KNOWLEDGE ORGANISER L05 - Ethical, Operational and threats to Computer Systems

1.5 Understand ethical and operational issues and threats to computer systems.

- Ethical Issues
- Operational Issues
- Threats
- Physical Security
- Digital Security

Ethical Issues - Morally right or wrong in the work place.

whistle blowing - raising a concern about a wrong doing in their workplace
disability/gender/sexuality discrimination - the unjust or prejudicial treatment of different categories of people, especially on the grounds of race, age, or sex
use of information - Organisations and individuals have access to various information, laws and protections are in place in how those information is used (Check legislations)
codes of practice - is a set of written regulations issued by a professional association or an official body that explains how people working in a particular profession should behave. A code of practice helps workers in a particular profession to comply with ethical and health standards
staying safe online - Web **safety**, or online **safety** or **Internet Safety**, is the knowledge of maximizing the user's personal **safety** and security risks to private information and property associated with using the **internet**, and the self-protection from computer crime in general.
Bias - inclination or prejudice for or against one person or group, especially in a way considered to be unfair.

Operational Issues:

Organisations have to store and manage countless pieces of information, with some being far more important than others. Lying at the heart of any information system are two fundamental issues of ensuring that:

- the organisation receives the information it requires
- the appropriate member of staff receives the information

To make sure that information is managed appropriately, a number of policies and procedures have to be put in place, concerning:

- security of information - Security means that data is safe from unauthorised or unexpected access, alteration or destruction
- Backups - Organisations need to safeguard against physical data loss or processing problems
- health and safety - Regulations for using Computers (check Legislations)
- organisational policies - Organisations can have policies related to the use of information systems.
- business continuance plans -Plan in case any major part of an IT System fails
- Costs - It is important to manage the costs of IT Projects
- Increase in Sophistication of Systems - People need to be trained

Scale of Changes:

- New policies
- Staff Turn over
- New Management

Threats

Phishing - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers

Hacking - gain unauthorized access to data in a system or computer.

Virus - a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Trojan - A program that appears legitimate but performs some illicit activity when run. Such as locate password information or make the system more vulnerable to future entry or simply destroy the user's stored software and data. A Trojan is similar to a virus, except that it does not replicate itself. Often sneaking in attached to a free game or other supposedly worthwhile utility, the Trojan remains in the computer doing damage or allowing someone from a remote location to take control.

Interception - some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

Eavesdropping - unauthorized real-time interception of a private communication

data theft - the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.

Social Engineering - a fraudulent methods of tricking people in giving out private information such as passwords, can be done by any method, or person, social networking etc.

KNOWLEDGE ORGANISER

Physical security	Digital security
Locks - lock rooms when not in use **Biometrics** - Biometric security-based systems or engines store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition. **RFID -** (radio-frequency identification) access-control system allows only authorised persons to enter a particular area of an establishment. The authorised persons are provided with unique tags, using which they can access that area. **Tokens** - a security token is a physical object. A key fob, for example, is practical and easy to carry, and thus, easy for the user to protect. **Privacy filters** - From the side, others see a darkened screen, providing worry-free privacy of your on-screen information **Shredding -** for digital and paper data, to completely erase data, through the means of using a shredder.	**Anti-virus -** Software designed to detect and destroy computer viruses, protection from viruses, identity theft, spyware, spam. **Firewalls -** A firewall is a barrier between the internet and your computers or network – preventing unauthorised visits to or egress (remove data) from your systems. **Anti-spyware** - software that is designed to detect and remove unwanted spyware programs. Spyware is a type of malware that is installed on a computer without the user's knowledge in order to collect information about them **Username/password** - authorised people will have username and passwords to be able to access certain information. **Permissions -** permissions are attached to an object depend on the type of object. For example, the permissions that can be attached to a file are different from the permissions that can be attached to a registry key, allows only authorised people to have access, (read and write permissions) **Encryption** - the process of converting information or data into a code, especially to prevent unauthorized access

Safe Disposal of data & Computer Equipment

Physical Destruction:

The most secure way to destroy data—and the storage medium it's on—is by shredding it, just like your paper documents. The large, industrial shredding machines grind up the storage media into unrecognizable bits of scrap metal.

Legislations

You need to be aware that your organisation has a Duty of Care to take all reasonable measures to protect the environment. You should be aware that:

- All redundant (no economic value) computer equipment is classed as Waste.
- CRT monitors are classed as Hazardous waste.
- You must ensure your collection agents hold a Waste Carrier Licence.
- You must ensure that your waste equipment goes to a licensed disposal site.
- Your legal Duty of Care extends to when your equipment is reused, recycled or disposed of

Electromagnetic write:

In a computing context, means to render all data on a hard drive unreadable. The term is often used in reference to making data stored on a computer, smartphone or tablet inaccessible before disposing of the device

- Deleting a file only removes the file listing, anyone can still access it with the right software.
- The same is true if you reformat a drive
- The most common method of wiping a computer's data is to use a hard drive over-writer product, such as Darik's Boot and Nuke.

Overwrite data:

Overwriting is a process of writing a binary set of data in computer data storage and is a term used to describe when new information replaces old information or data. In general it writes over the previous data, hence the name

Overwrite each area of the hard disk several times.

Degauss your hard drives and backup tapes. Degaussing means to demagnetize; so, degaussing as a data destruction method magnetically erases data from your magnetic storage media, like hard drives and backup tapes.