SVQ for IT Users (ITQ) — level 3 (SCQF level 6)

F99V 04: IT Security for Users 3

3 SCQF credit points at SCQF level 6

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, use and develop appropriate procedures to monitor and minimise security risk to IT systems and data.	1 Select, use and evaluate a range of **security precautions** to protect IT systems and monitor security. 2 Manage access to **information sources securely** to maintain confidentiality, integrity and availability of information. 3 Apply, maintain and develop **guidelines and procedures** for the secure use of IT. 4 Select and use effective backup and archiving procedures for systems and data.	1 Evaluate the security issues that may **threaten system performance**. 2 Evaluate the **threats to system and information security** and integrity. 3 Explain why and how to **minimise security risks** to hardware, software and data for different users.

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 3. It has a stated number of SCQF credit points = 3 at SCQF level 6.

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 6 (ITQ level 3) user can monitor potential risks and take steps to protect their own and others' systems, data and software (eg from unauthorised remote access, disaster recovery or contingency planning).

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

- develop backup and security guidelines for others to follow
- setting up a backup and recovery plan for a small business running a peer to peer network
- in larger organisations, aspects relating to security policy and practice at an advanced level may be the responsibility of IT professionals

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; *vulnerability.*

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; *effectiveness of security measures.*

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 and management, online identity/profiles; 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.*

Security 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.*

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, the management of access to information sources, application of the guidelines and procedures for the secure use of IT and the selection of appropriate and effective backup and archiving procedures. Extended response questions which will 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**