Gold INGOT Unit 4: IT Security

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: Being able to describe an effective backup strategy for their files.

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

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

Assessors' guide to interpreting the criteria (Unit 4)

General Information
QCF general description for Level 2 qualifications

- Achievement at QCF level 2 (EQF Level 3) reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straightforward problems. It includes taking responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance
- Use understanding of facts, procedures and ideas to complete well-defined tasks and address straightforward problems. Interpret relevant information and ideas. Be aware of the types of information that are relevant to the area of study or work
- Complete well-defined, generally routine tasks and address straightforward problems. Select and use relevant skills and procedures. Identify, gather and use relevant information to inform actions. Identify how effective actions have been
- Take responsibility for completing tasks and procedures subject to direction or guidance as needed

Requirements

- Standards must be confirmed by a trained Gold Level assessor or higher
- 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

(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');

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 20 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 (Gold Unit 4)

1. The candidate will select and use appropriate methods to minimise security risk to IT systems and data

1.1 I can describe security issues that might threaten system
Candidates should be able to describe common security issues that could affect the way their computer performs. Viruses, spyware and spam are the most common straightforward threats to performance.

Evidence: Description in web pages, assessor observations.

Additional information and guidance
Main difference between Level 1 and Level 2 is the ability to describe some of the key issues at level 2. This could be making a simple risk assessment to describe issues and their importance, perhaps linked to the work on collaborative technologies. First of all, using an operating system that is the target of most malware is a consideration. Windows is by far the riskiest environment, especially older versions but they may not have any choice in its use. Virus checkers significantly affect performance when running too. Early versions of Windows allowed programs to install themselves without reference to the users and by far 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 do no damage. While later versions of Windows are much more secure, they are still targeted by vast numbers of malware applications, and these will infect them if inexperienced users do silly things!

Unsolicited e-mail (spam) and associated attachments could be intended to damage the system or applications software and SPAM reduces performance because it takes time to download and delete. They should be able to describe why they should not reply to spam and never install or open any file attachments from any source unless they are 100% sure that the attachment is useful and from a trusted source. They should be able to describe sources of virus infections such as web sites, USB keys and discs especially on computers running Windows with older versions far more susceptible than the more recent ones. 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. Stealing a personal identity might not affect system performance but it is likely to have a significant impact on the individual.

Many news articles [5] show how dangerous lack of security can be.

Virus checkers for Linux are targeted on servers that provide information to Window's client machines. The virus checker then strips out the virus on the server before it reaches the client. For informed IT literate users, there is no practical virus problem for Linux or Apple computers that use variants of the Unix operating system design. For some reason, perhaps commercial interest, this disadvantage in using Windows never seems to get much discussion.

(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');

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 it is not possible to 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 is that there are fewer of them and so virus writers target the big numbers. It is also true that on average the IT literacy of Unix users is probably higher than for the average Windows user.

If you can achieve what you need to achieve with a Linux based computer it is unnecessary to have any anti-virus software and so system performance is unlikely to be reduced by viruses or the software needed to check for them or other malware. There are massive commercial interests at stake here 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. 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 apply a range of security precautions to protect IT systems and data
Candidates should show practical capability of a responsible attitude to security in their every day work with a degree of self-sufficiency. 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.

Evidence: Assessor observations.

Additional information and guidance
The first precaution to take is never to install anything from anything other than a trusted source. Always use a secure password. (single words that can be found in a dictionary are NOT secure passwords). Secure passwords can be memorable eg A*isBorn3 or 1NeverB# or 10%Interest. On Windows Systems install up to date anti-virus software and run regular checks. If connected to the internet check there is a firewall between the client machine and the wider internet. Back up data and ensure back ups are in a physically separate place from the source. Avoid displaying your personal details on-line. (PLTS)

1.3 I can describe the threats to information security and integrity
Candidates should be able to describe the following threats:

- 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
- The use of insecure passwords, sharing of passwords, storing username and passwords in public web browsers
- Leaving computers logged in while unattended especially in public places
- People who pretend to be trusted entities in order to get personal information from users. (Phishing)
- Files can be dumped into your system to be activated later (Trojan Horses)
- Providing personal information on public networks that could enable criminals personal access to individuals

Evidence: Description in web pages, assessor observations.

Additional information and guidance
It is relevant to link with the unit on collaborative technologies. 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)

(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');

1.4 I can keep information secure and manage personal access to information sources securely
Candidates should demonstrate practical skills in keeping information secure and managing their personal information securely in their day to day work.

Evidence: Assessor observations.

Additional information and guidance
They can describe the particular care needed if entrusted to carrying sensitive information on discs, laptops and memory sticks. Such physical devices can be lost or misplaced. Candidates should be able to describe how security is a particular 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 can describe ways to protect hardware, software and data and minimise security risk
Candidates should describe ways of protecting hardware, software and data from theft, damage or corruption.

Evidence: From their web page descriptions.

Additional information and guidance
The descriptions in the web pages should include:

- ensuring that there is a firewall in operation between their computer and the internet.
- ensuring that passwords are in place and of reasonable strength
- ensuring that data is backed up regularly
- ensuring that hardware is in a secure place

1.6 I can apply guidelines and procedures for the secure use of IT
Candidates should show that they have conformed to acceptable use policies and local guidelines for the secure use of IT.

Evidence: Assessor observations

Additional information and guidance
This work can be linked to other units where there is a need to apply AUPs and local procedures. What matters is that the assessor judges the candidate to be competent to apply guidelines and procedures in the context of practical day to day work.

1.7 I can describe why it is important to backup data and how to do so securely
The candidate should be able to describe why backups are important and the procedures they use to back up their personal data. If they are working on a network and their data is backed up for them, they should be able to describe the system and the principles of why it is used.

Evidence: From descriptions in web pages.

Additional information and guidance
Most companies that do not have a secure data backup that they can use to rebuild a broken system will go out of business quickly. Candidates need to describe some of the implications of failing to understand how important data is. As we become more reliant on digital materials, for example not writing information down on paper, so we become dependent on our computer systems functioning properly at all times. In addition, many companies have assumed that keeping their data backups in the same server room was safe enough, only to discover that a fire at the facility destroyed both their live servers and their backups. Not using some type of security facilities and procedures will result in problems and some firm will employ deep encryption algorithms on their data to make sure that if they are to fall into unsafe hands, there is little value to anyone. All of these processes and procedures need to be explained with working examples where appropriate.

(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');

1.8 I select and use effective backup procedures for systems and data
The candidate should be able to choose a back up strategy that is relevant to their particular circumstances and manage their information securely. eg it might be that the local network is backed up with tapes on a regular basis with the tapes taken off site. They can still backup important files to USB and have a system for naming different versions of files.

Evidence: From descriptions in web pages and assessor observation of carrying out the descriptions in practical every day work.

Additional information and guidance
There are different ways and means of carrying out backups and these will vary on the size of data and the nature of the data. Many systems offer either difference backups, just keeping what has changed since the last time, or incremental, adding the new data each time. Both of these have strengths and weaknesses and need to be understood before being deployed. At a personal level, candidates should be able to show that they have some processes in pace to protect their own data. They might use a cloud facility for their general data and perhaps an external USB drive for data that is important. Do they then have a copy of this? How many copies of copies is it reasonable to keep and maintain? What are the issues with keeping copies? If material is kept on CDs, for example, how long before these are no longer accessible?

1.9 I can explain the steps that I take to make sure that my use of IT does not reduce my personal security
The candidate should be able to explain that they understand how connected they are and what they can do to protect themselves from harm

Evidence: Assessor observations and reflections in web pages and journals.

Additional information and guidance

Most candidates will use a range of online systems and services. Each of these will require personal details to be used. That means that they are tracked and logged at every step of their online journey. How do they make sure that this journey is safe? There are many changes in the way the Internet is being used, especially for criminal intent [6], and candidates should keep abreast of these developments.

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 authorising certification, the Account Manager must be satisfied that the assessors judgements are sound.

Source URL: https://theingots.org/community/SIL2U4X

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/PupilFNC7.pdf
[5] http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS
[6] https://en.wikipedia.org/wiki/Dark_web

(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');

-->

(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');