INFO2 3.2.5 Safety and Security of ICT Systems

1. (a) Using ICT examples, explain the difference between malpractice and crime (4)
(b) Describe **one** method of reducing malpractice. (2)
(c) Describe **one** method of reducing crime. (2)

1 Mark must be given for the example
(a)
- ***Principle that malpractice is concerned with bad or incorrect practice (1)***
- ***actions within the company or organisation/caused by own staff (1)***
- ***not following procedures/internal rules/code of practice (1)***
- ***Example (1)*** ***2 marks***

- ***Crime is concerned with illegal activities/against the law (1)***
- ***frequently caused by people from outside the organisation/but may beown staff too (1)***
- ***Crime is actions that are .without permission. or .unauthorised. (1)***
- ***Example, e.g Hacking (1)***

DO NOT ACCEPT NON ICT ANSWERS SUCH AS MEDICAL ***2 marks***

(b)Password Protection. Users of a system should keep strong passwords, change them regularly and should not deliberately disclose them. (Or similar to describe clerical procedures) ***2 marks***
(c) **(<u>DESCRIBE one of these methods</u>)**
Biometric passwords e.g. retina scan, thumb print, voice recognition
  Swipe cards/keys for access to system e.g. for keyboard
 Access rights/levels
  Firewall
 Encryption
 Data stored on a computer/workstation that cannot be physically be/ accessed e.g. data stored on a standalone computer in a locked room ***2 marks***

2. An employee who copies a piece of software and takes it home. The employee has committed a crime.
(a) Give two other examples of crime involving the use of ICT. (2)

- ***unauthorised access to material without any intent to do anything other than just gain access. An example would be the student who gains access to the administrative side of a college network or to another student's user area. The person who tries to get into a system just for the sake of it.(1)***
- ***unauthorised modification of computer material/ The code or data is actually changed rather than simply viewed and used. For example changing the balance in a bank account/ altering someone's credit status/ changing an examination mark.(1)***

(b) Give two ICT examples of malpractice. (2)

- ***(b) Users not leaving the computer logged on/leaving workstation unlocked***
- ***Create levels of access/ use passwords (1) so users only have access to data that they need for their job/ prevent modifications or deletions of data(1)***
- ***Have automatic save functions built into software to prevent data loss in event of system failure (1)***

3. People who access computer systems without authorisation can be prosecuted under the Computer Misuse Act.
(a) State and give an example of, each of the three sections of the Computer Misuse Act.
(b) Explain why few companies ever prosecute people under the Computer Misuse Act.
Independent marks
a) unauthorised access to material without any intent to do anything other than just gain access (1). An example would be the student who gains access to the administrative side of a college network or to another student's user area. The person who tries to get into a system just for the sake of it.(1)
unauthorised access with intent to commit or to facilitate commission of further offences(1). For example accessing bank records with the intent of committing fraud. Accessing personal details with the intent of committing blackmail.(1)
unauthorised modification of computer material/ The code or data is actually changed rather than simply viewed and used (1). For example changing the balance in a bank account/ altering someone's credit status/ changing an examination mark.(1)
b) Fear of effect on customers/reputation (1) if think their data/system is unsafe (1)
(6 marks) (2 marks)

4. One of the biggest threats to an organisation's ICT systems can come from the organisation's own employees. Discuss this statement including in your answer examples of how employees can be a threat and what measures the organisation can take to protect their systems from these threats. (5)

Internal threats are from within the company or organisation / caused by own staff(1)
Can accept theft of components or hacking as an example or any illegal activity - it is not just malpractice. Issues and Examples
Procedures for using disks/virus checking/ prevents employees introducing virus onto network (1)
Auto save/ confirmation of delete/ other software functions designed to prevent loss/corruption of data from careless mistakes (1)
Passwords/Access levels to prevent unauthorised modification/copying of data (1)
Guidelines on working practice to prevent health and safety issues with employees/ loss of staff from illness etc (1)
Good pay/benefits prevent loss of experienced/vital staff (1)
Code of conduct to prevent.......(1)
Training of staff to prevent misuse/accidental mistakes (1)
<u>Total:25</u>