Qualification title: Level 2 Technical Certificate in Digital Technologies (5220-21)

Exam name: 5220-022/522 Digital Technologies - Theory Exam

Exam date: 27 Feb 2018

Exam start time: 9:30

Exam finish time: 12:00

Base mark: 80

Q	Acceptable answer(s)	Guidance	Max mks	Ref
1a	1 mark for **each** item, maximum of 3 marks. • CPU (1) GPU (1) • RAM (1) ROM (1) BIOS (1) CACHE (1) • HDD (1) SSD (1) CD-ROM (1) • USB (1) VGA (1) HDMI (1) DVI (1) SATA(1) Firewire (1) Thunderbolt (1) • Keyboard (1) Mouse (1) NIC (1)	Any of the following or any other reasonable answer	**3**	**201-1.2 A01**
1b	2 marks for **each** correct explanation, maximum of 6 marks. <u>Processors</u> • Performing mathematical calculations (ALU) (1) and stores the results in cache until required by the application (1). <u>Memory</u> • Volatile (RAM) (1) fast temporary storing of programme instructions or data (1). <u>Storage</u> • HDD/SSD Permanent long-term storage (1) of data, programs and Operating Systems (1). <u>Connection methods</u> • VGA display standard for generating images (1) and connecting display devices via specific pathways (1). <u>Input/output devices</u> • Providing communication between peripheral devices and system (1) allowing user interaction (1).	Any of the following or any other reasonable answer	**6**	**201-1.2 A02**

2	2 marks for **each** explanation, maximum of 6 marks. <u>File management</u> • Responsible for organising and keeping track of files (1) managing file systems (1) such as NTFS / FAT 32 / RAID. <u>Memory management</u> • Responsible for keeping track of every memory location (Address) (1) and allocating the address space as required by programmes (1). <u>Resource management</u> • Controlling the interaction between peripherals and the system (1) allowing multitasking (1) between programs. <u>Security</u> • Responsible for account creation allocating different privilege levels (1) and user authentication (log on/log off) (1). <u>User interface</u> • Graphical User Interface (GUI) uses icons/pointers (1) to simplify user interaction with programs (1).	Any of the following or any other reasonable answer	**6**	**201-2.1** **A02**
3	1 mark for **each** correct conversion, maximum of 2 marks. • $55_{10} = 00110111_2$ • $116_{10} = 01110100_2$		**2**	**201-3.2** **A02**
4a	1 mark for **each** risk identified, maximum of 3 marks. <u>Personal</u> • Cyber bullying (1) • Phishing (1) • Identity theft (1) <u>Organisational</u> • Loss of sensitive information (1) • Loss of reputation (1)	Any of the following or any other reasonable answer	**3**	**201-4.1** **A01**
4b	2 marks for **each** description, maximum of 6 marks. <u>Cyber bullying</u> • Do not respond or retaliate (1) to communications saving any evidence (1) for use when informing authorities.	Any of the following or any other reasonable answer	**6**	**201-4.1** **A02**

	Phishing • Do not open attachments in unsolicited emails (1) do not clink on links in emails from unknown individuals or sources (1). Identity theft • Do not disclose unnecessary personal information (1) via social media and protect the device(s) used to access social media with strong passwords (1). Loss of sensitive information • Implement strong authentication (1) throughout the organisation. Configure anti-virus / anti-malware to scan all emails (1) for infections. Damaged reputation • Educate all organisation employees in the use of social media (1) when responding on behalf of the organisation, setting and circulating clear organisational rules (1) and monitoring compliance.			
5a	1 mark for **each** principle, maximum of 2 marks. • Personal data shall be accurate and, where necessary, kept up to date (1). • Personal data processed for any purpose shall not be kept for longer than is necessary (1).	Any of the following or any other reasonable answer	**2**	**201-5.1 A01**
5b	2 marks for an explanation, maximum of 2 marks. • A business must keep its database of customers up-to-date (1) removing the details of any customer that no longer interacts (1) with the business.	Any of the following or any other reasonable answer	**2**	**201-5.1 A02**
6a	1 mark for **each** action identified, maximum of 2 marks. • Clicking on links in unverified emails (1) • Using weak passwords (1)	Any of the following or any other reasonable answer	**2**	**202-1.3 A01**
6b	2 marks for **each** explanation, maximum of 4 marks. • Upgrade and regularly maintain a spam filter (1) on the email system, disabling links in all emails that originate from outside the organisation (1).	Any of the following or any other reasonable answer	**4**	**202-1.3 A02**

	• Educate users in complying with an organisational password policy (1) enforcing password complexity through system logon processes (1).			
7a	1 mark for **each** method identified, maximum of 2 marks. • Biometrics (1) • Cypher locks (1)	Any of the following or any other reasonable answer	**2**	**202-2.1 A01**
7b	2 marks for **each** explanation, maximum of 4 marks. • Biometrics authenticate a physical characteristic (1) of a user prior to logging on to the system which is unique to that user and is pre-stored on a database (1). • Cypher locks send an encrypted electronic signal querying a fob / token (1) with the correct reply enabling the system to be unlocked (1).	Any of the following or any other reasonable answer	**4**	**202-2.1 A02**
8a	1 mark for **each** identification, maximum of 2 marks. • Network Attached Storage (NAS) (1) • Tape Drive (1)	Any of the following or any other reasonable answer	**2**	**202-3.2 A01**
8b	2 marks for **each** explanation, maximum of 4 marks. NAS The backup is performed over network media using the same network protocol (1) (TCP/IP) as other activities which could result in congestion and leading to a slow backup process (1). Tape Drive The backup is sequential, taking a long time (1) with the process usually having to be completed overnight when the system is least likely to be used (1).	Any of the following or any other reasonable answer	**4**	**202-3.2 A02**
9	2 marks for **each** description, maximum of 4 marks. System restore Where Operating System files and settings (1) are restored from a recent or an original backup (1). Archived file restore Where selected data files (1) are restored from one or more backups (1).	Any of the following or any other reasonable answer	**4**	**202-3.4 A02**

10a	1 mark for **each** method, maximum of 4 marks. • Face-to-face (1) • Email (1) • Fault reporting software (1) • Telephone (1)	Any of the following or any other reasonable answer	**4**	**203-1.3** **A01**
10b	2 marks for **each** description, maximum of 6 marks. <u>Face-to-face:</u> The ability to easily clarify information (1) received, while picking up additional non-verbal communication (1). <u>Email:</u> Allows for attachments (screenshot of a problem) to be sent (1) and a written record maintained (1). <u>Fault-reporting software:</u> Maintains an automatic audit trail (1) and allows the identification of trends (1). <u>Telephone:</u> Allows for interactive questioning / probing (1) about the issue lending itself to the use of open questioning to gather additional information (1).	Any of the following or any other reasonable answer	**6**	**203-1.3** **A02**
11	**Band 1:** **1 – 3 marks** Minimal consideration given to the role of the hardware and software. There is limited discussion of the back-up types (full / incremental / differential) proposed in the back-up strategy. The technical discussion is limited and lacks structure. **Band 2:** **4 – 6 marks** Adequate consideration given to the role of the hardware and software. The discussion of the back-up types (full / incremental / differential) proposed in the back-up strategy is appropriate. The technical discussion is adequate and structured. **Band 3:** **7 – 9 marks** The consideration of the hardware and software is comprehensive.	Indicative content • Types of back-up: ○ full ○ incremental ○ differential • Back-up ○ individual file backup ○ large data backup ○ data transfer ○ external storage backup ○ Operating System backup • Restore: ○ system restore ○ data restore • Hardware ○ backup media • Software ***For no awardable content, award 0 marks.***	**9**	**201 1.1, 1.2, 2.1, 2.2, 2.3, 3.1, 5.1** **202 1.3, 2.1, 3.1, 3.2, 3.3, 3.4** **203 1.1, 1.2, 3.1**

	The discussion of the back-up types (full / incremental / differential) proposed in the back-up strategy is detailed. The technical discussion is well developed and structured.			
12	**Band 1:** **1–3 marks** The discussion is lacking detail and structure. Use of appropriate technical language is limited and inconsistently applied. Limited consideration given to planning the documentation with a minimum of 3 elements from the indicative content being discussed. **Band 2:** **4–6 marks** The technical discussion is adequate and structured. Appropriate technical language is mostly accurate and consistent. Appropriate consideration given to the planning and production of the documentation with a minimum of 4 elements from the indicative content being discussed. **Band 3:** **7–9 marks** The technical discussion is well developed and structured. Appropriate technical language is accurate and consistent throughout. Comprehensive consideration given to the planning and production of the documentation with a minimum of 5 elements from the indicative content being discussed.	Indicative content • Local policies • Local guidelines • Available websites • Forums • User groups • Target audience • End user skills / understanding • Technical jargon • Style and tone • Use of multimedia (videos / images etc.) ***For no awardable content, award 0 marks.***	**9**	**201 1.1, 1.2, 2.1, 2.2, 2.3, 3.1, 3.3, 4.1, 4.2** **202 1.3, 3.1, 3.2** **203 1.1, 1.2, 1.3, 2.1, 2.2, 3.1, 3.2**