7907ICT

Workshop Document

**This document is where you write-up the TEN weekly workshop tasks, each one of which is worth 10% of your total marks.**

# How to Approach these workshops (1 - 10)

This document lays out the ten workshop exercises to be completed each week. Either during the workshop session or at another time at your convenience. It contains detail of the task, plus a read-made template to be used when answering the questions.

This is the document that will be submitted for marking in two stages; Part A in week 6 to include workshops 1 through 5. Part B submitted in Week 11 to include weeks 6 to 10.

Key points to note:

* The output of each workshop is a **600-word written report**.
* Write your 600-word report into this workbook, accumulating them until you have completed all ten, then submit it via the Turnitin portal at the bottom of the assignment page of the course website.
* Don’t be tempted to leave doing the workshop write-up until the week the submission. It is a fact that we usually under-estimate the amount of work needed.
* As per university policy, extensions to the allowed time to submit can be granted with the necessary documentation. But please bear in mind that the IT industry is a very deadline driven profession.
* The workshops follow a similar format. Once you become familiar with the process, you should be able to work through the ten workshops over the duration of the course.
* The workshops can be completed individually or in discussions with groups of 2-4 students. Your submission will be an individual one, not a group submission.
* Ensure your report has clear headings for each.
* Try to do one workshop write-up per week.
* Avoid directly copying and pasting information from online sources, including generative language models like ChatGPT or other.

# Module 2: Developing an Ethical Hacking Policy

**<Your Exercise Title>**

### Introduction

As a CISO, I should ensure that the cybersecurity in our system is at highest level as we are a financial company, any accident, invasion or data breach may cause serious consequence and huge amount of money. So, I would like to develop an ethical hacking program to find out the vulnerabilities in our system and fix it before the potential attackers know it. However, there are some risks and challenge in implementing such an ethical hacking practice, so I must make a very detailed blueprint to avoid any accident as much as possible.

### <content>

#### <scope and objective>

The aim of this ethical hacking program is to find the defects and test the resilience of our systems. Thus, anything that is not related to our goal should be excluded as we should lower the risk as much as possible. Specifically, we want to check our access control and identity management to ensure that only the person who is authorized can access our system. Furthermore, operating systems security, network security and database security are also included in this project.

#### <Roles and responsibilities>

There are many roles in our information security office. In this program, we will assign roles such as penetration testers, who will try to hack in our system with permission and must follow the policies in the whole process, a program director, who will supervise the activities and respond to superior officer, and a cybersecurity consultant, who has rich experience in the field and will provide us advice for improvement. There are some other roles outside of our information security office, such as legal team, we will consult with them to ensure that our activities are fully aligned with the related laws and regulations.

#### <Implement process>

In the initial step, we have to draft a consent and authorization document which should include the scope and purpose of this program, responsibilities, and legal compliance, then submit it to the related department for approval. After getting approval, we can start our program. Our ethical hackers are going to use their techniques and knowledge to invade our system through all potentially vulnerabilities we might have such as WIFI network, devices with Bluetooth, control panel password, fishing email or even by social engineering. In this step, our respond team will be standing by, if an incident happens, they will start the plan we have made for remedy, like shutting down our power to terminate the hacking activity, notifying related stakeholders and superior officers. This process will be lasting for 30 days, 24/7, without any break. We design it in this way because the real hackers always hack in your computer or system at unexpected time and with creative approaches. Hence, I think it’s a good practice to set limit as less as possible for real-life scenarios.

#### <Reporting>

After the hacking activity, we will list all the vulnerabilities founded in this program and analyse it with our cybersecurity consultants to find out the reasons and improve it. At the same time, I will audit and inspect the record of the whole process to make sure all our activities comply with the policies, terms and regulations. Then, we will summarise the report and send it to the CEO.

### Conclusion

This ethical hacking program it to help our organisation prevent the potential invasion of our system in the future. As I said in the beginning, we are a financial institute, so a cybersecurity incident could cause huge loss, millions, billions of dollars, or even more. It’s impossible to make any physical or virtual system absolutely safe, because the technology evolves every year, or maybe faster. For example, in the field of Cryptography, it’s nearly impossible to crack a 20 digits password encrypting in SHA-512 with brute-force attack approach, as the time it requires for computing is way more longer than the earth lifespan. But as the rapid development of Semiconductor industries, the computility of GPU and CPU grows exponentially, so it’s hard to say these encryption methods we apply these days will still be safe after 10 years. However, we don’t need to be too worried about it, as long as we keep the core spirit of cybersecurity, that is, continuous improvement, I believe the justice parties will always win in the end.

### References

<Use APA referencing style>

<References not included in wordcount>