Names:
Wong Ann Yi (1004000)
Liu Bowen (1004028)
Tan Chin Leong Leonard (1004041)

Exercise 1

Classify each of the following as a violation of confidentiality, of integrity, of availability or of some combination thereof.

a) John copies Mary's Foundations of Cybersecurity homework.
Answer:
Confidentiality – because the information is not meant for John.
Availability – because John has access to information of Mary which he should not have.

b) Paul crashes Linda's iPhone remotely through Wi-Fi.
Answer:
Availability – because Paul gains unauthorized access to Linda's iPhone.

c) Carol changes the amount of Angelo's check from 1B to 100B.
Answer:
Integrity – Carol changes the original data and breaches its consistency, accuracy and trustworthiness
Availability – Carol gain unauthorized access to the check however, if Carol is a bank teller and has access to the check as part of her work, it is not a breach.

d) Gina forges Roger's signature on a deed.
Answer:
Integrity – the original data is changed to affect its accuracy.
Availability – if the deed is secured in a safe and Gina forcibly gain access to the deed by breaking the safe.

e) Jonah obtains Peter's credit card number and has the credit card company cancel the card.
Answer:
Confidentiality – the credit card number is confidential and not publicly known to Jonah
Integrity – Carol breach integrity of the card by changing the status of Peter's credit card.

e) Henry guesses Julie's twitter password and tweets on her behalf.
Answer:
Confidentiality – Henry should not have possession of Julie's password
Integrity – Henry change the contents of Julie's tweets which changes the accuracy of the contents
Availability – Henry gains unauthorized access to Julie's twitter account and send "fake" information.

Exercise 2

With the following mechanisms being implemented, state what policy or policies they might be enforcing and what informal security requirement might have inspired such policies.

a) A password changing program will reject passwords that are less than five characters long or that are found in the dictionary.
Answer:
Policy of password – follow the National Institute of Standards and Technology (NIST) password guideline. Periodic password changes, length of words, avoidance of common words, not repeated password
Informal requirements include: never write password on a piece of paper, do not use your birthday as password and others words related to self.

b) The login program will disallow logins of any students who enter their passwords incorrectly three times.
Answer:
Policy – limited attempted password times in order to prevent attacker from using Brute Force attack mode.
Informal requirement – use a password tool to remember password (example: password manager).

c) The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it.
Answer:
Policy – student cannot copy files from another student's homework folder
Informal security – individual homework is confidential and plagiarism is a serious offence.

d) When too many connections to Facebook are detected from students enrolled to the Foundations of Cybersecurity class on Fridays from 7:00 PM to 10:00 PM, bandwidth should be throttled.
Answer:
Policy – students are not allowed to surf casually during class hours. Students must pay attention to lecturers.

f) eDimension will stop accepting homework submissions after the due date.
Answer:
Policy – homework submission deadline is not to be breached, all students must submit homework on time.
Informal security – every student should have the same fair amount of time to complete the homework.

Exercise 3

The aphorism “security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.

Answer:
One example of hiding information which does not add appreciably to the security of a system. For example, if one is to hide his password in text file buried deep into several directories may be secured but given time and sufficient computing resources, one can easily use “search” to find out the password.
The other opposite example is: when the password is being encoded with simple method such as the Caesar cipher and stored in the drive, an ill-intention person will not easily decode it and use the password.

Exercise 4

Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write Bob's file bobrc, but Alice can only read it. Only Cyndy can read and write her file cyndyrc. Assume that the owner of each of these files can execute it.

a) Create the corresponding access control matrix.

	alicere	bobrc	cyndyrc
Alice	own, execute	read	
Bob	read	Own, execute	
Cyndy	read	read, write	own, read, write, execute

b) Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix and spell out the commands needed to perform these changes.

	alicere	bobrc	cyndyrc
Alice	own, execute	read	read
Bob		Own, execute	
Cyndy	read	read, write	own, read, write, execute

```
Command grant_read_file(Cyndy, cyndyrc, Alice)
        if own in a[Cyndy, cyndyrc]
        then
                enter read into a[Alice, cyndyrc]
        end
Command grant_delete_file(Alice, alicere, Bob)
```

```
    if own in a[Alice, alicere]
    then
        enter read from a[Bob, alicere]
    end
```

Exercise 5

Answer:
Consider the set of rights {read, write, execute, append, list, modify, own}.

a) Using the syntax in Section 2.3 of Bishop's, write a command delete all rights(p,q,s). This command causes p to delete all rights the subject q has over and objects.
Answer:

```
command delete_all_rights(p, q, s)
    if own in a[p,s]
    then
        delete read from a[q,s]
        delete write from a[q,s]
        delete execute from a[q,s]
        delete appends from a[q,s]
        delete list from a[q,s]
        delete modify from a[q,s]
end
```

b) Modify your command so that the deletion can occur only if p has modify rights over s.
Answer:

```
command delete_all_rights(p, q, s)
    if modify in a[p,s] and own in a[p,s]
    then
        delete read from a[q,s]
        delete write from a[q,s]
        delete execute from a[q,s]
        delete appends from a[q,s]
        delete list from a[q,s]
        delete modify from a[q,s]
end
```

c) Modify your command so that the deletion can occur only if p has modify rights over s and q does not have own rights over s.
Answer:

```
command delete_all_rights(p, q, s)

    if modify in a[p,s] and own not in a[q,s] and own in a[p, s]

    then

        delete read from a[q,s]
```

```
        delete write from a[q,s]
        delete execute from a[q,s]
        delete appends from a[q,s]
        delete list from a[q,s]
        delete modify from a[q,s]
end
```