ITS: IT security for users

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

Note: aspects of personal safety when working online are covered in the Email and Internet AoCs

A. A foundation 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: Regular change of password using a range of alphanumeric characters and symbols.Understanding the importance of applying organisational procedures for maintaining security consistently.

B. An intermediate 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: Run anti-virus software to scan system and maintain security log. Home user ensuring their PC is protected by firewall and runs up-to-date anti-virus software routinely.

C. An advanced 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: 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 Level 3 may be the responsibility of IT professionals.

ITS: IT security for users

Element The competent person will…	**Performance Criteria** To demonstrate this competence they can…	**Knowledge** To demonstrate this competence they will also …	**Examples of Content** The examples given are indicative of the learning content at each level and are not intended to form a prescriptive list for the purpose of assessment
ITS:A1 Use appropriate methods to minimise security risks to IT systems and data	A1.2 Take appropriate **security precautions** to protect IT systems and data A1.4 Take appropriate precautions to **keep information secure** A1.5 Follow relevant **guidelines and procedures** for the secure use of IT A1.7 Ensure personal data is backed up to appropriate media	A1.1 Identify security issues that may **threaten system performance** A1.3 Identify **threats to information security** associated with the widespread use of technology A1.6 Describe why it is important to backup data securely	**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: 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

ITS: IT security for users

Element The competent person will…	**Performance Criteria** To demonstrate this competence they can…	**Knowledge** To demonstrate this competence they will also …	**Examples of Content** The examples given are indicative of the learning content at each level and are not intended to form a prescriptive list for the purpose of assessment
ITS:B1 Select and use appropriate methods to minimise security risk to IT systems and data	B1.2 Apply a range of **security precautions** to **protect IT systems and data** B1.4 **Keep information secure** and manage personal access to information sources securely B1.6 Apply **guidelines and procedures** for the secure use of IT B1.8 Select and use effective backup procedures for systems and data	B1.1 Describe the security issues that may **threaten system performance** B1.3 Describe the **threats to system and information security** and integrity B1.5 Describe ways to **protect hardware, software and data** and minimise security risk B1.7 Describe why it is important to backup data and how to do so securely	**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 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, 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

Using IT Systems

ITS: IT security for users

Element	Performance Criteria	Knowledge	Examples of Content
The competent person will…	To demonstrate this competence they can…	To demonstrate this competence they will also …	The examples given are indicative of the learning content at each level and are not intended to form a prescriptive list for the purpose of assessment
ITS:C1 Select, use and develop appropriate procedures to monitor and minimise security risk to IT systems and data	C1.2 Select, use and evaluate a range of **security precautions** to protect IT systems and monitor security C1.4 Manage access to **information sources** securely to maintain confidentiality, integrity and availability of information C1.6 Apply, maintain and develop **guidelines and procedures** for the secure use of IT C1.7 Select and use effective backup and archiving procedures for systems and data	C1.1 Evaluate the security issues that may **threaten system performance** C1.3 Evaluate the **threats to system and information security** and integrity C1.5 Explain why and how to **minimise security risks** to hardware, software and data for different users	**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