

SVQ for IT Users (ITQ) — level 1 (SCQF level 4)

F99R 04: IT Security for Users 1

1 SCQF credit points at SCQF level 4

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

Outcome	Skills and Techniques	Knowledge and Understanding
On completion of this Unit the candidate should be able to:		
1 Use appropriate methods to minimise security risks to IT systems and data.	1 Take appropriate security precautions to protect IT systems and data. 2 Take appropriate precautions to keep information secure . 3 Follow relevant guidelines and procedures for the secure use of IT. 4 Ensure personal data is backed up to appropriate media.	1 Identify security issues that may threaten system performance . 2 Identify threats to information security associated with the widespread use of technology. 3 Describe why it is important to backup data 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 1. It has a stated number of SCQF credit points =1 at SCQF level 4.

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 4 (ITQ level 1) user can identify day-to-day security risks and the laws and guidelines that affect the use of IT; and use simple methods to protect software and personal data (eg risks from people getting access to it who are not authorised) from viruses or from hardware not working properly.

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

- ◆ regular change of password using a range of alphanumeric characters and symbols
- ◆ understanding the importance of applying organisational procedures for maintaining security consistently

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 dialers) and hackers; hoaxes.

Security precautions: Use access controls: physical controls, locks, passwords, access levels; run 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.

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 diallers), 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, 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.

Security guidelines and procedures: Set by employer or organisation; security, privacy.

Guidance on examples of evidence

Typical examples of evidence for Outcome 1

Assessor checklist(s) which will record results of any candidate practical exercises. Knowledge may be tested using a mixture of multiple-choice questions and extended response questions. Candidate product evidence — electronic and/or hard copy.

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**