MODULE H SOFTWARE · H5

User management and file management: mark scheme

20 marks · OCR J277 spec 1.5.1: the purpose and functionality of operating systems: user management (e.g. allocation of an account, access rights, security) and file management (e.g. naming, allocating to folders, moving files, saving)

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. **...** means the point builds on the one before. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.5.1	Username / user ID / login name Password Access rights / permissions (to files, folders or programs) Account type / level, e.g. standard user (Own) folder / storage area for the user's files (Own) settings / desktop / preferences	**2**	1 mark per bullet, max 2. Mark the first answer on each line. Credit any other valid account item. Do not accept "a login" / "an account" alone (repeats the question). Do not accept "security" alone (NE).
1(b) J277 1.5.1	Administrator / admin (account) // an account with the highest / full access rights // an account that is allowed to create / manage other users' accounts	**1**	Accept superuser / root. Do not accept "an account with more access" alone (NE). Do not accept "manager account" / "main account" (NE) or "standard user".
2(a) J277 1.5.1	Edit vs view only: True Record of where each file is stored: True Copying removes it from its folder: False Folder inside another folder: True	**4**	1 mark per correct row. 2 ticks in a row = 0 for that row.
3(a) J277 1.5.1	Stops someone (unauthorised) from trying / guessing lots of passwords (until one works) ... so they cannot log in to the account // cannot access / open / change / delete that user's files The locked account can only be used again after it is unlocked (e.g. by an administrator / after a set time) // the user / administrator can be alerted that someone tried to log in	**2**	1 mark per bullet, max 2. Do not accept "stops hackers" / "makes it more secure" alone (NE). Do not credit answers that say locking the account encrypts the files.
4(a) J277 1.5.1	Copy (and paste) // copying (the file)	**1**	Accept "duplicate". Do not accept move / cut / save / rename.

QUESTION	ANSWER	MARKS	GUIDANCE
4(b) J277 1.5.1	Moving puts the file in the new folder / location and removes it from the original folder // after a move there is only one file Copying makes a second / duplicate file in the new folder / location and leaves the original where it was // after a copy there are two (identical) files	**2**	1 mark per bullet. One clear contrast that covers both sides (e.g. "moving takes the file out of the first folder but copying leaves it there") = 2 marks. Do not accept "copying makes it twice" without saying the original stays.
4(c) J277 1.5.1	Gives the file its name (and file type / extension) Stores / writes the file (data) to secondary storage // places it in the chosen folder (Accounts) Records where the file is stored // updates the folder (structure) to include it ... so it can be found / opened later Checks the user has the access rights / permission to save in that folder Checks / warns if a file with the same name is already in that folder	**2**	1 mark per bullet, max 2. Do not accept "stores it in RAM" / "stores it in memory" for the second point. Do not accept "saves it" alone (repeats the question).
5(a) J277 1.5.1	Each member of staff has their own user account (with a username and password) ... so the operating system knows who is logged in // who is trying to open a file The manager uses an administrator account to set / change the access rights Access rights / permissions are set for each folder / file, for each user or group of users The bookkeeper is given read and write / edit access to Accounts The planners are given no access to Accounts // the OS refuses / blocks a planner who tries to open Accounts The planners are given read and write / edit access to Clients The bookkeeper is given read-only access to Clients The planners can be put in a group, so their access rights are set once for the whole group Passwords stop one member of staff logging in as another (to get round the access rights)	**6**	1 mark per bullet, max 6. Answers that only repeat the manager's four needs, without saying how the operating system controls access (user accounts / access rights / permissions / read-only), max 2. Accept "full access" for read and write; accept "view" for read. Do not credit encryption, firewalls or anti-malware (not user or file management). Do not accept "lock the folder" alone (NE).

Total: 20 marks