IFS4101 LEGAL ASPECTS OF INFORMATION SECURITY

FINAL EXAMINATION

Examination Period:	**27 April 2022 (24-hour period)**
Submission Deadline:	**2359 hours on 27 April 2022**
Submission Folder:	Please check your email for the hyperlink to the OneDrive folder where you will need to upload your answer file.
FORMAT:	**OPEN BOOK TAKE-HOME EXAM**

A. HONOUR CODE

Please be reminded that cheating is a violation of NUS's Code of Student Conduct. The Code requires all students to maintain and uphold, **always**, the highest standards of integrity and academic honesty. Any student who is found to have engaged in any form of cheating, plagiarism, copying and pasting answers found on the Internet, soliciting aid from anyone (e.g., by seeking help on stackexchange, reddit and other forums) **will be subject to disciplinary action by the University**.

B. INSTRUCTIONS

1. This exam may be taken at home or elsewhere. You are allowed to refer to any written, printed, or electronic material. YOU ARE NOT PERMITTED TO DISCUSS THIS PAPER OR ANY PROPOSED ANSWER WITH ANYONE.

2. If you refer to a specific legislation, case, or other secondary materials to explain a legal position that you have taken, you **must cite** that specific legislation, case, or secondary material. Quotes must be attributed by indicating their source. You may use short form referencing instead of precise citations. As an example, to cite to case law, you may use the short form *Kamal Luddin at Paragraph XXX*, instead of *Public Prosecutor v. Muhammad Nuzaihan bin Kamal Luddin [2000] 1 SLR 34 at Paragraph XXX*.

3. This exam should not take more than **THREE** hours to complete. Do not leave submission to the last minute. The exam duration of 24 hours gives you plenty of time to submit your work and check that your submission has uploaded successfully.

4. Upload your answer file to the submission folder in PDF format. Please make sure to name your file using your student ID number. DO NOT WRITE YOUR NAME ANYWHERE ON YOUR SUBMISSION.

5. **Please include a coversheet that contains the following statement written and signed in ink:**

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, [your name], am a person of integrity.

_____*[your signature]*

You may take a photograph of the coversheet and upload it together with your answer file or as a separate .jpg or .pdf file.

6. **THIS EXAM COMPRISES THREE PARTS**. Make sure you have received all three parts. You must answer all questions in all three parts.

Part	**Total Marks**
1	75
2	60
3	20
Total	**155**

7. When answering each question, make no further assumptions beyond the information you have been provided in the facts. If you need to refer to any conventions or practices to resolve issues in your answer, identify them clearly and unambiguously.

PART 1 (75 Marks Total)

Adam is a first-year student at the University of Fort Canning in Singapore (‘**UFC’**). Because of the relaxation of COVID restrictions, he wants to earn some money so that he can travel with his friends during the school break.

MakerLab is a Singapore-based company that sells electronic parts. MakerLab wants to get a list of email addresses of the UFC community so that it can send electronic newsletters to promote MakerLab products. MakerLab offers to pay Adam $0.50 for each valid email address that Adam manages to collect.

After some thought, Adam had an idea for collecting the email addresses that MakerLab needs. Adam decided to create a programme (the "**Programme**") that will display a funny video of a cute, crazy cat dancing on a banana and, after the video ends, will activate a pop-up window (the "**Pop-Up Window**") containing following message:

‘Forward this to your friends via your email to get a $5 promo code from MakerLab! Your friends will each get a $5 promo code.’

and five blank fields into which a user can key in the email addresses of her friends ("**User Supplied Emails**").

When a user enters the User Supplied Emails and clicks on the "submit’ button, the Programme will: (a) retrieve the user’s email login; (b) scan the user’s computer system for the default email client; and (c) use that email client to send out emails to each of the User Supplied Emails. Each such email will include the Programme as an attachment.

If the Programme cannot find the user’s email login, it will prompt the user for her email login details before carrying out parts (c) and (d) described above. After the Programme has caused the user’s default email client to send out emails to the User Supplied Emails, the Programme will send the user’s email address and the User Supplied Emails to MakerLab’s server. Once MakerLab receives the user’s email address and the User Supplied Emails, MakerLab sends to each of these email addresses an email that includes a promo code for $5. The promo code can only be redeemed by the owner of the email address tied to the code. MakerLab’s email also contains a statement that by using the promo code, the email address owner consents to MakerLab’s collection and use of the email address for marketing purposes.

Adam sends an email with the Programme attached to his best friends at UFC, Bucky, and Charlie, with the note, ‘Bro, check it out.’ Bucky and Charlie loved the cat video and promptly supplied their friends’ email addresses via the Programme, which caused the Programme to send emails attaching the Programme to those friends, who then shared the Programme with their friends, and so on. Very soon, almost all of the UFC community had received a copy of the Programme.

The Programme generated so much network traffic that it alarmed the system administrator, Mr. Grouch. After tracing the congestion to the Programme, Mr. Grouch decided that the best course of action was to delete the Programme from the UFC system. He programmed UFC’s email system to delete all existing emails with

the Programme as attachments that is stored in all the staff and students' email accounts. This caused consternation among the UFC community when they discovered that their emails with the Programme had mysteriously vanished from their accounts.

Imagine that you are part of an elite team working with the Deputy Public Prosecutor in the Attorney-General's chambers in charge of handling this case. The Attorney-General has asked you and your team for your opinion on Questions 1.1 to 1.6.

*1.1 Assess whether Adam committed an offence under Section 3 of the Computer Misuse Act 1993 (the '**CMA**'). (10 marks)*

1.2 Suppose you discovered an email from Adam to his friends Bucky and Charlie in which he expressed the following sentiments: 'I'm not sure if the users will object to me keeping their email addresses and their friends' email addresses.' Evaluate this evidence for its admissibility and weight in relation to deciding if Adam has committed an offence under Section 3 of the CMA. If you need to make any assumptions of fact to answer this question, please state them clearly and unambiguously. (10 marks)

1.3 Assess whether MakerLab has committed an offence by abetting Adam in the commission of a CMA offence. (10 marks)

1.4 Suppose you have secured MakerLab's accounting records (extracted from a cloud-based software that is operated by a third party) that showed the following:

'XX/XX/XXXX – advance payment to Adam to develop a multi-media animation package that could track its users: $1,000'

Evaluate this evidence for its admissibility and weight. If you need to make any assumptions of fact to answer this question, please state them clearly and unambiguously. (10 marks)

1.5 Assess whether Mr. Grouch has committed an offence under Section 7 of the CMA when he deleted the emails attaching the Programme from UFC servers. (10 marks)

*1.6 What are Adam's obligations with respect to the User Supplied Emails under the Personal Data Protection Act 2012 ("**PDPA**")? (10 marks)*

1.7 The Deputy Public Prosecutor (DPP) has decided not to file charges against Adam. You no longer work for the DPP but are working as an independent IS consultant.

Adam wants to continue doing business with MakerLab and would like your advice on what he needs to do to keep himself on the right side of the law. In dealing with MakerLab, what documentation would you recommend Adam adopt for his email collection business? Describe in detail the key provisions you would require in such documentation to protect Adam's interest. If any business practices need to be changed, please describe them, and explain why. (15 marks)

PART 2 (55 Marks Total)

Acme Pte. Ltd. is a small business based in Singapore and employs 15 employees. Acme has a single employee who handles all of Acme's IT matters. Acme's CEO knows that the protection of personal data is important, and he leaves his IT manager to handle all the technical details of protecting personal data. However, the IT manager has never been officially appointed as the data protection officer. To protect Acme's business data, Acme has adopted a confidentiality policy requiring all its employees to make sure that company data (including any client data) is always secured.

Acme supplies payroll management services to various private companies and government agencies, including the Singapore Armed Forces, Agency for Integrated Care (a government healthcare agency) and PrivateCo. In the ordinary course of business, Acme's signed contracts with all its clients have a clause compelling Acme to provide reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to the

clients' personal data and the loss of any storage medium or device on which the clients' personal data is stored.

To supply its services, Acme connects its payroll system to its clients' human resource IT systems so that it can retrieve the most up-to-date employee-related information for payroll processing. Acme's payroll system synchronises with its clients' IT systems daily to ensure that the following date saved in Acme's system is kept up to date: employee names, identity numbers (NRIC and FIN numbers), dates of birth, home addresses, telephone numbers, personal email addresses, marital status, bank account numbers, salaries, and wages, CPF contributions, days, and hours worked. Acme uses the same payroll system to deliver services to both private and government clients.

Acme uses the data that it pulls in from its clients' IT systems to calculate salaries due, calculate Central Provident Fund (CPF) payments due, generate payslips and reports required to be filed with the CPF Board (NRIC, wages and CPF sums). Acme handles payroll for more than 5,000 individuals.

In its effort to digitalise, Acme hired an IT vendor (the '**Vendor**') to develop an email generation programme called 'PayOut' (the '**Programme'**) to automate the process of preparing password-protected payslips and emailing them to the recipients' email addresses. Acme intended for the Programme to be designed to allow Acme to send payslips to recipients simultaneously in one single execution of the Programme ('**Multiple Payslip Issuance'**). However, this intention was not effectively communicated to the Vendor and the Programme was designed with the incorrect understanding that only a single payslip would need to be issued to a single employee at any one time ('**Single Payslip Issuance**'). After the Programme was developed, Acme and the Vendor conducted user acceptance tests ("**UAT**") to identify all the bugs with the Programme so that the Vendor could rectify any outstanding issues. The case scenarios included in the UAT were limited to instances of Single Payslip Issuance. The Multiple Payslip Issuance scenario was never tested.

After the Programme was developed, Acme executed the Programme for the first (and only) time on 15 April 2022 to generate and deliver payslips to the 200 employees of the Agency for Integrated Services ('**AIC**'). Believing the Programme to be capable of Multiple Payslip Issuance, Acme selected all 200 AIC employees to be issued payslips in one selection screen of the Programme and executed the process. As the Programme had not been designed to be able to properly execute Multiple Payslip Issuance, this execution of the Programme resulted in 190 of the employees receiving their own payslip as well as the payslips of other employees. By way of illustration:

(a) The first employee in the selection received only his own payslip.

(b) The second employee in the selection received her own payslip as well as the payslip of the first employee.

(c) The third employee in the selection received his own payslip as well as the payslips of the first two employees.

Ten of the 200 employees had provided invalid email addresses and did not receive any emails with the payslips. However, their payslips were included in emails generated and sent to other valid email addresses.

The payslips contained the following data: (a) name; (b) NRIC or FIN number; (c) employment number; (d) bank account number; (e) monthly basic salary; (f) detailed breakdown of current payment; and (g) year-to-date earnings and deductions.

Moreover, it turns out that the auto-generated passwords for the payslips could be easily guessed as they consisted of a combination of the date of the payslip and the name of the payslip file. As a result, several recipients were able to open the password-protected payslips belonging to others.

2.1. Is the data breach a notifiable event? Justify your conclusion. If the breach is notifiable, identify all the parties to whom the breach should be reported and justify your conclusion. (5 marks)

2.2 Justify whether each of the following have breached the PDPA: AIC, Acme, and the Vendor. If so, what parts of the PDPA have they breached? (15 marks)

2.3 What remedial steps that you would recommend Acme to undertake following the incident? (10 marks)

For the next two questions, the following facts apply:

Acme's CEO was notified that an auction on the dark web was selling access to Acme's business data, including access to their own client list. The CEO establishes that the data being 'sold' was seven years old and likely obsolete. The breached data included some client employee data (including employees of government agencies) from 2015. Forensic investigation reveals that a senior employee had downloaded a malicious email attachment, thinking it was from a trusted source.

2.4 Is this new incident a notifiable event? Justify your conclusion. If the breach is notifiable, identify all the parties to whom the breach should be reported and justify your conclusion. (5 marks)

2.5 Has Acme breached the PDPA? If so, which section? When answering this question, you do not have to repeat anything that you used to answer Question 2.2. (10 marks)

2.6 You are an information security consultant. Advise Acme on the business practices and documentation that they need to change and/or adopt to reduce Acme's risks and protect Acme from similar incidents (both the Vendor error and the phishing attack incidents) in the future. (15 marks)

PART 3 (20 Marks Total)

You are the information security manager at Acme Pte. Ltd. You have identified new information security policies and procedures that Acme needs to adopt to make sure that the company's trade secrets are properly secured. Acme has 20,000 employees and you want to make sure that the employees agree to the terms of your new policies / rules. You want to obtain evidence of their agreement electronically.

3.1 Explain the most cost-effective method that you can implement to obtain evidence of your employee's agreement that will survive any later legal challenge against the authenticity or admissibility of the evidence. The use of electronic signature applications such as DocuSign or HelloSign is not available to you as the cost is too high (at least $4.00 per document, for a total of $80,000). Explain why each step of your implementation is needed by referencing the relevant law. (20 marks).