Level 3 Implementing an ICT systems security policy (7266/7267-511)

www.cityandguilds.com/e-quals07
August 2009
Version 1.1

e-Quals
Assignment guide for Candidates
Assignment D

About City & Guilds
City & Guilds is the UK's leading provider of vocational qualifications, offering over 500 awards across a wide range of industries, and progressing from entry level to the highest levels of professional achievement. With over 8500 centres in 100 countries, City & Guilds is recognised by employers worldwide for providing qualifications that offer proof of the skills they need to get the job done.

City & Guilds Group
The City & Guilds Group includes City & Guilds, ILM (the Institute of Leadership & Management) which provides management qualifications, learning materials and membership services, NPTC which offers land-based qualifications and membership services, and HAB (the Hospitality Awarding Body). City & Guilds also manages the Engineering Council Examinations on behalf of the Engineering Council.

Equal opportunities
City & Guilds fully supports the principle of equal opportunities and we are committed to satisfying this principle in all our activities and published material. A copy of our equal opportunities policy statement is available on the City & Guilds website.

Copyright
The content of this document is, unless otherwise indicated, © The City and Guilds of London Institute 2009 and may not be copied, reproduced or distributed without prior written consent.

However, approved City & Guilds centres and learners studying for City & Guilds qualifications may photocopy this document free of charge and/or include a locked PDF version of it on centre intranets on the following conditions:

- centre staff may copy the material only for the purpose of teaching learners working towards a City & Guilds qualification, or for internal administration purposes
- learners may copy the material only for their own use when working towards a City & Guilds qualification

The *Standard Copying Conditions* on the City & Guilds website also apply.

Please note: National Occupational Standards are not © The City and Guilds of London Institute. Please check the conditions upon which they may be copied with the relevant Sector Skills Council.

Publications
City & Guilds publications are available on the City & Guilds website or from our Publications Sales department at the address below or by telephoning +44 (0)20 7294 2850 or faxing +44 (0)20 7294 3387.

Every effort has been made to ensure that the information contained in this publication is true and correct at the time of going to press. However, City & Guilds' products and services are subject to continuous development and improvement and the right is reserved to change products and services from time to time. City & Guilds cannot accept liability for loss or damage arising from the use of information in this publication.

City & Guilds
1 Giltspur Street
London EC1A 9DD
T +44 (0)20 7294 2800
F +44 (0)20 7294 2400
www.cityandguilds.com
learnersupport@cityandguilds.com

Contents

Introduction – Information for Candidates	2
Level 3 Implementing an ICT systems security policy (7266/7267-511)	3
Candidate instructions	3

Level 3 Implementing an ICT systems security policy (7266/7267-511) Assignment D

Introduction – Information for Candidates

About this document

This assignment comprises all of the assessment for Level 3 Implementing an ICT systems security policy (7266/7267-511).

Health and safety

You are asked to consider the importance of safe working practices at all times.

You are responsible for maintaining the safety of others as well as your own. Anyone behaving in an unsafe fashion will be stopped and a suitable warning given. You will **not** be allowed to continue with an assignment if you compromise any of the Health and Safety requirements. This may seem rather strict but, apart from the potentially unpleasant consequences, you must acquire the habits required for the workplace.

Time allowance

The recommended time allowance for this assignment is **5 hours**.

Level 3 Implementing an ICT systems security policy (7266/7267-511) Candidate instructions

Time allowance: 5 hours

Assignment set up:

This assignment is made up of **four** tasks

Scenario

You work as an IT systems support engineer specialising in IT security. A customer has just purchased a new system but is sceptical about the level of security threats that actually exist. The new system has not yet been installed.

The data contained within the customer's system is commercially sensitive and extremely valuable. Data back-ups are done once a week and back-up tapes are stored on-site.

The customer's new system covers two separate sites, half a mile apart with a wireless link between the two. Within each site there is a network using wireless, Cat 5 and fibre-optic media. There is an interactive company website with a facility to contact the company directly, via email, using an on-site mail server. Employees are allowed unlimited use of the Internet and email facilities for work purposes.

You have been asked to research a range of current threats to businesses that use email, the Internet and other electronic means of communication. You have also been asked to report on the security implications of the various transmission media in the new system and to make recommendations for improvement. Your findings will be in the form of a report that will include an overview of possible effects of these threats on the business and ways that the effects can be minimised. You will then be asked to carry out surveys and preventative actions on an IT system.

Read all of the instructions carefully and complete the tasks in the order given.

Task A

Use the narrative description of the company system organisation and available research resources such as the Internet, library etc for the following tasks.

1 Identify **four** parts of the system and organisational activities that make the system and its data vulnerable to attack, either physically or digitally. Make written notes of your findings for use in writing reports.

At least one of the threats must be a physical one. For **each** of the security risks identified, you must provide reasons why this is a risk on this particular system.

2 Write a report for the customer covering the risks to their business you have identified. The report should include

- details of the **four** weaknesses and how they could be used to disrupt the system and/or steal data
- risk levels associated with **each** mode of attack and **one** possible intended outcome for each mode of attack
- **three** different motivations of the people who may attempt to attack the company
- the likely effects **each** type of attack could have on the company's business and also that of their customers

Information should be gathered from all available sources. Information obtained should be listed with source references.

Task B

1 Make recommendations to the customer as to how the risks from each of the **four** threats identified in Task A could be minimised, including

- recommended actions/solutions proposed
- **three** key issues to consider when costing security solutions
- a relative estimate of cost (eg 'this proposal is likely to cost about x% more/less than the original')
- **two** possible impacts to the business if the recommendations are not accepted and implemented
- The importance and purpose of a defined security policy.

Task C

The customer has asked for information about what should be done in the event of a security breach on the system.

1 Give an overview of the following when gathering evidence of a breach of security.

- Preservation of evidence.
- Collection of evidence.
- Chain of custody.

2 Describe the roles and responsibilities of key personnel, in an Incident Response Team, following a major Denial of Service (DOS) attack that has disabled the company's main server. Briefly outline the effect such an attack might have on the business.

3 Outline a typical password policy **and** give reasons why such a policy should be adopted for the system.

Task D

You are required to configure a computer to access the corporate network using wireless. The computer you will be given will not have any protocols or wireless software installed on it.

1 Select, install and configure the most secure wireless networking protocol available to you.

2 Install the wireless software provided and configure the computer to access the wireless network using the most secure encryption method available to you

When you have finished working:

- Sign each document above your name and label all removable storage media with your name.
- Hand all paperwork and removable storage media to your assessor.

If the assignment is taken over more than one period, all paperwork and removable media must be returned to the test supervisor at the end of each sitting.

End of assignment

Published by City & Guilds
1 Giltspur Street
London
EC1A 9DD
T +44 (0)20 7294 2468
F +44 (0)20 7294 2400
www.cityandguilds.com

City & Guilds is a registered charity established to promote education and training