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 3: Data Breach Response Plan

**<Your Exercise Title>**

### Introduction

### <content>

#### <Key roles and responsibilities>

A data breach response team requires agility very much so that we can mitigate the loss of data breach incident. We have a team leader, who is responsible for leading the team, integrating ideas, assigning tasks and reporting to senior management. Two Risk management supports, whose job is to assess the risks from the breach. A Legal support, who is in charge of identifying regulations and laws related to us. 3-5 IT supports, they are responsible for establishing the cause and impact of a data breach that involved ICT systems, recovering data and making sure our system is secure.

#### <response>

A data breach response team should develop various SOPs for incidents in different scenarios so that we can respond to the incidents as fast as possible. In general, it’s a good practice to follow these 4 steps to respond to a data breach incident, that is, contain, assess, notify and review. The purpose of contain process is to prevent the scale-up of the harm that is made already, like when we are bleeding, we always keep pressure on our wound to stop bleeding so that we can avoid the risks caused by excessive bleeding. In this step, we can shut down the system and revoke most computer access privileges to cease the on-going data breach process. Second step is assess, it helps us identify the risks and find solutions for it. In this step we have to evaluate the risks and impact by collecting detailed information, then we could have a clear understanding of how it happens and the potential harm which could affect our system, organisation or customers. Next step is notify, it’s necessary to notify related stakeholders about the data breaches so that they can take some actions to protect themselves, for example, they can change their password and apply multi-factor authentication to prevent the potential breaches in the future. The final step is review, this is a critical step as if we don’t examine our vulnerabilities and fix it, then it might happen again and again which is not a good practice. In this step, we have to analyse the incident thoroughly and product a report and develop a prevention plan to avoid data breaches incidents in the further.

#### <OAIC>

OAIC stands for Office of the Australian Information Commissioner, which is responsible for legislating privacy regulation and information policies and providing data protection guidelines to organization. When serious data breach incidents happen, including unauthorized access into database or disclosure of personal information, we should notify OAIC as soon as possible. In some cases, we should notify some third parties as well, such as related bank, financial institutions, educational institutions or hospitals. It could help the harm keep scaling-up.

#### <Other actions>

In the discussion above, we ignore the human factors in this scenario, while acknowledging that human error and behaviours play a critical role in both the occurrence and response to data breaches. Thus, if we have additional resources, we may use it to train our employees so that we can reduce the probability of data breach caused by individuals.

### References

<Use APA referencing style>