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

e-Quals
Assignment guide for Candidates
Assignment C

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

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

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

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 **three** tasks

A brief scenario should be read in conjunction with the diagram that will be given to you by your Assessor.

- Task A – Compile a report detailing the issues revealed by the security risks analysis, together with likely impacts to their business.
- Task B – Compile a series of recommendations for the company, IES, including recommendations for company policy on email and IM.
- Task C – Configure a typical workstation to protect it against threats, including the removal of insecure protocols.

Scenario

You are an IT security expert employed by an IT consultancy firm and you have been given the following assignment.

Your customer is IT-Electro Supplies Ltd (IES), a large Internet-based IT and electronics retail company. IES is revising its customer service provision and has decided to reduce its telephone call centre activity by 90%. The customer plans to introduce instant messaging (IM) and email, via its website, as the primary contact method with its customers with greater use of remote assistance for technical support. A high proportion of IES's customers are small businesses.

The customer is aware that there are security and data protection issues attached to this change and has asked for a report detailing the common high-risk issues and recommendations for minimising those risks. You are also asked to examine the configuration of a typical workstation and, assuming the system is similarly configured, to identify protocols that could cause security issues. You are then asked to remove those items, taking steps to avoid compromising system performance.

Task A – Compile a report detailing the issues revealed by the security risks analysis, together with likely impacts to their business.

1 Identify **six** parts of the system and organisational activities that are vulnerable to attack via web-based email, client based email and IM. Make written notes of your findings for use in writing reports in Tasks A and B.

2 Write a report for IES that covers the risks to their business you have identified. The report should include

- how email, IM and website access could be used to cause disruption to their on-line business
- how data could be subjected to unauthorised access and theft using these methods and what types of data might be at risk
- **seven** types of potential risks associated with email, IM and web pages
- **three** motivations of the people who may attempt to attack IES
- the likely effects each type of attack could have on the business of IES and also that of its customers.

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

Task B – Compile a series of recommendations for the company, IES, including recommendations for company policy on email and IM.

Use the information from Task A to complete the following task.

1 Produce a proposal for a company policy on employee use of email and IM for both company and personal purposes using the company's IT system. The proposal should contain

a an outline of the legal (privacy and data protection) issues and considerations surrounding email and messaging privacy covering specifically

i employee email/IM intercept

ii email retention

iii IM script retention

iv acceptable use policies

b **three** recommendations for an organisation wide policy in relation to email and IM systems

c practical proposals for email and IM security in terms of protective software and system settings.

Task C – Configure a typical workstation to protect it against threats, including the removal of insecure protocols.

For this task, you will be given a PC workstation which has email and IM software installed together with protective software such as firewall, antivirus etc. Use screen prints to record your actions.

1 Identify **and** remove all protocols likely to pose an unacceptable security risk (eg greater than TCP/IP).

2 Configure the protective software to give protection against threats arriving via
 a email (attachments and message body) – **two** threats
 b IM – **two** threats
 c website alteration (eg spoof addresses embedded in links) – **one** threat

3 Record the threats you have chosen to protect against and provide a short explanation for **each** of your choices.

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