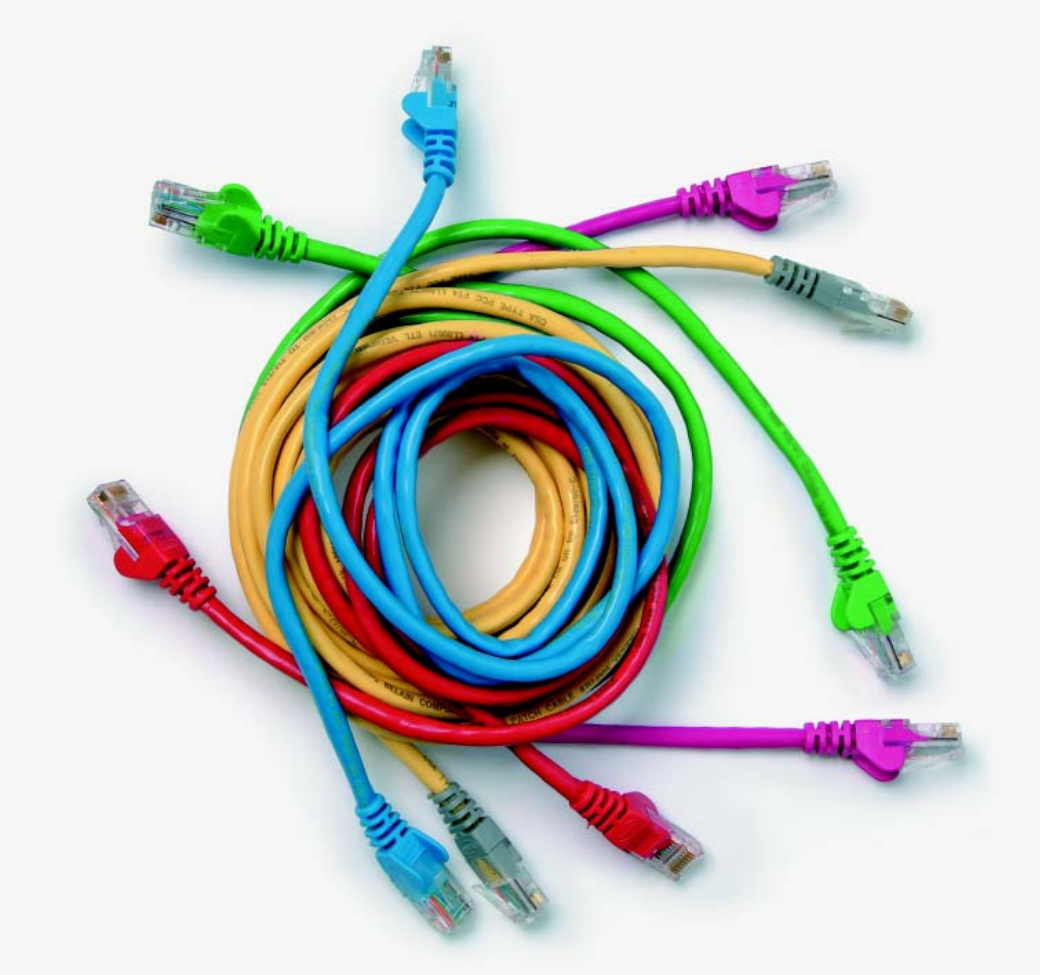
Systems and Principles Unit Syllabus

Level 2 Principles of ICT system and data security

7540-011

www.cityandguilds.com
January 2011
Version 1.0



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, City & Guilds Institute, 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

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)844 543 0000 (Centres)
T +44 (0)844 543 0033 (Learners)
F +44 (0)20 7294 2413
www.cityandguilds.com
learnersupport@cityandguilds.com

Contents

Unit 011 Principles of ICT system and data security

Unit 011 Principles of ICT system and data security

Syllabus Overview

Unit accreditation number **L/601/3508**

Credit value **6**

Rationale

This unit introduces the common types of threat to ICT systems and data and methods of protecting against them. It also covers an awareness of the applications of cryptography to ICT systems and data

Learning outcomes

There are **three** outcomes to this unit. The candidate will:

- Know the common types of threat to ICT systems and data
- Know how to protect ICT systems
- Be aware of the applications of cryptography to ICT systems and data

Guided learning hours

It is recommended that **45** guided learning hours should be allocated for this unit. This may be on a full time or part time basis.

Connections with other qualifications

This unit contributes towards the learning outcomes and assessment criteria required for the level 2 Diploma in ICT Professional Competence.

Assessment and grading

Assessment will be by means of a **set assignment** covering practical activities and underpinning knowledge.

Unit 011 Principles of ICT system and data security

Outcome 1 Know the common types of threat to ICT systems and data

Underpinning knowledge

The learner will be able to

1 Identify common types of physical threats to ICT systems and data including

Accidental damage to hardware or equipment eg

a Incorrect connections
b Drink spills
c Power failure
d Fire
e Impact damage to portable devices

Deliberate damage to hardware or equipment eg

Malicious damage

Inadequate physical security eg

a Entry locks
b Open access to servers

Loss or theft due to size or portability of devices eg

a Loss of USB drive
b Portable hard disk drive
c Laptop

2 Identify common types of electronic threats to ICT systems and data eg

a Electrostatic discharge (EDS)
b Unauthorised access to data (including removal / copying of data or code)
c Denial of service attacks
d Malware
e Adware
f Rootkits
g Phishing
h Weak or inadequate passwords
i Unsolicited e-mail attachments
j “drive by download” attack
k Failure to install Operating System or Program Security updates

3 List the security vulnerabilities associated with remote access technologies eg

a Home working
b ‘remote’ or ‘web’ e-mail access
c Wireless connections
d Mobile phones
e Web page hijack

Unit 011 Principles of ICT system and data security
Outcome 2 Know how to protect ICT systems

Underpinning knowledge
The learner will be able to

1 Identify methods of providing physical access control and security for ICT systems eg
- a Locks (entry locks, hardware locks)
- b Biometric controls (fingerprint, voice recognition)
- c CCTV
- d Shielding (cable screening)
- e Fire detection and control

2 State methods of providing electronic access control and security for ICT systems eg
- a Firewalls
- b Virtual Networks
- c Secure connection/transfer protocols
- d Wireless connection security
- e Login and password protection
- f Access rights and permissions (including limiting data access)
- g Virus, malware and spyware protection
- h Secure remote access
- i Backup and restore systems

3 Identify common types of malicious code eg
- a Virus
- b Trojan
- c Logic Bomb
- d Worm
- e Spyware

4 Identify the characteristics of strong passwords eg
- a Complexity
- b Storing (electronic / non-electronic)
- c Sharing

Unit 011 Principles of ICT system and data security

Outcome 3 Be aware of the applications of cryptography to ICT systems and data

Underpinning knowledge

The learner will be able to

1 State how cryptography can be applied to ICT system and data security eg

- a Encryption and decryption of data
- b Encryption systems (symmetric–key, public-key)
- c Authentication (users, documents, e-mails)
- d Setting up secure communication channels

2 State how Public Key Infrastructure (PKI) operates eg

- a Public keys / Private keys
- b Certificate Authority