Silver Unit 4 IT Security for Users (ITQ: ITS)

Relevant LINKS

BACK TO ITQ UNITS **[1]**

Handbook home page **[2]**

Overview

This is the ability to protect hardware, software and the data within an IT system against theft, malfunction and unauthorised access. The candidate will be able to identify day-to-day security risks and key laws and guidelines that affect the use of IT. They will use simple methods to protect software and personal data (e.g. risks from people getting access to data who are not authorised). They will identify the risk from viruses or from hardware not working properly and take simple steps to remedy the situation.

Examples of context: Knowing the need to run regular virus checks computers running the Windows operating system.

Activities supporting the assessment of this award **[3]**

Example of work at this level **[4]**

Assessor's guide to interpreting the criteria

General Information

QCF general description for Level 1 qualifications

- Achievement at QCF level 1 (EQF Level 2) reflects the ability to use relevant knowledge, skills and procedures to complete routine tasks. It includes responsibility for completing tasks and procedures subject to direction or guidance.
- Use knowledge of facts, procedures and ideas to complete well-defined, routine tasks. Be aware of information relevant to
  the area of study or work
- Complete well-defined routine tasks. Use relevant skills and procedures. Select and use relevant information. Identify whether actions have been effective.
- Take responsibility for completing tasks and procedures subject to direction or guidance as needed

Requirements

- Standards must be confirmed by a trained Silver Level Assessor or higher

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

- Assessors must at a minimum record assessment judgements as entries in the on-line mark book on the INGOTs.org certification site.

- Routine evidence of work used for judging assessment outcomes in the candidates' records of their day to day work will be available from their e-portfolios and on-line work. Assessors should ensure that relevant web pages are available to their account manager on request by supply of the URL.

- When the candidate provides evidence of matching all the criteria to the specification subject to the guidance below, the assessor can request the award using the link on the certification site. The Account Manager will request a random sample of evidence from candidates' work that verifies the assessor's judgement.

- When the Account Manager is satisfied that the evidence is sufficient to safely make an award, the candidate's success will be confirmed and the unit certificate will be printable from the web site.

- This unit should take an average level 1 learner 10 hours of work to complete.

Assessment Method

Assessors can score each of the criteria L, S, H. N indicates no evidence and is the default starting position. L indicates some capability but secure capability has not yet been achieved and some help is still required. S indicates that the candidate can match the criterion to its required specification. H indicates performance that goes beyond the expected in at least some aspects. Candidates are required to achieve at least S on all the criteria to achieve the unit.

Expansion of the assessment criteria

1. Plan and create web pages

1.1 I can identify security issues that might threaten system performance
Candidates should be familiar with common security issues that could affect the way their computer performs.

Evidence: Assessor observations and day to day document files

Additional information and guidance:
A simple risk assessment can be used to identify the issues, for example selecting and prioritising risks from a provided list, sorting and classifying security issues. Relate this work to safety and security issues in the other units.

Examples of risks are:

- Using an operating system that is the target of most malware. Is it necessary?
- Unsolicited e-mail (spam) and associated attachments that could be intended to damage the system or applications software.
- Running anti-virus and spyware programs slows down other operations
- Viruses and malware that consume resources without the user being aware
- Web browser pop ups and advertising

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

They should also realise that most information sources, web sites, USB keys and discs are potential sources of virus infection especially on computers running older versions of the Windows operating system that are not now supported with security patches. Physical security of hardware is also important. If a memory module is taken from inside a computer the computer might still work if it still has some memory but performance will be affected.

Virus checkers significantly affect performance when running too. Early versions of Windows allowed programs to install themselves without reference to the user and there was a resulting explosion in the proliferation of viruses with internet connectivity making things worse. The vast majority of malware (viruses, spyware, etc) are targeted on Windows. Since a virus is a program, it will only run on a specific operating system (although in principal it is possible to devise cross-platform viruses in practice this does not seem to be a problem) Opening a file with a Windows virus on a Linux computer will not normally do damage. Virus checkers for Linux are targeted on servers that provide information to Windows client machines. The virus checker then strips out the virus on the server before it reaches the Windows client.
With most up to date operating systems, in order to install a program you have to enter the system password so unless you actually go ahead and install something you are not sure about you won't accidentally install a virus. For this reason viruses are much less likely to proliferate and so there is little incentive for virus writers. Some people say the reason there is no practical virus issue with Unix based computers (Linux, Mac, BSD) is that there are fewer of them so virus writers target the big numbers. It is also true that on average the IT literacy of Unix users is probably a good bit higher than for the average Windows user. Overall, Windows users are currently much more at risk from viruses than Unix users.
The latest versions of Windows have better security but there are still masses of viruses that will infect them if inexperienced users do silly things! There are massive commercial interests at stake so be careful about sources of information. A vendor of a particular system is going to talk up the benefits and talk down the risks related to security for their system and currently too few people are technically capable enough to give reliable advice even though many think they are. Improving the general technical knowledge of the population will reduce the risk to that population as a whole.

1.2 I can take appropriate security precautions to protect IT systems and data

Candidates should show practical capability and a responsible attitude in relation to basic security in their every day work.
Evidence: Assessor observations and day to day document files

Additional information and guidance
They should not be awarded this criterion if they do any of the following.

- Swap passwords with others
- Fail to keep their passwords secure
- Use ineffective passwords (eg the word "password" or a single key stroke)
- Download or attempt to download information that is either against local policies or is not known to be secure.

They should know that on Windows Systems up to date anti-virus software and regular checks are essential. If connected to the internet check there is a firewall between the client machine and the wider internet. Back up data and ensure backups are in a physically separate place from the source. (PLTS)

1.3 I can identify threats to information security associated with widespread use of technology

Candidates should be able to identify some specific key threats relevant to their circumstances. Relate this to safety and security in other units.

Evidence: Assessor observations and recording in day to day document files

Additional information and guidance

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

1. Technologies with very widespread take up that are directly related to communications are very likely targets for people that want to breach security. A good example is Outlook address books which can use e-mail addresses in a sort of pyramid spam. Particular care needs to be taken when using such applications.
2. The use of insecure passwords, sharing of passwords, storing user name and passwords in public web browsers
3. Leaving computers logged in while unattended especially in public places
4. People who pretend to be trusted entities in order to get personal information from users. (Phishing).Providing personal information on public networks that could enable criminals to access individuals' personal data.

Note that a lot of the technological solutions are in place and the human factor of inexperienced and under-educated users is probably more important than flaws in any particular technology. In general, the better the technology is understood the less likely the individual is to be a victim of technologically expert criminals. (PLTS)

1.4 I can take appropriate precautions to keep information secure
Since information is organised data, keeping data secure will keep any associated information secure. (see 1.2 above)
Evidence: Assessor observation and secure user accounts in practice.

Additional information and guidance
Since information can make immediate sense to a candidate whereas data need some sort of processing, greater care is needed to keep information secure. Candidates should also take particular care if entrusted to carrying sensitive information on discs, laptops and memory sticks. Such physical devices can be lost or misplaced. If sensitive information exists on a secure network, it will increase the security risk every time that information is copied to another device or server so making backup copies has a downside as well as a benefit. Candidates can use security as a focus for identifying the benefits and limitations of using ICT. Being able to copy information quickly and easily is useful but also a potential security risk.

1.5 I I can follow relevant guidelines and procedures for the secure use of IT
Candidates should demonstrate that they conform to any local acceptable use policies and procedures related to security. This can be related to other units and criteria related to safety and security.

Evidence: Assessor observation and secure user accounts in practice.

1.6 I can explain why it is important to backup data securely
Candidates should be able to explain that digital data is easy to corrupt and delete and that hardware on which the data is stored can be stolen or fail. For this reason, backups should be taken and stored on a physically separate device from the original.

Evidence: Assessor observation and spot checks of candidate back ups where relevant.

Additional information and guidance Since data can be come corrupt without the user knowing it is possible to inadvertently destroy a good backup by overwriting it with corrupt data. For this reason, especially with important data, relying on a single backup is risky. There can also be a penalty in the time taken to get work restored from a backup. Even on systems that centrally backup your work on a server, you are then dependent on other people to get it back. It is worth considering taking a separate backup e.g. to a USB key of important and often used work simply because it makes it quick and convenient to restore. This has to take into account how sensitive the information might be. One change that is taking place globally is the shift from desktop systems to the internet. Cloud computing, where all important files are stored remotely on the internet, offers the possibility of centrally backing up thousands and maybe millions of user files. This means that IT users don't have to worry about back ups and restoring files because the service provider will take care of this administration for them. They still might want to back up important and often used files personally.

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

Systems like Dropbox [5] provide a system for synchronising files on a local computer to an internet based file store. This is useful if you have several computing devices but it also provides an effective backup. Typically 2Gb or more of free storage is provided. Dropbox is also a collaborative technology because it can be used for sharing files with other people.

1.7 I can ensure that my personal data is backed up to appropriate media

The candidate should be able to show that the back up(s) applied to their work are effective e.g. it might be that the local network is backed up with tapes on a regular basis with the tapes taken off site. They should show that they are aware that their work is included and that they backup important files to USB or similar media on a personal basis.
Evidence: Assessor observation and spot checks of candidate back ups where relevant.

Moderation/verification

The assessor should keep a record of assessment judgements made for each candidate and make notes of any significant issues for any candidate. They must be prepared to enter into dialogue with their Account Manager and provide their assessment records to the Account Manager through the on-line mark book. They should be prepared to provide evidence as a basis for their judgements through reference to candidate e-portfolios. Before authorizing certification, the Account Manager must be satisfied that the assessors judgements are sound.

Source URL: https://theingots.org/community/SIL1U4X

Links
[1] http://theingots.org/community/ITQ_Unit_development
[2] http://theingots.org/community/handbook2
[3] http://www.theingots.org/community/ITQcourse1
[4] https://theingots.org/community/sites/default/files/uploads/user4/pupila.pdf
[5] https://www.dropbox.com/

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');