COMPUTER STUDIES NOTES

FORM 2

**PHYSICAL CONTROL MEASURES**

Positioning a security guard to watch over a building or a room that has a computer.   
Re-enforcing weak access points such windows, doors with metal grills. Casing the computers with metal grills. Installing electrical alarm systems.   
Installing automated control access systems to buildings or rooms.   
  
**LOGICAL CONTROL MEASURES**

Use of Passwords.   
Use of firewall systems.   
Password   
  
This is a special word, code, or symbol that is required to access a computer system. Passwords are one of the weakest security links as they can be guessed, forgotten or stolen. To reduce chances of passwords being guessed, it is recommended that a strong password be used i.e. combination of characters, letters and symbols.  
  
**User Access Levels**

User access levels determine how users have access to different parts of the system depending on their role (or position) within the organization. Access levels determine what data the user can view, copy and edit.  
  
**Data Encryption**

Data encryption is the process of scrambling stored or transmitted information so that it is meaningless until it is unscrambled by the intended user. Historically, data encryption has been used primarily to protect diplomatic and military secrets from foreign governments. It is also now used increasingly by the financial industry to protect electronic funds transfers (EFT), by merchants to protect credit-card information in electronic commerce, and by corporations to secure sensitive communications of proprietary information.

**Proprietary information**

Proprietary information is information on which the producer has set restrictions on use, private modification, copying, or republishing cursor position  
Word wrap feature that automatically moves a word or a cursor to the beginning of the next line

Scrolling feature. This involves the vertical movement of text on the screen.  
HELP. It contains instructions, tips, pointers, explanations and guidance. This is achieved by pressing F1 on the keyboard or clicking help from the menu bar.  
Editing modes. Word processors have two editing modes: Insert and type over.

**Formatting**

It refers to applying various features to enhance the document's appearance. Three main formatting styles are Text, Paragraph and Page formatting.   
  
**Virus and Worms**

To control viruses and worms attacks to a computer system, antivirus software is used. Here are examples of antivirus software.  
For antivirus software to be effective, constant updates are required to manage new and up coming viruses.  
Some common examples of antivirus software include; Norton, AVG, Kerspersky  
Errors and Accidents   
The following are some of the control measures that can be used to check errors and accidents in computer systems

***i. Backups:***

These help in recovery of data/information incase of accidental or intentional deletion.

***ii. Training of computer users:***

Computers users need to be well equipped with the necessary skills to operate a computer system

***iii. Provide a comprehensive user manual :***

Any complete system should have a comprehensive documentation to assist the user understand the system at hand.

***Natural Calamities and other Hazards***To save data against natural calamities and other hazards keep backup copies of the original data/information in storage devices.  
  
**Computer Crimes, detection and Protection**

1. identify types of computer crimes 2. describe how to protect data/information against computer crimes   
Computer Crimes

Computer crimes can be of two types. It can be an illegal act perpetrated against computers and communications systems or it can be the use of computers and communication systems to accomplish an illegal act.

**Fraud**

Computer fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by: Altering computer input in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes.

Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions which is difficult to detect;   
  
**Altering or deleting stored data**

Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes. For example, a certain employee in a local university working in the salaries department conspired with other employees to alter their basic salaries. He wrote a program that instructed the payroll software to add a zero to the said employees salaries thereby increasing the figures. This went on for a while before it was detected by a hawk eyed secretary who discovered that a mere cleaner was earning more than a professor.

**Tapping**It is the illegal connection of a computer to a network with the intention of listening to data signal on transit. This is also referred to as eavesdropping  
  
**Tresspass**This refers to the process of a person without authorization intentionally gaining access to a computer and communication systems of another with the intent to copy, alter, delete data or cause a computer malfunction. Hackers and crackers are examples of tresspassers Hackers Crackers  
  
**Sabotage**

This is deliberate destruction/damage of computer systems or obstruction of normal operations of a computer system. It can involve the destruction of the computer equipment, software and data/information i.e. it can range from simple deletion, alteration to vandalism of computer parts to web site defacement.

For example, hackers accessed UNICEF website in 1998 and posted pictures of nude women.

**Detection & Protection**

***Audit Trail***This is a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions. Most accounting systems and database management systems include an audit trail component. In addition, there are separate audit trail software products that enable network administrators to monitor use of network resources.

***Log file***A log file is a file that lists actions that have occurred. For example, Web servers maintain log files listing every request made to the server. With log file analysis tools, it's possible to get a good idea of where visitors are coming from, how often they return, and how they navigate through a site. Using cookies enables Webmasters to log even more detailed information about how individual users are accessing a site.   
  
**Laws Governing Protection of Information Systems**

There has been a growing concern about the threats that computers pose to personal privacy. Most countries around the world have introduced laws to safe guard the privacy of the individual. The establishment of Data Protection Act (DPA) in most countries has the following Key Principles

* Data may only be used for the specific purposes for which it was collected.
* Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information.
* Individuals have a right of access to the information held about them, subject to certain exceptions. (for example, information held for the prevention or detection of crime).
* Personal information may be kept for no longer than is necessary.
* Personal information may not be transmitted outside the country unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.
* Subject to some exceptions for organizations that only do very simple processing, and for domestic use, all entities that process personal information must register with the government agent in charge.
* Entities holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organizational measures (such as staff training).

**Computer threats**

There has been a growing concern about the threats that computers pose to personal privacy. Most countries around the world have introduced laws to safe guard the privacy of the individual.The establishment of Data Protection Act (DPA) in most countries has the following Key Principles; click to view then close X - Data may only be used for the specific purposes for which it was collected.

- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information.  
- Individuals have a right of access to the information held about them, subject to certain exceptions. (for example, information held for the prevention or detection of crime).  
- Personal information may be kept for no longer than is necessary.  
- Personal information may not be transmitted outside the country unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.  
- Subject to some exceptions for organizations that only do very simple processing, and for domestic use. All entities that process personal information must register with the government agent in charge.  
  
***Features of a Word Processor***

Word processor features allow the user to create a document file, save it and open it again for reuse, editing or formatting. They have similar document windows with features. Examples of these features are:   
A design like a piece of paper with electronic improvements  
A blank screen  
A cursor blinking at a position where you can begin entering text  
A status bar that provides user with the current status information such as saving operation, name of file, use, current page and