safety when working online are covered in:

EML: Using e-mail

and

INT: Using the Internet

Support Notes

Summary

A SCQF level 5 (ITQ level 2) user can 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).

Examples of context which illustrate typical activities which might be undertaken by users:

- run anti-virus software to scan system and maintain security log
- (home user) ensure that their PC is protected by a firewall and runs up-to-date anti-virus software routinely

Examples of content are given separately for highlighted text, where explanatory notes are required on terminology in the Outcomes, and do not form part of the standards. Such examples are not meant to form a prescriptive list for the purposes of assessment but rather to amplify and interpret the generic terms used in the Performance Criteria in the light of current usage of ICT systems and software. These examples are subject to change as new tools and techniques become commonplace and older ones drift out of use.

The examples given below are indicative of the learning content and are not intended to form a prescriptive list for the purpose of assessment.

Outcome 1

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: Use access controls. *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; malicious programs (including viruses, worms, trojans, spyware, adware and rogue dialers), hackers, phishing and identity theft; unsecured and public networks, default passwords and settings, wireless networks, Bluetooth, portable and USB devices.

Access to information sources: Username and password/PIN selection *and management, password strength*; how and when to change passwords; online identity/profile; Real name, pseudonym, avatar; what personal information to include, who can see the information; 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*.

Security guidelines and procedures: Set by employer or organisation; security, privacy, legal requirements; how to use products to ensure information security within organisations.

Guidance on examples of evidence

Typical examples of evidence for Outcome 1

Assessor checklist which will record candidate competence in the selection and use of appropriate methods employed to minimise security risks to IT systems and data. Extended response questions which test the candidate's understanding of the knowledge and content items.

Disabled candidates and/or those with additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering whether any reasonable adjustments may be required. Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**