TOPIC 13: SYSTEM SECURITY, ICT ETHICAL ISSUES & EMERGING TECHNOLOGIES

Sub Topic 1: **Computer System Security**

Sub Topic 2: **Privacy and ICT Ethical Issues**

Sub Topic 3: **Emerging Technologies**

Sub Topic 4: **ICT Industry**

Sub Topic 1: Computer System Security

Computer security

Refers to safe guarding computer resources, ensuring data integrity, limiting access to unauthorized users, and maintaining data confidentiality.

Computer Integrity refers to methods and procedures of ensuring that data is real, accurate and safeguarded from unauthorized user modification in the computer.

Information security means protecting information and systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. - The purpose is to have digital equipment, information and services to be protected from unintended or unauthorized access, change or destruction. - It includes physical security to prevent theft of equipment and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security.

Cyber security is the process of applying security measures to ensure confidentiality, integrity, and availability of data. Cyber security assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. - The goal of cyber security is to protect data both

in transit and at rest. Measures put in place to ensure cyber security include access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization.

Physical Security refers to the measures put in place by protect computer systems from physical damage and mitigate physical security risks. Physical security includes:

- Locked doors
- Burglar proofs.
- Parameter fences.
- Security guards.
- Server room environmental protection, optimization.
- Concrete walls.
- Lightening conductors.

- Fire extinguishers.
- Strategic server and storage placement

What is a computer security risk?

A computer security risk is an action that causes loss of or damage to computer system**.** Security threats to computers-based information systems, private or confidential data include:

- System failure
- information theft
- computer viruses, worms and Trojan horses
- unauthorized access and use
- hardware theft
- software theft
- unauthorized alteration

- malicious destruction of hardware software, data or network resources, as well as sabotage

ii. Security threats for (hardware and software)

Some of the causes of computerized information system failure include

- Hardware failure due to improper use.
- Unstable power supply as result of brownout or blackout and vandalism.
- Network breakdown.
- Natural disaster
- Program failure

What are hardware theft and hardware vandalism?

Hardware theft is act of stealing computer equipment and components. Cables sometimes used to lock equipment like some notebook computers use passwords, possessed objects, and biometrics as security methods. For PDAs, you can password-protect the device

Hardware vandalism is act of defacing or destroying computer equipment

Security threats for (hardware and software)

Software theft is the act of stealing or illegally copying software or intentionally erasing programs.

Software piracy is illegal duplication of copyrighted software. To guard against software theft and piracy, product activation is used.

Product activation allows user to input product identification number online or by phone and receive unique installation identification number

License agreement

A license agreement gives the right to use software. Single-user license agreement allows user to install software on one computer, make backup copy, and sell software after removing from computer.

Control measures against hardware failure

- Protect computers against brownout or blackout which may cause physical damages or data loss by using surge protectors and Uninterruptible power supply (UPS). For critical systems, most organizations have put into place fault tolerant systems.
- A fault tolerant system has redundant or duplicate storage, peripherals devices and software that provide a fail-over capability to backup components in the event of system failure.
- Disaster recovery plans Disaster recovery plan involves establishing offsite storage of an organization’s databases so that in case of disaster or fire accidents, the company would have backup copies to reconstruct lost data

Computer crimes are criminal activities, which involve the use of information technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering computer data. - Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data as well as system interference.

This is the criminal offence illegal or unauthorized use of computer technology to manipulate critical user data. It refers to any crime that involves a computer and a network.

Computer crimes may not necessarily involve damage to physical property. They rather include the manipulation of confidential data and critical information. - Computer crimes involve activities of software theft, wherein the privacy of the users is hampered. These criminal activities involve the breach of human and information privacy, as also the theft and illegal alteration of system critical information.

Types of computer crimes

Hacking: The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking. It may involve hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. - Phishing is carried out through emails or by luring the users to enter personal information through fake websites. - Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

Cyber stalking is the use of communication technology, mainly the Internet, to torture other individuals which include activities such as false accusations, transmission of threats and damage to data and equipment.

The physical theft of computer hardware and software is the most widespread related crime especially in developing countries. The most common issues now, we here cases of people breaking into an office or firm and stealing computers, hard disks and other valuable computer accessories. In most cases such theft can be done by untrustworthy employees of firm or by outsiders. The reason behind an act may be commercial, destruction to sensitive information or sabotage

Control measures against theft

- Employ security agents to keep watch over information centers and restricted backup sites.
- Reinforce weak access points like windows, door and roofing with metallic grills and strong padlocks.

- Motivate workers so that they feel a sense of belonging in order to make them proud and trusted custodians of the company resources.
- Insure the hardware resources with a reputable insurance firm.
- Piracy is a form of intellectual property theft which means illegal copying of software, information or data. Software, information and data are protected by copyright and patent laws.

Control measures against piracy

There are several ways of reducing piracy

- Enforce laws that protect the owners of data and information against piracy.
- Make software cheap enough to increase affordability.
- Use licenses and certificates to identify original software.

- Set installation passwords that deter illegal installation of software.

Fraud is stealing by false pretense. Fraudsters can be either employees in a company, non-existent company that purports to offer internet services such as selling vehicles etc. other form of fraud may also involve computerized production and use of counterfeit documents. This is due to the dynamic growth of internet and mobile computing, sophisticated cybercrimes.

Sabotage refers to illegal destruction of data and information with the aim of crippling services delivery, or causing great loss to an organization. Sabotage is usually carried out by disgruntled employees or competitors with the intention of causing harm to an organization.

Surveillance refers to monitoring use of computer system and networks using background programs such as spyware and cookies. The information gathered may be used for one reason or the other e.g. spreading sabotage.

Identity theft-Act of pretending to be someone else by using another person's identity

Computer industrial espionage-Involves stealing of trade secrets or spying through tech means for bribery, blackmail, etc

Software piracy-The illegal act of duplicating copyrighted software.

Phreaking-The act of illegally breaking into a communication system to make calls without paying

Unauthorized use This is the use of a computer or its data for illegal/unapproved activities.

Spoofing Is a malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

Spamming=Sending of unwanted e-mails.

Knowingly selling-Is the act of distributing and selling child pornography.

A backdoor is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. - The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device. - A specific form of backdoor is a rootkit, which replaces system binaries and/or hooks into

the function calls of an operating system to hide the presence of other programs, users, services and open ports. - It may also fake information about disk and memory usage.

Denial of Service attack-This is an attack designed to render the system unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. - These types of attacks are, in practice, difficult to prevent, because the behaviour of whole networks needs to be analyzed, not just the behavior of small pieces of code.

Eavesdropping is the act of secretly listening to a private conversation, typically between hosts on a network or telephone conversations. - For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers.

Cyber extortion is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks.

Information disclosure (privacy breach or data leak) describes a situation where information, thought to be secure, is released in an untrusted environment.

Others include

- **Cyber terrorism**
- **Cyber bullying**
- **Cyber harassment.**

Computer Viruses

A computer virus is a program designed specifically to damage, infect and affect other programs, data or cause irregular behavior to the computer. OR

A computer virus is a piece of software that can replicate itself and infect a computer, data and software without the knowledge of the user.

Computer Malware

Malware or short for malicious software is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. - Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. - Malwares include computer viruses, worms, Trojan horses, ransom ware, spyware, adware, scare ware, and other malicious programs. Malware is often disguised as, or embedded in, non-malicious files

Symptoms of a virus infected computer

- System slows down.
- System crushes and hangs up.
- Hard disk won’t boot.

- Corrupted hard disk data.
- Program sizes keep changing.
- Computer programs take long to boot than normal.
- Files won't open.

TYPES OF VIRUSES

A boot sector virus-This executes when a computer starts up because it resides in the boot sector of a floppy disk or the master boot record of a hard disk.

A file virus-This attaches itself to program files, and is loaded into memory when the infected program is run.

A macro virus -This uses the macro language of an application (e.g., word processor or spread sheet) to hide the virus code.

A logic bomb-This is a virus that activates when it detects a certain condition.

A time bomb-This is a kind of logic bomb that activates on a particular date.

A worm -This copies itself repeatedly in memory or on a disk drive until no memory or disk space remains, which makes the computer stops working.

A Trojan horse -This is a program that hides within or looks like a legitimate program, but executes when a certain condition or action is triggered.

A polymorphic virus -This modifies its program code each time it attaches itself to another program or file, so that even an antivirus utility has difficulty in detecting it

Scare-ware is a type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software. – Scare-ware, which generates pop-ups that resemble Windows system messages, usually purports to be antivirus or antispyware software, a firewall application or a registry cleaner.

Adware-The term **adware** is frequently used to describe a form of malware (malicious software), usually that which presents unwanted advertisements to the user of a computer. The advertisements produced by adware are sometimes in the form of a pop-up.

Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another individual without the consumer's consent, or that claims control over a computer without the consumer's knowledge.

A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and other malicious codes into one single threat. - Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack.

Viruses are activated in three basic ways

- Opening an infected file
- Running an infected program
- Starting up the computer with an infected floppy disk, flash disk

How viruses are spread (Sources of viruses)

- Through E-mail attachments.
- Rogue websites. E.g. some adult sites, gambling sites, e.t.c.
- Sharing infected disks.
- Through networks.
- Through infected software.
- Hackers.
- Through downloads from the internet.
- Through software updates

Precautions to prevent virus infection

- Ensure that the e-mail is from a trusted source before opening or executing any e-mail attachment.

- Install an antivirus utility and update its virus definitions frequently for detecting and removing viruses.
- Never start up a computer with a floppy disk in the floppy drive.
- Scan all floppy disks and files for possible virus infection before opening them.
- Set the security level for macros in an application so that the user can choose whether or not to run potentially unsafe macros.
- Write-protect the recovery disk before using it.
- Back up important files regularly.
- Ensure that there is a policy of how computers are used and protected.

How to protect data from viruses in a computer system

- Make a back-up of all important files.
- Always update your software.

- Perform regular maintenance.
- Scan all disks from other computers.
- Protect your password and change it after some time.
- Use anti-virus software.

Anti-Virus Software

Anti-Virus Software Antivirus software is a set of utility programs that looks for and eradicates a wide range of problems, such as viruses, Trojan horses, and worms.

Examples of Anti-Virus Software

1. AVG Anti-Virus
2. Avira Anti-Virus
3. Norton Anti-Virus Software
4. Kaspersky Anti-Virus
5. Avast Anti-virus
6. Smadav USBAnti-Virus

How to protect Computer Systems?

Installing Antivirus Program:- Computer programs that attempt to identify, prevent and eliminate computer viruses and other malicious software (malware).

Installing Firewall:- This serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks.

Data Encryption:- This method is used to alter the information in a form that it cannot be understood or followed by other people during transmission.

Data Backup:- Users should frequently duplicate (copy) the information to different storage devices such as DVDs, external hard disk to be able to recover their information in case of a disaster.

User ID and Passwords:- This is to restrict access to the computer systems, only allowing authorized users. A password is a secret code that combines characters and numbers that allow a user to access a computer or a network.

Access rights:- Access rights help to protect the IT system and the data stored on the system by restricting who can do what. Most company networks will be set up so that different users have appropriate levels of access rights. For example a manager of the company will have higher level access right than his subordinate staffs.

Audit Logs:- Network managers should ensure that their system is able to create an audit log. An audit log will record every important event in an 'audit file such as who logged on to the system at what time and onto which computer, which files were opened, altered, saved or deleted or log events such as attempts to access proxy servers

Rules for creating Secure Passwords

- Do not use your name or names of your close friends.
- Pick a mix of alphabetic and numeric characters. Never use an all-numeric password (especially your phone number or social security number).
- Pick long passwords. If your password is only a few letters long, an attacker will find it easy to try all combinations.

- Pick different passwords for the different machines or network nodes you access.

Intellectual property (IP)

Is a legal term that refers to creations of the mind that may include software, music, literature, discoveries and inventions.

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time. - Intellectual property rights include patents, copyright, industrial design rights, trademarks, trade dress, and trade secrets.

A patent grants an inventor the right to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention.

- An invention is a solution to a specific technological problem, which may be a product or a process.

A copyright is the exclusive legal right that prohibits copying of intellectual property without permission of the copyright holder. - A copyright gives the creator of original work exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or "works". Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed.

A trademark is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.

Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. - It is the process of scrambling plaintext (ordinary text, sometimes referred to as clear-text) into an unreadable format (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as **Cryptographers.** - It is a technique used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified. - The art of

protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. - Only those who possess a secret key can decipher (or decrypt) the message into plain text. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. - Cryptography is used to protect e-mail messages, credit card information, and corporate data. - Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and asymmetric-key systems (public-key systems) that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Secret Vs. Public Key

Secret Keys (Symmetric Systems):- Both sender and receiver use the key to encrypt and decrypt. This is the fastest computation method, but getting the secret key to the recipient in the first place is a problem.

ii) Public Keys

Asymmetric Systems):- Each recipient has a private key that is kept secret and a public key that is published for everyone. - The sender is sent the recipient's public key and uses it to encrypt the message.

The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. - Thus, the private key is never in transit and remains invulnerable.

Use of Biometrics

Biometrics is the identification of a person by the measurement of their biological features. - For example, users identifying themselves to a computer or building by their finger print or voice is considered a biometric identification.

- When compared to a password, this type of system is much more difficult to fake since it is unique to the person. Below is a listing of all known biometric devices.

Types of biometric devices

- A **fingerprint scanner**, which captures curves and indentations of a fingerprint

- A **hand geometry system**, which can measure the shape and size of a person's hand
- **A face recognition system**, which captures a live face image and compares it with a stored image
- A **voice recognition system**, which compares a person's live speech with their stored voice pattern
- **A signature verification system**, which recognizes the shape of handwritten signature of a person
- **An iris recognition system**, which reads patterns in the tiny blood vessels in the back of the eye, which are as unique as a fingerprint.

COMPUTER ETHICS

These refer to a set of moral principles that regulate the use of computers. The human values and moral conduct relating to right and wrong decision made when using computers. Moral guidelines that govern use of computers and information systems

A code of conduct is a written guideline that helps determine whether a specific action is ethical or unethical.

Three useful ethical principles

- An act is ethical if society benefits from the act.
- An act is ethical if people are treated as an end and not as a means to an end.
- An act is ethical if it is fair to all parties involved.

Computer ethics involves use of computers & software in morally acceptable way. Standards or guidelines are important in this industry, because technology changes are outstripping the legal system's ability to keep up

Computer Ethics for Computer Professionals

- According to the Association for Computing Machinery (ACM) code, a computing professional:
- Contributes to society and human well-being.
- Always avoids harm to others.

- Should be honest and trustworthy.
- Should exercise fairness and takes action not to discriminate.
- Honors property rights, including copyrights and patents
- Gives proper credit when using the intellectual property of others.
- Respects other individuals' rights to privacy.
- Honors confidentiality.

Information privacy

Right of individuals and companies to restrict collection and use of information about them.

Private data or information is the collection and use of personal information. This information should not be accessed or disclosed to any other person unless permitted by the owner.

Data held by an organization or government that should be disclosed to authorized people only is said to be **confidential**.

Concerns related to collection and use of private data

- Data should not be disclosed to other people without the owner's permission.
- Data and information should be kept secured against loss or exposure
- Data and information should be kept longer than necessary
- Data and information should be accurate and up to date.
- Data and information should be collected, used and kept for specified lawful purposes.

What are some ways to safeguard personal information?

- Limit the amount of information you provide to Web sites; fill in only required information
- Inform merchants that you do not want them to distribute your personal information
- Set up a free e-mail account; use this e-mail address for merchant forms
- Sign up for e-mail filtering through your Internet service provider or use an anti-spam program
- Do not reply to spam for any reason
- Install a personal firewall

- Turn off file and print sharing on your Internet connection
- Surf the Web anonymously with a program such as Freedom Web Secure or through an anonymous Web site such as Anonymizer.com
- Install a cookie manager to filter cookies
- Clear your history file when you are finished browsing.

Unethical computer codes of conduct

- Modifying certain information on the internet
- Selling information to others without the owner's permission
- Using information without authorization
- Invasion of privacy
- Involving in the stealing of software

Computer ethics to be put in place

- Respect the privacy of others.
- Always identify the user accurately

- Respect copyrights and licenses
- Respect the intellectual property.
- Respect the integrity of the computer system.
- Exhibit responsible and sensible use of hardware and software

EMERGING TECHNOLOGIES

This involves innovations and advancements in the use of new technological tools that make technology more amazing.

Concepts of emerging technologies covers the rapid evolution of computers and information technology with the future trends in computer and information and communication technology which is characterized by artificial intelligence and digital forensics.

Application areas of specific emerging technologies

Affective computing - Is the study and development of systems and devices that can recognize, interpret, process, and simulate human affects. It is an interdisciplinary field spanning computer science, psychology, and cognitive science.

Affect is the experience of feeling or emotion. Affect is a key part of the process of an organism's interaction with stimuli. The word also refers sometimes to affect display, which is "a facial, vocal, or gestural behavior that serves as an indicator of affect"

Ambient Intelligence (AmI)

In computing, ambient intelligence refers to electronic environments that are sensitive and responsive to the presence of people. - Ambient intelligence is a vision on the future of consumer electronics, telecommunications and computing that was originally developed in the late 1990s for the time frame 2010–2020.

Artificial Intelligence (AI)

Artificial intelligence refers to a branch of computer science that is concerned with the development of machines that emulate human-like qualities such as learning, reasoning, communication seeing and hearing. Also artificial intelligence refers to the ability of a machine to perform tasks that normally require human intelligence.

Computer scientist and engineers are still working hard to come up with computer reality in near future which can think and learn instead of relying on static programmed instructions

This is the intelligence exhibited by machines or software. It is an academic field of study which studies the goal of creating intelligence.

Major AI researchers and textbooks define this field as "the study and design of intelligent agents", where an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success.

There are four main application areas of artificial intelligence namely:

- Expert systems. Software that operate at the level of human expert in specific application.

- Natural language processing.
- Artificial neural networks.
- Robotics/perception systems.

Bioelectronics

This is a recently coined/invented term for a field of research that works to establish a synergy/interaction between electronics and biology. The emerging field of Bioelectronics seeks to exploit biology in conjunction with electronics in a wider context encompassing, for example, biological fuel cells, bionics and biomaterials for information processing, information storage, electronic components and actuators.

A key aspect is the interface between biological materials and micro- and nano-electronics.

Digital forensics

Digital forensic refers to the science encompassing the recovery and investigation of material found in digital devices often in relation to computer crime.

Main application areas of digital forensic namely

- Legal consideration-use of digital evidence in court
- Branches-perception of the computer forensic, mobile device forensic, network forensic
- Application of digital forensic such as electronic discovery, intrusion etc
- Forensic process-analysis and reporting.

Cloud computing

Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid. – This is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources.

Future Internet

As wireless and mobile technology advance, users can not only surf the online world - but can also do it on the move, through a plethora of portable devices, including laptops, smart phones and

tablets; with an increasing need for high-bandwidth, high-speed broadband that can cope with rich multimedia content.

Other Emerging technologies

Virtual reality/artificial reality-Simulates physical presence in places of a real world as well as an imaginary world

Computer vision-Includes methods of acquiring, processing, analyzing, understanding images so as to produce symbolic information.

Implications of emerging technologies

- Technophobia/techno stress
- Loss of jobs say for massagers in case of networking
- Health issues for eye defects, back pain.
- Fear of cost of retaining or learning new skills
- Fear of increased electricity and subscriptions costs
- Fear of computer related crimes like forging of documents

- Fear of loss of man-hours through computer games and video during working hours
- Data loss by virus and system crashing
- Computer related errors and accident
- Unemployment//redundancy//financial/family problems.
- Local businesses/economy affected
- Possible increase in crime (Idle youth)
- People leaving community (to find other work)
- Opportunities for high skilled/programming jobs

Computer Professionals

A computer professional might be: - A person working in the field of information technology.

OR

A person who has undergone training in a computer-related field colleges, universities and computer institutes. A person who has an extensive knowledge in the area of computing.

CAREERS IN ICT FIELD

a) Computer operator

- Some of the responsibilities of a computer operator include;
- Entering data into the computer for processing.
- Keeping up-to-date records (log files) of all information processing activities.

b) Computer technician

- Troubleshooting computer hardware and software related problems.
- Assembling and upgrading computers and their components.
- Ensuring that all computer related accessories such as printers modems, storage media devices are in good working condition.

c) Computer engineer

- Computer and electronic engineers are coming up with new and more efficient technologies in information and communication technology almost daily. Since computers are electronic devices, hardware designers must be good in electronic engineering in order to be able to:

- Design and develop computer components such as storage devices, motherboards and other electronic components.
- Determine the electrical power requirement of each component.
- Re-engineer computer components to enhance its functionality and efficiency.
- Design and develop engineering and manufacturing computer controlled devices such as robots.

d) Computer programmer

- Large organizations such as insurance companies, banks, manufacturing firms and government agents hire programmers to work together with system analysts in order to:
- Develop in house application programs or system programs.
- Customize commercial application packages to suite the organization needs.
- Install, test, debug, and maintain programs developed or customized for the organization.

e) Web administrator/webmaster

- Developing and testing websites.
- Maintaining, updating and modifying information on the website to meet new demands by the users.

f) Software engineers

Most Software engineers analyses user needs and create application software. Software engineers usually have experience in programming, but focus on the design and development of programs using the principles of mathematics and engineering.

g) Computer Trainers

Computer trainers typically teach new users how to use the computer software and hardware.

h) Network administrator

- A network administrator is a specialist whose responsibilities are to:
- Set-up a computer network.
- Maintain and enforce security measures on the network.
- Monitor the use of network resources.
- Maintain and troubleshoot network related problems.

i) Database Administrator (DBA)

Database Administrator (DBA) is an IT professional responsible for installation, configuration, upgrade, administration, monitoring, maintenance, and securing of databases in an organization.

j) Graphic designer

A graphic designer is a professional within the graphic design and graphic arts industry who assembles together images, typography, or motion graphics to create a piece of design.

k) System Administrators

A system administrator, or system admin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers

A system administrator may acquire, install, or upgrade computer components and software; provide routine automation; maintain security policies; troubleshoot; train or supervise staff; or offer technical support for projects.

END