Practical No. 1

Aim: To study various legal, ethical and professional issues in cyber and information security.

Practical No. 1

Aim: To study various legal, ethical and professional issues in cyber and Information security.

Theory:

Ethical and legal Issues:

Many ethical and legal issues in computer security system seem to be in the area of the individual's right to privacy versus the greater good of a larger entity (eg. a company, society & etc.)

For example:

- tracking how employees use computer,
- crowd surveillance,
- managing customer profiles,
- tracking a person's travel with passport.
- Location tracking so as to spam cell phone with text message advertisements and so on.

A key concept in resolving this issue is to find out is a person's expectation of privacy.

Classically, the ethical issues in security systems are classified into the following four categories:

Privacy: This deals with the right of an individual to control personal information.

Accuracy: This talks about the responsibility for the authenticity, fidelity and accuracy information.

Property: Here we find out the owner of the information. we also talk about who controls access.

Accessibility: This deals with the issue of the type of info. an organisation has the right to collect. And in that situation, it also expected to know the measures which will safeguard against any unforeseen eventualities.

Privacy is the protection of personal or sensitive information. Individual privacy is the desire to be left alone as an extension of our personal space and may or may not be supported by local regulations or laws. privacy is subjective. Different people have different ideas of what privacy is and how much privacy they will trade for safety or convenience.

when dealing with legal issues. we need to remember that there is a hierarchy of regulatory bodies that govern the legality of information security.

- Internation : International cybercrime Treaty.
- Federal : eg. FERPA, GLB, HIPAA, DMCA, Teach Act, etc.
- State : eg. UCITA, SB 1986 etc.
- Organization : eg. computer use policy.

The Ten commandments of computer Ethics

From The Computer Ethics Institute.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use propiesary software for which you have not paid.

conclusion: The study of various legal, ethical and professional issues in cyber and information security done successfully.

Name of Practical

(7) Thou shalt not use other people's computer resources without authorization or proper compensation.

(8) Thou shalt not appropriate other people's intellectual output.

(9) Thou shalt think about the social consequences of the program you are writing or the system you are designing.

(10) Thou shalt always always use a computer in ways that ensure consideration and respect for your fellow humans.

Conclusion:

Study of various legal, ethical and professional issues in cyber and information security done successfully.

Viva Questions :

(1) What are various legal issues ?

→ Data privacy and protection, cybercrime, intellectual property, cloud computing and third party liability, Government surveillance & privacy & etc.

(2) What are various ethical issues ?

→ Privacy, accuracy, property and accessibility are various ethical issues.

(3) Explain different computer ethics ?

→ (1) Thou shalt not use a computer to harm other people.

(2) Thou shalt not interfere with other people's computer work.

(3) Thou shalt not use a computer to steal.

(4) Thou shalt not snoop around in other people's computer file.

(5) Thou shalt not appropriate other people's intellectual output.