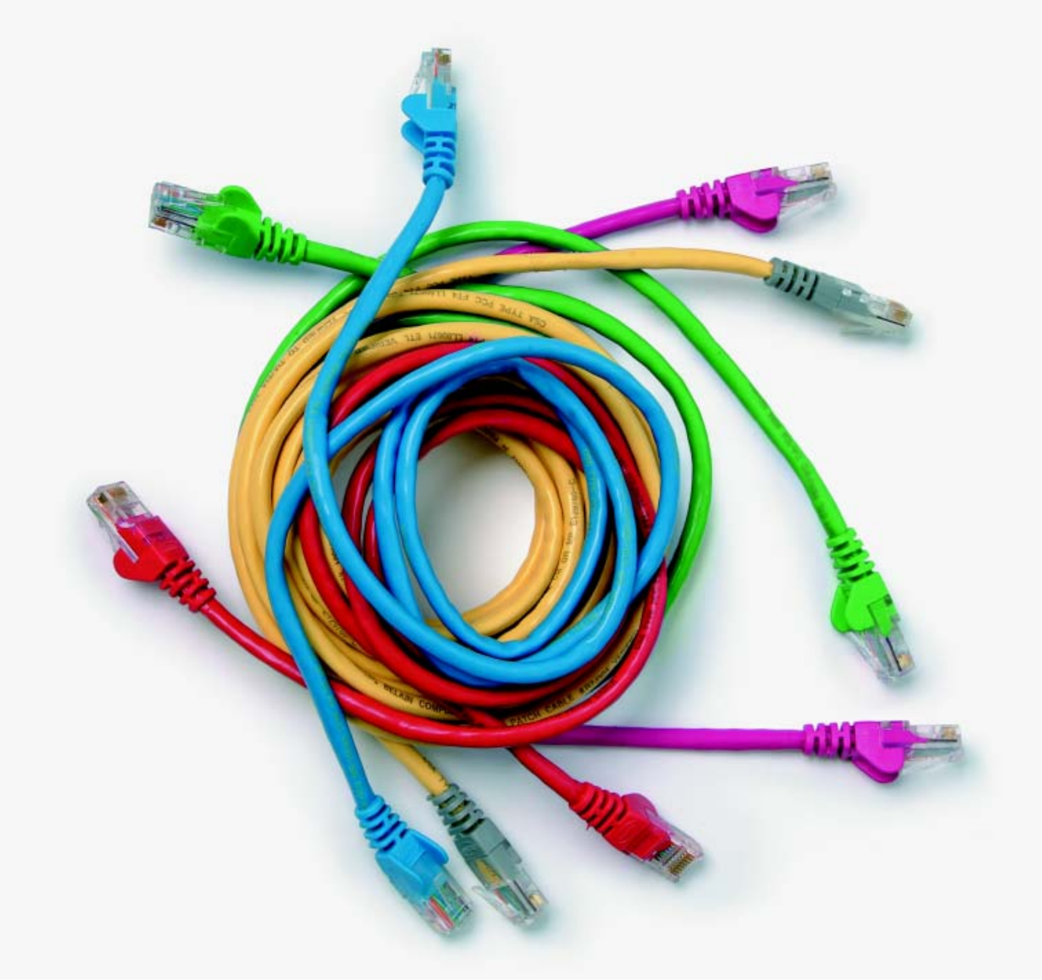
Systems and Principles Unit Syllabus

Level 3 Principles of ICT system and data security
7540-040

www.cityandguilds.com
January 2011
Version 1.0



Contents

Unit 040 Principles of ICT system and data security

Unit 040 Principles of ICT system and data security

Syllabus Overview

Unit accreditation number **R/601/3509**

Credit value **9**

Rationale

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

Learning outcomes

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

- Understand the common types of threat to ICT systems and data
- Understand how to protect ICT systems
- Understand the applications of cryptography to ICT systems and data

Guided learning hours

It is recommended that **75** 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 3 Diploma in ICT Professional Competence.

Assessment and grading

Assessment will be by means of an assignment covering practical activities and underpinning knowledge.

Unit 040 Principles of ICT system and data security

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

Underpinning knowledge
The learner will be able to

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

Accidental damage to hardware or equipment including:

a Incorrect connections
b Drink spills
c Power failure
d Impact damage to portable devices
e Unforeseen events or disasters

Deliberate damage to hardware or equipment eg
Malicious damage

Inadequate physical security including:

a Entry locks
b Hardware Locks
c Open access to servers
d Unescorted / Unbadged Visitors

Loss or theft due to size or portability of devices including:

a USB pen drive
b Portable hard disk drive
c Laptop

2 describe common types of electronic threats to ICT systems and data including:

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

3 describe the operation of common types of malicious code including:

a Viruses
b Malware
c Spyware
d Adware
e Trojans
f Logic Bombs
g Worms
h Rootkits
i Keylogger

4 explain the security vulnerabilities associated with remote access technologies including:

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

Unit 040 Principles of ICT system and data security

Outcome 2 Understand how to protect ICT systems

Underpinning knowledge

The learner can

1 describe methods of providing physical access control and security for ICT systems including:

- a Locks (entry locks, hardware locks)
- b Biometric controls (fingerprint, voice recognition, retina recognition)
- c CCTV
- d Motion Detectors
- e Shielding (cable screening)
- f Faraday Cage
- g Fire detection and control

2 describe methods of providing electronic access control and security for ICT systems including:

- 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
- j Monitoring systems (activity logging, access logs; audit logs)

3 differentiate the following Access Control methods:

- a Mandatory
- b Discretionary
- c Role Based

4 describe the characteristics of strong passwords and methods of attacking password-protected systems including:

- a Complexity
- b Length
- c Duration (mandatory changing)
- d Password History
- e Storing (electronic / non-electronic)
- f Dictionary Attack
- g Brute Force Attack
- h Social Engineering Attack
- i Keyboard Attack
- j "Man in the Middle" Attack

Unit 040 Principles of ICT system and data security

Outcome 3 Understand the applications of cryptography to ICT systems and data

Underpinning knowledge

The learner will be able to

1 describe cryptographic algorithms including:

a Hashing
b Symmetric
c Asymmetric

2 describe how cryptography can be applied to ICT system and data security in terms of:

a Confidentiality
b Integrity
c Authentication
d Non-repudiation
e Access Control

3 explain the operation of Public Key Infrastructure (PKI)

4 explain the concepts of Key Management and Certificate lifecycles

Published by 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 2400
www.cityandguilds.com

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