Date :

Page No. : 1

0309 - MJS - 18CE1009 - Shivam Kendre

Q.1]

1) 1] Recognize an ethical issue :-
   i) Could this decision or situation damage someone or some group?
   ii) Does this decision involve a choice between a good and a bad alternative?
   iii) Does this issue involve more than legal considerations? if so, in what way?

2] Get the facts :-
   i) what are the relevant facts of the situation?
   ii) Do I have sufficient information to make a decision?
   iii) Which individuals and/or groups have an important stake in the outcome?
   iv) Have I consulted all relevant persons and groups?

3] Evaluate alternative actions :-
   i) Which option will produce the most good and do the least harm? (the utilitarian approach)
   ii) Which option best respects the rights of all stakeholders? (the right approach)
   iii) which option treats people equally or proportionately? (the fairness approach)

0309_mis_18cflo09_Shivamkendre

4] Make a decision and test it
i) Considering all the approaches, which option best adresses the situation?

5] Act and reflect on the outcome of your decision.
i) How & can I implement my decision with the greatest care and attention to the concerns of all stakeholders?
ii) How did my decision turn out, and what did I learn from this specific situation?

0309_MIS_18CE1009_Shivembendre

Q.1]
2) Information Security Threats :-
Information security threats come in many different forms.
Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage and information extortion.
Most people have experienced software attacks of some sort. Viruses, worms, phishing attack and Trojan horses are a few common example of software attacks.
The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field.
Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information through social engineering.

Responses to threats :-

1) Reduce/ mitigate :- implement safeguard and countermeasures to eliminate vulnerabilities or block threats.
2) Assign/ transfer :- place the cost of threat onto another entity or organization such as purchasing insurance or outsourcing.

0309 - MIS - 18CF1009 - Shivam Kendre

Q.2]

1] Computer Based information System (CBIS) is an information system in which the computer ~~says~~ plays a major role. Such a System consists of the following elements

1) Hardware :- The term hardware refers to machinery. This category includes the computer itself, which is often referred to as CPU and all its support equipment's. Among the support equipment's are input and output devices, Storage devices and communications devices

2) Software :- The term software refers to computer programs and the manual (if any) that support them. Computer program are machine readable instructions that direct the circuitry within the hardware parts of the computer based information system (CBIS) to function in ways that produce useful information from data. Programs are generally stored on some input/output medium - often a disk or tape

0309_mis_18CE1009_Shivam Kendre

3) Data :-
Data are facts that are used by program to produce useful information like programs, data are generally stored in machine readable from on disk or tape until the computer needs them.

4) Procedure :-
These are policies that govern the operation of a computer system.

5) People :- every CBIS needs people if it is to be useful. this is most influence the success or failure of information system