01

4 marks for AO1 (understanding) and 8 marks for AO2 (apply)

Level	Description	Mark Range
4	**Level 4 High mark range** **Subject Criterion Context** A **clear understanding** shown through the use of at least **four** relevant examples that **discuss** the methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection. Examples are well supported by reasoned arguments and the detail given should explain how and why the methods\techniques would be in/effective.	10-12
3	**Level 3 Higher mid mark range** **Subject Criterion Context** A **more developed understanding** shown through the use of suitable examples that **discuss\explain** at **least three** methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection. Examples are supported by explanations of how the methods\techniques would be in/effective.	7-9
2	**Level 2 Lower mid mark range** **Subject Criterion Context** **Some understanding** shown through the use of suitable examples that **describe** at **least two** methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection. Examples are supported by limited descriptions and at least one explanation of how the method\technique would be in/effective.	4-6
1	**Level 1 Lower mark range** **Subject Criterion Context** At the higher end of the mark range there is a simple **description** about at **least one** method\technique that could be used by a company or individual to protect their devices from malware and/or minimise the damage caused by infection. The answer may not include an explanation of how the method(s) would work. Simple **statements\example(s)** of methods\techniques (for example a bulleted list) supported by no comments is limited to the middle of this range.	1-3
	No creditworthy material	0

12

Method **AO1 (Understanding)**	**Explanation** **AO2 (apply)**
Regularly back up data and test backups.	Back up data so that you can restore data that has been accidentally deleted or destroyed. It is important to test that back-ups work on a regular basis.
Secure the backups.	Make sure that backups are off site so they are not lost under the same circumstances as the main data. Also if the backups are air-gapped then this will prevent a severe malware infection getting access to the backups as there is no physical connection.
Block or remove email attachments or links.	Check links contained in e-mails and do not open attachments included in unexpected e-mails.
Disable pop-ups.	Ensure the pop-up blocker is turned on and any website screening options are also on.
Control software downloads.	Only download software, especially free software, from sites you know and trust. Or prevent software downloads completely.
Ensure software is up to date.	Make sure all software is up to date and patched to prevent any exploitation of known vulnerabilities.
Anti-virus is up to date.	Ensure anti-virus automatically updates so that the latest vulnerabilities are detected and dealt with.
Disable macro scripts.	Prevent macros from running which could cause or run malicious code.
Only allow specified programs to run.	Preventing any unknown programs running should prevent any malicious code before it gets a chance to run.
Manage the use of privileged accounts and access levels to files.	Controlling the access to files should act as an internal firewall\barrier to prevent unauthorised access or execution of programs.
Use virtualized environments\sandboxes.	Operations are carried out in a controlled and temporary working space\environment which can be easily reset without effecting anything outside of the space\environment.
Use network filtering or a firewall.	Prevent\block access into and out of the network using filtering and firewall to stop any malicious communications or transfer of viruses.
Remove the ability to use removable media.	Prevent unknown or unauthorised files to enter or leave the network.
MAC address filtering.	Can prevent access by unauthorised devices.
User training.	To educate staff in dangers of social engineering techniques and other unsafe practices.
Pen testing.	To allow organisation to understand where weaknesses may be, in order to strengthen their system security.

R. Encryption, unless it is discussed in terms of minimising damage

02	2	**3 marks for AO1 (understanding) and 3 marks for AO2 (apply)** 2 marks per method, 1 mark for stating the method, 1 mark for an explanation. • Passwords; a set of characters that is only known by the person who is being authenticated// a set of characters that is entered and compared against a database/recorded version; • Biometric; measures such as fingerprint, facial, iris, voice-print that use the user's physical features to prove who they are; • Email confirmation; sends an email which requires a valid email address and for the recipient to respond to prove the email and hence user is valid; **A.** Other methods that are not in the specification that are appropriate should also be awarded marks. Examples such as 2 Factor Authentication (2FA), Authenticator Apps, security questions.	6

Qu	Part	Marking guidance	Total marks
03	5	**4 marks for AO2 (apply)** A **maximum of 4 marks** can be awarded. **One mark** for each point and **one mark** for an expansion. Answers that are too similar to each other must only be credited once. Example responses include: • Train staff/students to be cautious of emails; ○ that come from unrecognised senders; ○ that ask you to confirm personal/financial information (over the Internet); ○ that make urgent requests for personal/financial information; ○ that are not personalised; ○ that try to upset you into acting quickly by threatening you with frightening information; • Train staff/students not to click on links/download files/open attachments (in emails); from unknown senders/sources; • Prevent students from being able to download; anything from the internet/email links; • Train staff/students to never enter personal information; in a pop-up screen; • Train staff/students not to copy web addresses (into a browser); from pop-ups; • Protect the school computers with a firewall/spam filters/anti-virus/anti-spyware software; and keep the software updated;	4

Qu	Part	Marking guidance	Total marks
04	1	**2 marks for AO1 (understanding)** Maximum of **two** marks from: • (weak) passwords are easily cracked // a program could be used to try out lots of passwords // users might choose passwords which are not strong enough // (weak) passwords can be easily guessed; • usernames/passwords may have appeared in data leak; • (if users write down/store their passwords) these can be stolen; • susceptible to shouldering; • it is difficult to verify the actual identity of the person logging in (eg compared to fingerprint/Touch/facial recognition/Face ID, multi-factor authentication);	2

Qu	Part	Marking guidance	Total marks
04	2	**2 marks for AO1 (understanding)** **1 mark** for the method and **1 mark** for a valid expansion. • A code can be sent to your phone as a (text) message/in an email/as a pop-up to one of your devices; the user then types in the code (as well as the password); any hacker would need to access the phone as well as the password; • An authenticator app on a mobile phone; this generates a code which the user uses to complete the log-in; • Use two-factor authentication/2FA // strong customer/multi-factor authentication; this asks for a second form of identification such as something you know/ possess/are; • Biometrics; (to be authenticated) reference data is compared to the individual's (unique) biometric data; • Smart cards/fobs; the user inserts a Smart Card to a reader and enters the PIN, the authentication request is then verified (using digital certificates); • Ask security / memorable question; the user is asked a question that only they know the answer to;	2

Qu	Part	Marking guidance	Total marks
04	3	**2 marks for AO1 (understanding)** Maximum of **two** marks from: • A user may forget to do updates manually; • Automatic updates mean that a computer is protected more quickly; • Automatic updates from a trusted / known (secure) source will be safe // manual updates may be from an infected source;	2

Qu	Part	Marking guidance	Total marks
05	3	**9 marks for AO2 (apply)**	9

Level	Description	Mark Range
3	Answer tackles **all** of the threats listed in the question and demonstrates a **clear** understanding of both how the threats could be exploited and how AQAware could protect themselves against the threats. Explanations are **clear** and **detailed**. **A range of relevant examples are covered** and these are clearly focused on how the company can protect its systems.	7–9
2	Answer tackles **most or all** of the threats listed in the question and demonstrates **some** understanding of how the threats could be exploited and how AQAware could protect itself against the threats. Explanations are **generally clear** but sometimes lack detail. **Some relevant examples are mentioned** and these are generally focused on how the company can protect its systems but may sometimes stray into referring to individual users.	4–6
1	Answer tackles **one or more** of the threats listed in the question and demonstrates a limited understanding of how the threats could be exploited and/or how AQAware could protect itself against the threats. Explanations may not always be clear. **Examples may be provided** but these may not always be focused on how the company can protect its systems and may stray into general points about computer security.	1–3
0	**No creditworthy material**.	0

<u>Indicative Content</u>

How the threat could be exploited:

Weak and default passwords

- hackers could use brute force methods to crack passwords
- weak admin passwords would allow hackers to gain admin level access
- default passwords allow hackers to gain access without any effort
- default / stolen passwords published online so that everyone can find them.

Misconfigured access rights

- allows staff to access areas they are not supposed to
- network admins might not know that secure areas had been breached as no-one has ‘broken in’
- staff could reconfigure network
- staff could create new user accounts to give themselves admin access.

Unpatched or outdated software

- could allow staff or hackers to exploit known weakness / flaw
- known weaknesses / flaws are published online
- once in a hacker could install malware.

How AQAware could protect themselves:

Weak and default passwords

- enforce a strong password policy, including admin accounts on all devices, across the company with passwords that are regularly changed // force users to change their passwords regularly to strong ones.
- ensure default passwords are changed on all devices
- implement biometric measures such as fingerprint / facial / retinal scans for user authentication.

Misconfigured access rights

- careful application of suitable access rights across the network reducing the level of access level of any one individual
- make sure users only have access to the data / software they need
- give read-only access instead of full access where possible
- ensure that only relevant accounts have access to change DNS files.

Unpatched or outdated software

- software patches and updates are applied regularly (automatically) to keep the systems up to date, ensuring any recently discovered bugs or security issues are patched.

A. Any sensible threat and relevant protection method

Qu	Part	Marking guidance	Total marks
06	1	**All marks AO2 (apply)** Staff could forget their password // staff can't forget biometric measure; Shouldering risk when staff entering their password // no risk of shouldering when using biometric data; Lower risk of hacking; **Max 2**	2
06	2	**All marks AO2 (apply)** Network is made available to members of the public; Won't know the MAC addresses for (most) of the devices connecting to the network;	2

Question	Part	Marking guidance	Total marks
07	**2**	**4 marks for AO1 (understanding)** **Maximum of two marks** from**:** CAPTCHA MP1. Used to stop computer programs/bots from accessing the website/creating an account; MP2. Checks the user is human (using a test that only a human can pass) // check the user is not a bot (by using a test that a bot cannot pass); MP3. (Helps to) prevent web-based database access; **Maximum of two marks** from**:** Email confirmations MP4. Send an email to a (registered) email address when an account is created (on the website); MP5. (Helps to) prevent unauthorised users (of the website) as they would also need access to the email account // confirms the user's identity by checking they have access to the (registered) email address; MP6. Stops unauthorised accounts/bots from creating accounts (for the website); MP7. Stops the creation of a high volume of accounts (for the website) and crashing the website;	4