I know breaching the Code of Student Conduct diminishes my personhood and gravely violates the accepted standards of the NUS community. I respect my fellow students and will not devalue their hard work because I, Edward Ng, am a Person of integrity.

1.1

The Programme created by Adam will perform a few functions. Initially, it will create a Pop-Up Window to show a funny video of a cat and a message asking users to forward this video to their friends via email. If a user enters the User Supplied Emails and clicks on the submit button, the Programme will then attempt to retrieve the user's email login credential, scan the user's computer for the default email client and then use that email client to send out emails, with the Programme attached, based on the details supplied in the User Supplied Emails fields.

For Adam to commit an offence under Section 3 of the CMA, based on s3.1 of the CMA, Adam has to cause a computer to perform a function for the purpose of securing access and he has to know that this would be done without authority.

For the first part, to show that Adam had caused a computer to perform a function for the purpose of securing access. The computer here would be classified as the computers which the recipient of the Programme uses to open. This fits under the definition of a computer under s2.1 of the CMA as it is a data processing device with communications capabilities. Adam's Programme also fits the requirements of securing access which is defined in s2.2 of the CMA as the Programme will use the user's email client to send out emails with the Programme as an attachment. This is done after the Programme retrieves the user's credential and scans the computer for the default email client.

With reference to s2.5 in the CMA, access by a person is unauthorized if he is not himself entitled to control access of the kind in question and does not have consent to access from any person who is so entitled. From Lim Siong Khee v PP, it is found that there was a general understanding in a relationship of consumer and industry, the account holder is entitled to access the data and is responsible for control of access. In this case, the user who received the Programme is the person who provides consent to access their own email account. Adam's Programme did not receive explicit authority by the user to login into their default email and use that email account to send out emails to their friends listed. It can also be noted that the user did not give Adam's Programme explicit authority to also scan their computer for their default email client.

We then need to prove that Adam was aware that his actions were unauthorized. The act of retrieving the user's email login automatically can be used to show that Adam has met the mens rea element required. By comparing against a reasonable person who does not know if the authority had been given, any reasonable person would know that obtaining secrets such as email credentials automatically without permission would result in without authority. A reasonable person would first ask for the email credential and ask again if they are able to help send the email on behalf of the user. In the situation where the Programme cannot find the user's email login, the Programme prompting the user for their email login details might not be as clear under the mens rea criteria. However, Adam has made the Programme to first automatically retrieve user's email login credentials and only ask for these credentials as backup to continue his Programme shows that Adam knows beyond reasonable doubt that his Programme would access the user's email without authority.

This thus shows that Adam would most likely have committed an offence under s3.1 of the CMA.

1.2

To determine if a certain piece of evidence is admissible, there is first a need to show that the evidence is relevant to the case. “Relevant” is defined in the Evidence Act which states that a fact is relevant to another when the one is connected with the other in any of the ways referred to in the provisions of the Act relating to relevancy of facts. The email in question here from Adam is relevant to deciding if Adam has committed a Section 3 offence under the CMA through s14 in the Evidence Act which are facts showing existence of state of mind or of body or bodily feeling. The email can be used to determine how Adam is thinking and feeling about his plan to use his Programme to collect emails. The evidence would thus be able to show his state of mind and will be used to show if the mens rea element required in s3 of the CMA is met.

Although the email discovered is a statement that is made out of court, the email will not classify as Hearsay as the purpose of this evidence is to justify how Adam’s state of mind was to use his Programme. This evidence will not be used to justify if Adam had actually made this claim.

This discovered email would be classified as an electronic record as defined in the Evidence Act s3 since the email is a record generated, communicated, received or stored in an information system. With the assumptions that the email is authentic, meaning that it was actually Adam himself who logged into his email account to send this email and that this email has not been tempered with. Moreover, assuming that this email was discovered from the email platform itself, a third party service providing email service to it users such as Adam, we are able to use the presumptions in s116A(2) as it is generate, record and stored not by a party to the proceeding and did not generate, record or store it under the control of Adam.

The weight given to this email as evidence can be treated as it were real evidence.

1.3

Based on the Penal Code s107(1), abetment of doing of a thing is a person who instigates any person to do that thing, engages with one or more other person or persons in any conspiracy for the doing of that thing, or intentionally aids by any act or illegal omission of doing the things. For MakerLab to be considered as abetting Adam in the commission of a CMA offence, would require the same intention or knowledge as Adam, who might or might not have committed the offence under CMA, based on s108 of the Penal Code.

MakerLab has gave Adam the task of getting valid email addresses which they will then pay Adam $0.50 for each of the valid email address. Although they have the same intention of getting valid email addresses, this does not mean that MakerLab has the same knowledge as Adam on how to collect those emails. MakerLab had task Adam to collect the emails without specifying how to collect these emails and did not outright tell or instigate Adam to go through the process of unauthorised access to get these email addresses.

Therefore, MakerLab should not be considered as abetting Adam in the commission of a CMA offence.

1.4

To determine if a certain piece of evidence is admissible, there is first a need to show that the evidence is relevant to the case. “Relevant” is defined in the Evidence Act which states that a fact is relevant to another when the one is connected with the other in any of the ways referred to in the provisions of the Act relating to relevancy of facts. The accounting records in question here is relevant to deciding if Adam has committed a Section 3 offence under the CMA through s8 in the Evidence Act which are facts showing a motive or preparation for any fact. MakerLab paying Adam in advance shows that Adam is not influenced to follow through with collection valid emails addresses. This evidence, assuming that it is correct and authentic, and that it was actually Adam that received the money, can be used to show Adam’s state of mind which might show him more motivated to collect these emails addresses through any means possible after receiving payment in advance. This can help establish the mens rea element required in a s3.1 offence under the CMA.

This accounting record is classified as an electronic record as defined in the Evidence Act s3 since the email is a record generated, communicated, received, or stored in an information system. Since this accounting record is secured by a cloud based software that is operated by a third party, we can give it the presumptions in s116A(2) as it is generated, recorded and stored not by a party to the proceeding and did not generate, record or store it under the control of Adam or MakerLab.

This accounting record can be treated as it were real evidence as it is akin to a business record that MakerLab has paid Adam in advance, assuming that this record has not been tempered with.

1.5

Section 7 of the CMA is about unauthorised obstruction of use of a computer. To be classified as an offence under s7, we have to show that Mr Grouch interfered with, interrupts or obstruct the lawful use of a computer, and has to impede, prevent access to, or impair the usefulness or effectiveness of any program or data stored in a computer. We also have to show that Mr Grouch has to do the above actions knowing that he did not have authority to do so or without a lawful excuse.

By deleting all existing emails with the Programme as attachments in all staff and student of UFC email accounts, Mr Grouch did obstruct and prevent access to data stored in the user's computers such as the Programme and the effectiveness of said Programme by not allowing the users to see the cat video.

Mr Grouch, as the system administrator, might or might not also have the authority to delete emails in the staff and students email accounts and this would depend on the rights as a system administrator given to him through his role. This authority should be found in the School's Policy or other documents which lay out his roles and responsibilities as a system administrator.

Lastly, we have to show that Mr Grouch's action did not have a lawful excuse. After tracing the source of the network congestion to the Programme, Mr Grouch decided that deleting the Programme from the UFC system would be the best way to stop the network congestion. This can be claimed as a lawful excuse as a user who received the Programme will send the Programme to more users via email, based on the functions of the Programme. In some sense, this Programme can replicate and be quickly sent to other users with an exponential increase. This might quickly lead to much more network congestion and at worst system failures of the network systems if any of the network nodes become flooded with this network traffic. Thus, Mr Grouch had to act quickly and solve the problem by removing the Programme from the UFC system.

Thus, Mr Grouch would most likely not have committed an offence under s7 of the CMA.

1.6

Under the User Supplied Emails field, Adam would have access to email addresses, which might be personal email addresses or even UFC email addresses of staff or students. These personal email addresses can be classified as personal data as in the PDPA s2 as the owners of those email addresses can be identified through their email addresses. For the UFC email addresses, they are not classified as a business contact information as they are provided by the users solely for their personal purpose of sharing the Programme with their friends to see the cat video.

In this situation, Adam is acting as a contractor of MakerLab as Adam is a freelancer paid by MakerLab to collect valid email addresses. Adam is obliged to any user's request to correct their email address user s22 of the PDPA. Adam is also obliged to make reasonable effort that the email addresses collected is accurate and complete under s23 of the PDPA. He must also protect the personal data in his possession by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored under s24 of PDPA.

1.7

Firstly, Adam has to change the Programme so that it will not do any function without authority from the user. This would include scanning the User computer for the default email client, finding the user's email credentials, and sending emails with the Programme attached. The Programme which Adam will send other users should indicate clearly at each step to allow the user to authorise each step of logging into the email, and sending out the email with the Programme attached. This can be done by having a multiple step process where the user will have to press a confirmation button at each step before the Programme continues its execution. The Programme can also ask the user to input their email credentials by themselves instead of finding them. This would help gain authority for each step of the Programme execution to ensure that Adam will not commit an offence under the CMA for unauthorised access.

Adam could also include a terms and conditions area for users to agree with. This could be a checkbox for users to agree before being able to click the submit button. The terms and conditions would ask for user consent in sharing their email and the emails listed in the User Supplied Emails field for marketing sharing of the email addresses to other companies for promotional activities and other similar business activities. This would be in the aim of covering Adam under PDPA obligations related to the collection use and disclosure of personal data.

Moreover, Adam might have to limit the number of times the Programme will be automatically sent out and ensure that it is limited to 100 emails in a day, 1000 emails a month and 10000 emails a year. This is to keep in compliance with the Spam Control Act s6. His emails might fall under "unsolicited" message as per s5 of the Spam Control Act. This is mainly since recipients of the email will usually not request to receive this message or consent explicitly to the receipt of this message.

2.1

No this data breach is not a notifiable event based on s26B of the PDPA as this data breach is related to the unauthorised disclosure of personal data only within the Organisation AIC. Only employees of AIC will receive these incorrect payslips.

2.2

AIC in this situation is the Data Owners. They did sign with Acme contracts with clauses compelling Acme to provide reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to AIC personal data and the loss of any storage medium or device on which the client's personal data is stored. This is done all as part of ordinary course of business. Thus, AIC would be considered to have done their due diligence if they had followed any policy on their part to ensure that Acme followed the above terms. In this situation, assuming that they checked in with Acme before actually using the Programme, even if they had done so, Acme would also have shown them how tests had been conducted between Acme and the Vendor to identify that there are no more bugs left in the Programme. This would leave AIC none the wiser.

Acme is acting as the data intermediary in this situation. Although they did sign the contract with AIC to provide reasonable security arrangements, the mistake in the programme would show that there was a lack of protection of personal data leading to a breach of s24 of the PDPA. This is due to Acme not doing enough due diligence in checking of the Programme. The mistake in which there is a communication issue between the Vendor and Acme would be Acme's fault as they should have checked if the Programme was developed properly according to their requirements. Moreover, Acme had conducted UAT's with the vendor to rectify any outstanding issues and had confirmed that the Programme was running correctly before using it live on the 15 April 2022.

Vendor in this situation would not really classify as a data intermediary as they are not handling any data belonging to AIC. The vendor would not have any personal data to hold and protect and should not be liable to a breach under PDPA. Although their Programme would access personal data of AIC when running, the vendors themselves will not be able to collect, use, or disclose this data as the Programme would only generate emails with the password protected payslips.

2.3

Acme has to notify the individuals affected that their personal data had been disclosed without their consent. They should then immediately inform AIC about the data breach and the reasons for failure which would be due to the incorrect Programme. Acme will then have to immediately inform the vendor to stop the execution of the Programme and immediately start checking the Programme for other bugs and conduct more testing to find out why the Programme had bugs.

2.4

Yes, this is a notifiable event. A notifiable event is not concerned with the timestamp of the data that is being disclosed. In this case, a notifiable event will be decided on if there is significant scale or significant harm to an affected individual as per s26B(1) of the PDPA.

Significant scale is defined as a data breach affects no fewer than the prescribed number of affected individuals as per s26B(3) of the PDPA. This prescribed number can be found in paragraph 20.20 of the Advisory Guidelines as 500 individuals. As the breached data includes multiple clients and their employee data from 2015. This would more than likely cross the requirement of 500 individuals.

Significant harm is defined as if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual. This can be found in paragraph 20.15 where it includes the individual full name or alias or full national identification number in combination with any of the personal data in sub-paragraphs (i) to (xxv). In this case sub-paragraph 20.15(i) would be met as it is the wages, salary, fee paid or payable to the individual by any person. Thus these employee data which might include their wages.

Hence Acme is required to notify the PDPC and each affect individual affected based on s26D of the PDPA.

2.5

Acme has breached the PDPA under s25 which requires them to cease retaining its documents containing personal data, or remove the means which personal data can be associated with particular individuals as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data and no longer necessary for legal or business purposes.

As the CEO has stated, these data would be obsolete and already 7 years old. Thus these data are considered unnecessary for business purposes for Acme anymore and should not be kept.

2.6

Acme would also have to add more stringent checks before deploying any programmes on their client's live system. This can be done by creating a Standard Operating Procedure to handle with the testing of newly developed programmes.

This process should allow them to conduct more complete testing of the programme to ensure that it fulfils their business requirements and to for bugs. They can also add a process to ensure that they test the programme completely with dummy data to ensure everything works as intended before using it with personal data.

Acme can also add more security for their email service which can include whitelisting of incoming emails, and scanning of all incoming emails for any malware through the implementation of a Host Intrusion Detection System.

Lastly, Acme should promote a culture of safe browsing and secure use of computers. This can be done by creating campaigns to raise awareness. This campaign will teach employees to not fall for phishing scams by being suspicious of unexpected emails and not to click on hyperlinks within any emails or documents.

3.1

The most cost-effective method would be requiring all employees to confirm that they have read and agreed to the new policies and rules by letting them log into their individual corporate accounts and then view a copy of the new policies and rules. At the bottom it would require them to check a checkbox that indicates that they have read and agreed to the above policies. This can repeat for all the new policies and rules created.

This will work in collecting the information as logging into their individual corporate accounts means that they are authenticated since they are the only ones who know their own corporate account. This information, which includes their employee id and which policies/rules they have read and agreed to, can be stored in a database. This will fit under the Electronic Transactions Act s8 where a signature is required and this method can be used to identify the person using their corporate account and can prove their intention which is that they have read and agreed to the new policies.

Acme would then have to create written policies and procedures which will state the formation of a legal template using the information found in the database. This template would be formalised in a company policy and will not be edited after its creation to ensure that it would be retained in its original form. This would be to ensure that it would be compliant under Electronic Transactions Act s10 which requires any document, record or information to be provided or retained in its original form. The document will be considered in their original form since the document will look exactly the same as per the when the employees agree with the checkbox and formalised without any changes to fit s10(a). This will also fit s10(b) where the record is capable of being displayed to the person.

This information in the database should also be hardened to ensure that the database will not be tempered with without any proper access controls. This is to ensure reliable assurance to the integrity of the information contained in the electronic record, the database in this case.

Lastly, this database can be used as the single source of truth of whether an employee has agreed to any new policy/rules. This means that the database will be consistently acted upon and relied upon to check or update any information regarding new policies or rules. This will help to ensure that the information in the database, a form of electronic record, can be considered primary evidence that the employee had read and agreed based on s64 of the Evidence Act.