CSC 201 Week Nine Lecture Note

SECURITY AND CONTROLS

Definition:- The protection of data from accidental or deliberate threats which might cause unauthorized invitation, disclosure or non-availability of services.

- The concept of PRIVACY is closely related to the idea of confidentially, or the need to prevent unauthorized disclosure of data

- Privacy is the right of the individual to control the use of information about him or her including information on financial status, health and life style

Lightning and storms pose an additional threat, as they can play havoc with power supplies, causing power failure couple with power surges as service are restored. One way of combating this is by the use of uninterrupted power supply (UPS). This will protect equipment from fluctuation in the supply. Power failure can be taken care of, with the use of a separate generator. Man-made problem arise largely through lack of proper training for users or carelessness minor crashes, paper jams, jammed floppy disk and so on, can easily do more harm than good. Office accidents such as spilled drinks due to absent-mindedness, or get over enthusiastic or simply to play the fool.

Proper training and the encouragement of sensible attitudes, also good office layout and a tidy desk policy are very helpful.

PASSWORD

- This is a set of characters which may be allocated to a person, a terminal or a facility, which are required to be keyed into the system before further access, is permitted.
- Password can be applied to data files, program files and to parts of a program.
- One password may be required to read a file, another to write new data and third if both operations are to be permitted.
- It is important to remove any standard password that come along with the system to guard against external penetration of the security system since such common password is known to people in the industry.

- The main drawback to using password systems is that they rely upon users to use them conscientiously. Password needs to be random since the easily remembered passwords are also highly predictable.
- Anyone who knows the authorised users well can often guess their passwords. Authorised user may tell an unauthorised person what the password is perhaps through carelessness.
- Password is often left in plain view or 'hidden' beneath or inside desk drawers where virtually anyone could readily find them.
- A password system requires both a software system and strong organisational policies if its is to be effective.

NETWORK CONTROLS

- In a system of networked PCs, individual PCs will generally have their own hard disk and also be able to access data stored on a 'server' computer, to which all other PCs are connected, and possibly to data on the PCs hard disks.
- Such system can be set up so that some files on the server cannot be seen at all for certain PCs and others can be opened and inspected but not altered.
- This form of logical access control is operated via the network operating system, which is set up to allow different levels of access to different PCs.