DATA SECURITY

It is important to protect data by implementing data integrity and data security measures. Data integrity refers to the quality and content of data and ensures that information is accurate, up to date and legitimate. Data security protects data from prying eyes, criminals or malicious persons, and accidental loss or damage.

You can protect data by using software restrictions or physical restrictions

**Software Restrictions**

Software restrictions can create barriers to data corruption; restrict access to software that may contain sensitive data, or to software that can cause damage.

- **Passwords** – A password is a combination of characters that must be entered before you can access, view and edit data.
- **Encryption** - Encoding (scrambling) data during storage or transmission so that it cannot be understood by someone who does not have the encryption key.
- **Firewall** – A firewall is software that defends the weak points in a computer network to prevent hackers from gaining entry.
- **Virus protection** – a virus is a piece of software intended to cause harm to a computer or to gain access to confidential data. Viruses can:
  1. damage software
  2. slow down a computer
  3. corrupt data
  4. prevent proper functioning of programs and the software that controls hardware

Viruses are often spread by e-mail attachments from e-mail addresses that you do not recognize. Antivirus software protects against viruses.

Worms and Trojan horses are not viruses but they are malicious software:

- A worm is a piece of software that attaches to computer memory, whereas a virus attaches to a program.
- A Trojan horse does not replicate itself like a virus. It looks and behaves like a genuine program but once it is running, it allows hackers to gain access to the computer system by accessing and saving passwords.

**Physical restrictions**

- **Backup and recovery procedures** - Store a second copy of the data files and programs away from the computer.
- **Archiving** – Archiving is similar to backup, except it is more commonly used for old data
- **Biometric systems** – For security reasons, a computer or even a building can control access by storing the fingerprints of authorised persons on a central system.
- **Locks and guards with alarm system**
- **Fireproof and waterproof cabinets**
- **Proprietary software and data**- Software owned and controlled exclusively by a company take legal and business measures)
- **Good maintenance of computers**
A computer should be kept in an area that is not too hot and not too cold, and should be kept free from dust and damp.

Three ways to protect computers against power cuts and power surges:
1. a surge protector
2. a voltage regulator
3. An uninterruptible power supply (UPS)

Misuse of data – How it is done

- Piracy – the act of taking or using someone else’s work without their knowledge and permission. Piracy is illegal. Software companies try to prevent the use of illegal copies of their software by providing a product key.
- Electronic eavesdropping – eavesdropping is listening to a conversion that you are not part of without the speakers being aware that you are listening to them.
- Industrial espionage – Spying to gain information that can be used to further a purpose or that can be used against the party being spied on.
- Surveillance and invasion of privacy – Many businesses install monitoring software that keeps track of their employee’s computer use, such as their internet use. Cookies are text files put on your computer by websites you visit. They are used to store information about you, such as your location or your activities on the website. Cookies are rarely used to cause harm.

Storing inaccurate information
Inaccurate data can have damaging consequences. It can occur when:
- Incorrect data is entered into a system
- Data is accidentally changed or modified
- People make what they think are valid changes but the changes corrupt the data.

Fraud and identity theft
Computer fraud means using computer systems to carry out fraudulent activities such as:
1. stealing personal data to do fraudulent transactions
2. accessing and modifying data to benefit the modifier
3. creating fake websites and sending e-mails that require users to enter their personal details

Identity theft is where someone uses another person’s personal details to carry out transactions and other activities in that person’s name. credit card fraud is a common type of identity theft. Credit cards can be used unlawfully without them having to be physically stolen from their owners. Hackers can use the internet to track credit card details and carry out transactions.

Be careful what information you store electronically and what you make available on the internet. Be wary of internet and e-mail scams that get you to give out bank details or other data to criminals. This is sometimes called phishing.