MERIT EXEMPLAR 2022

2

NEW ZEALAND QUALIFICATIONS AUTHORITY
MANA TOHU MĀTAURANGA O AOTEAROA

QUALIFY FOR THE FUTURE WORLD
KIA NOHO TAKATŪ KI TŌ ĀMUA AO!

COMMON ASSESSMENT TASK

Level 2 Digital Technologies and Hangarau Matihiko 2022

91898 Demonstrate understanding of a computer science concept

Credits: Three

Achievement Criteria		
Achievement	**Achievement with Merit**	**Achievement with Excellence**
Demonstrate understanding of a computer science concept.	Demonstrate in-depth understanding of a computer science concept.	Demonstrate comprehensive understanding of a computer science concept.

Type your School Code and 9-digit National Student Number (NSN) into the space below. (If your NSN has 10 digits, omit the leading zero.) It should look like "`123-123456789-91898`".

[redacted]-91898

There are three questions in this document. **Choose ONE question to answer.**

You should aim to write **800–1500 words** in total.

Your answers should be presented in 12pt Times New Roman font, within the expanding text boxes, and may include only information you produce during this assessment session. Internet access is not permitted.

Save your finished work as a PDF file with the file name used in the header at the top of this page ("`SchoolCode-YourNSN-91898.pdf`").

By saving your work at the end of the examination, you are declaring that this work is your own. NZQA may sample your work to ensure that this is the case.

INSTRUCTIONS

There are three questions in this assessment, on the topics of:

- Artificial intelligence (page 3)
- Computer security (page 8)
- Complexity and tractability (page 13).

Choose only ONE question to answer. Note that parts (b), (c), and (d) of the question include options for you to choose from.

Read all parts of your chosen question before you begin. Do not repeat information in different parts of the assessment.

EITHER: **QUESTION ONE: Artificial intelligence**

(a) (i) Name a **specific** New Zealand-based company or organisation that uses artificial intelligence.

(ii) How does this organisation use artificial intelligence?

(iii) What are at least TWO advantages of this organisation using artificial intelligence?

(b) Choose TWO of the following to answer:

- What common issues are found when developing an artificial intelligence solution?
- Give an example of how an artificial intelligence is trained.
- How can you evaluate the effectiveness of an artificial intelligence?

Choice (1) – (copy and paste below)

Response

Choice (2) – (copy and paste below)

Response

(c) Choose ONE of the following to answer:

- What positive effects might artificial intelligence bring in the future?
- What negative effects are artificial intelligences currently having on people?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

Response

Weak AI refers to systems that are programmed to accomplish a wide range of problems but operate within a predetermined or predefined range of functions. Strong AI, on the other hand, refers to machines that exhibit human intelligence.

Source (adapted): http://www.differencebetween.net/technology/difference-between-strong-and-weak-ai/

(d) Choose ONE of the following to answer:

- Organisations have a choice of developing “weak AI” or “strong AI”. Explain why an organisation may choose one over the other. What are the risks and opportunities for an organisation changing from “weak AI” to “strong AI”?

OR

- The Turing test originated in 1950. How likely is it that your chosen organisation’s artificial intelligence would pass the test?
  Discuss how relevant the test is in evaluating the effectiveness of your chosen organisation’s artificial intelligence.

Choice (copy and paste below)

Response

This page has been deliberately left blank.

OR: **QUESTION TWO: Computer security**

(a) (i) Name a **specific** New Zealand-based company or organisation that has had **issues** with computer security.

(ii) What were the issues this organisation had with computer security?

had a vulnerable and outdated firewall and network that allowed them to be hacked into by a group of hackers. Their systems were all outdated which allowed for their organization to be hacked by a group of hackers. had made plans to update their computer security but later abandoned the plans because of the lack of resources that they have. Their computer security being outdated allowed for them to be an easy target for ransomware attacks. This means that the group of hackers acquired personal information from the patients, the staff and all the finances involved.

(iii) What are TWO steps the organisation took to deal with these issues?

handed over the case to the police and government to help them. They did not pay the ransomware attack and instead they chose to recover all their information that they had lost. The National Cyber Security Centre assisted by recovering all their data that had been lost. National Cyber Security System is a government sourced company and is one of the best if not the best. They ended up recovering most of their data over months. This was the biggest NZ ransomware attack as could not do much over this.

They also updated their computer security so nothing similar in the future could happen. This is so ransomware attacks and other hackers couldn't access their network and get into their firewall. Keeping it updated meant to be ahead of the hackers since their software and coding couldn't access network since their software overwhelms the hacker's software now. This allows only secured software's to be able to enter the firewall.

(b) Choose TWO of the following to answer:

- What are common issues all individuals or organisations have with computer security?
- What steps can an organisation take to protect its computer security?
- What are the signs an individual might recognise that help them identify they are being targeted by a scammer?

Choice (1) – (copy and paste below)

> What are the signs an individual might recognise that help them identify they are being targeted by a scammer?

Response

A sign could be them getting a lot of spam emails pretending to be either a company or a person trying to tempt them to click on links. These websites that have strong security over it has HTTPS or HTTP because these links have strong and up to date security. This is so that the scammer can gain access into this individuals computer system and gaining control over all their personal information and belongings. If the user's firewall is protective enough, some of the spam emails will go into the spam section but if the user's firewall is outdated then all the emails will most likely make it through.

Another sign could be popups that appear on the user's screen if they are on an unsecured website. If the user clicks on these popups, they can ultimately lose all their data and information to the scammer. It is obvious to tell which one's scams and which ones are not by looking at whether they are trying to bait you or whether the website that the user is on is a secured website with strong security.

Choice (2) – (copy and paste below)

> What steps can an organisation take to protect its computer security?

Response

A step to protect computer security is to keep the computer systems updated. Keeping this updated allows for ransomware attacks to be near impossible as the latest updates to a system or computer is not vulnerable. The older a computer security system is then the more vulnerable it is to being attacked and targeted. Hackers are continuously improving their coding and resources to be able to access companies or individual's computer systems so keeping our systems updated allows them not to be able to be hacked as the more updated adds more computer security.

Enabling two factor authentication allows the security to be much more protective. Adding this means that there are two steps to logging into an account. These could have to go and verifying a code that has been sent to a specific number or email. This makes it much more difficult for someone who doesn't own the account to login especially if they don't have access to these. This will also let the user know if someone is trying to access and login to their account and if it's not

them then they will be able to tell the company whether it’s an unidentified individual.

My school has a policy where the staff change their passwords every 45 days. This allows for only the staff to be able to login into their own account. This doesn’t make their password predictable and keeps the password unpredictable to users. All these passwords are randomized, and they each involve special characters, numbers and a capital letter. This keeps it from unidentified users or groups to be able to login making the computer network safe and protected.

(c) Choose ONE of the following to answer:

- How can the security of computers be protected against future risks?
- What impact do peoples' attitudes and behaviour have on computer security?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

What impact do peoples' attitudes and behaviour have on computer security?

Response

Human responsibility plays a factor in whether the individual is easy to hack. No matter how high an individual's computer security is, if they don't handle and use the computer appropriately then they will get hacked. This means to be able to not be gullible and trust every link you see. This all depends on the human as it is in our nature to make mistakes, but some scams and hacks are easy to prevent, and it is easy to tell whether a link is a false advertising of what they portray. With emails, if they are from bigger companies that you are connected to, but you have never received an email from them then it is best to perceive that as spam and not think whether that is the real company. Most of these attempts to scam or hack are straightforward as they will have big red flags with how they are portrayed. If an individual isn't responsible with how they handle things and they are easy gullible then it is best for larger companies to not place them in those positions where they are in exposure to that.

(d) Choose ONE of the following to answer:

- Operating systems, drivers, software, and firmware all require updates. Discuss the purpose of these different updates in maintaining computer security.
- Organisations commonly have firewalls at the entry point of the internet as well as on individual computers. Discuss why these are needed to maintain computer security.

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

Organisations commonly have firewalls at the entry point of the internet as well as on individual computers. Discuss why these are needed to maintain computer security.

Response

Firewalls are the first security of defense and they either allow or disallow what enters the computer network. If they are what allows information to be what enters and leaves then the firewall needs to be strong. If there is no firewall, then anything can enter the network. This contains viruses, spams, malware. With no firewall the network will have no computer security and the organization's network will ultimately not be able to function. The whole network's data and information will be leaked and corrupted making it impossible for the organization to exist as their finances, staff and client's information will be leaked and no one would want to work for the organization or even be a potential client for the organization. If there is a strong firewall in entry point, then the information or software trying to enter the network will be either allowed or disallowed depending on whether it is harmful to the system. Even if the firewall is just average some potential harmful software can enter the network but if there's nothing there the organization will be an easy target and be very vulnerable to being hacked. A firewall is designed to protect the computer security and what gets into the network and what gets out.

This page has been deliberately left blank.

OR: **QUESTION THREE: Complexity and tractability**

(a) (i) Name a common example of complexity and tractability.

(ii) Explain in detail why this is an example of complexity and tractability.

(b) Choose TWO of the following to answer:

- Give a practical example where it would be good for a solution to an intractable problem not to be found.
- Give a practical example where it would be good for a solution to an intractable problem to be found.
- Give a practical example of a mechanism that can be used to partly solve an intractable problem. What are its limitations?

Choice (1) – (copy and paste below)

Response

Choice (2) – (copy and paste below)

Response

(c) Choose ONE of the following to answer:

- What are some ways that complexity or tractability can be future-proofed?
- What positive or negative effects does the field of complexity or tractability have on people?

Choice (copy and paste below)

Response

(d) Choose ONE of the following to answer:

- A real-world “solution” to an intractable problem, such as route planning, includes a number of additional factors such as one-way streets. Discuss how effective these solutions need to be and how you can measure their effectiveness.
- The “travelling salesman problem” is easy to solve with only a small number of destinations. Discuss why this becomes intractable as more destinations are added.

Choice (copy and paste below)

Response

Merit Exemplar 2022

Subject	Digital Technologies Level 2	Standard	91898	Total score	05

Q2	Grade score	Annotation
(a)		The candidate chose a suitable NZ organisation that had a well-publicised security issue. The issue and resolution was well-written, but needed more detailed evidence for an Excellence grade.
(b)		Two good signs were described showing how a scammer might be targeting the user. Good suggestions were made to improve computer security. The lack of repetition in the answers to questions (a) and (b) is noted.
(c)		Though this response has some good ideas, it was weak.
(d)	M5	This answer lacked in detail and though it discussed firewalls, it did not answer the question asked. However, considering all responses holistically, the candidate provided enough for a 05 grade.