**Section A 2022**

1. **Computer Security**: Computer security refers to the protection of computer systems, networks, and data from unauthorized access, disclosure, theft, damage, or disruption, as well as the preservation of their confidentiality, integrity, and availability.
2. **Physical Threats to a Computer System**:
   * Theft or loss of hardware devices (e.g., laptops, desktops, servers).
   * Damage due to environmental factors (e.g., fire, flood, power surges).
   * Hardware tampering or sabotage (e.g., vandalism, unauthorized modifications).
3. **Ways Attackers May Use to Identify an Individual Password**:
   * **Brute Force Attack**: Attempting all possible combinations of characters until the correct password is found.
   * **Dictionary Attack**: Using a list of commonly used passwords or words from a dictionary to guess the password.
   * **Social Engineering**: Manipulating or tricking individuals into revealing their passwords through techniques such as phishing, pretexting, or shoulder surfing.
4. **Functions of Information Security for an Organization**:
   * **Confidentiality**: Ensuring that sensitive information is only accessible to authorized individuals or entities.
   * **Integrity**: Maintaining the accuracy, completeness, and reliability of data and resources by preventing unauthorized modifications.
   * **Availability**: Ensuring that information and resources are accessible and usable by authorized users when needed.
   * **Authentication and Authorization**: Verifying the identity of users and determining their level of access rights and privileges to resources and systems.
5. **Example of a Cyber Security Threat**: A distributed denial-of-service (DDoS) attack, where multiple compromised computers (botnets) flood a targeted system or network with an overwhelming amount of traffic, causing it to become inaccessible to legitimate users.
6. **Identity Theft in Computer Security**: Identity theft involves the unauthorized acquisition and misuse of an individual's personal information, such as their name, social security number, or financial data, to commit fraud or other criminal activities online. Attackers may use stolen identities to access accounts, make unauthorized transactions, or impersonate victims for malicious purposes.
7. **Vulnerability Assessment vs. Penetration Testing**:
   * **Vulnerability Assessment**: Identifies and assesses security vulnerabilities in a system or network, typically through automated scanning tools, to determine potential weaknesses that could be exploited by attackers.
   * **Penetration Testing**: Simulates real-world cyber attacks to evaluate the effectiveness of security defenses, procedures, and controls by attempting to exploit vulnerabilities and gain unauthorized access to systems, networks, or data.
8. **Importance of Using a VPN on Public Networks**:
   * Encrypts Data: Protects sensitive information transmitted over the public network from interception and eavesdropping by encrypting data traffic.
   * Ensures Privacy: Masks the user's IP address and browsing activities, enhancing privacy and anonymity while browsing the internet on public Wi-Fi networks.
9. **Ways Data from within the Organization May Be Exposed or Accessed by Unauthorized Entities**:
   * **Insider Threats**: Malicious or negligent actions by employees, contractors, or trusted insiders who have access to sensitive data.
   * **Data Breaches**: Unauthorized access or disclosure of sensitive information due to security breaches, vulnerabilities, or hacking attacks targeting internal systems.
   * **Lack of Access Controls**: Inadequate access controls or weak authentication mechanisms that allow unauthorized individuals to gain access to sensitive data.
10. **Major Classifications of Computer Hackers**:
    * **White Hat Hackers**: Ethical hackers who use their skills to identify and address security vulnerabilities in systems and networks, often employed by organizations to conduct security assessments and penetration testing.
    * **Black Hat Hackers**: Malicious hackers who exploit security vulnerabilities for personal gain, financial profit, or malicious intent, such as stealing data, disrupting services, or spreading malware.
    * **Grey Hat Hackers**: Hackers who operate between the ethical boundaries of white hat and black hat hackers, sometimes engaging in activities that may be considered unethical or illegal but without malicious intent.
11. **Symptoms of a Computer Virus**:
    * Slow Performance: Noticeable decrease in the speed and responsiveness of the computer system or applications.
    * Unusual Behavior: Unexpected errors, crashes, or freezes occurring frequently during normal operation.
    * Pop-up Messages: Display of unexpected pop-up messages or alerts, often indicating infection or attempts to execute malicious code.
    * File Corruption: Files becoming inaccessible, corrupted, or modified without user intervention, indicating potential virus activity.
12. **Ways to Prevent Brute Force Attacks**:
    * **Implement Account Lockout Policies**: Enforce account lockout mechanisms that temporarily or permanently lock user accounts after multiple failed login attempts, preventing attackers from continuously guessing passwords.
    * **Use Strong Passwords**: Encourage users to use complex and strong passwords that are difficult for attackers to guess, combining uppercase and lowercase letters, numbers, and special characters.
    * **Implement Rate Limiting**: Implement rate-limiting measures that restrict the number of login attempts allowed within a certain time frame, making it harder for attackers to perform rapid brute force attacks.

**Section B 2022**

**13.**

a) **Elements of an Information Security Policy:**

1. **Policy Statement**: This outlines the organization's commitment to information security, its objectives, and the scope of the policy. It sets the tone for the entire policy document and provides a clear direction for implementing security measures.
2. **Roles and Responsibilities**: This section defines the roles and responsibilities of individuals and departments within the organization regarding information security. It specifies who is accountable for various aspects of security management, including policy enforcement, incident response, and compliance.
3. **Access Control Policies**: Access control policies define the rules and procedures for granting and managing access to information and resources within the organization. This includes user authentication, authorization mechanisms, and privileges assigned based on job roles and responsibilities.
4. **Data Classification and Handling**: This element establishes guidelines for classifying and handling different types of data based on their sensitivity and criticality. It outlines procedures for labeling, storing, transmitting, and disposing of data to ensure appropriate protection and compliance with regulatory requirements.
5. **Security Awareness and Training**: Security awareness and training programs educate employees about information security risks, policies, procedures, and best practices. This element aims to promote a culture of security awareness and ensure that employees understand their roles in safeguarding sensitive information.

b) **Types of Malicious Software:**

i. **Viruses**: Viruses are malicious programs that infect legitimate files or software and replicate themselves when executed. They can spread through infected email attachments, file downloads, or removable storage devices. Viruses can cause damage by corrupting files, stealing data, or disrupting system operations.

ii. **Trojans**: Trojans are deceptive programs that appear legitimate but contain malicious code. They often masquerade as useful software or files to trick users into downloading and executing them. Trojans can perform various malicious actions, such as stealing sensitive information, creating backdoors for remote access, or launching denial-of-service attacks.

iii. **Worms**: Worms are self-replicating malware that spread across networks by exploiting vulnerabilities in software or network protocols. Unlike viruses, worms do not require a host file to propagate and can spread independently. They can rapidly infect a large number of systems, causing network congestion, system slowdowns, or unauthorized access.

iv. **Ransomware**: Ransomware is a type of malware that encrypts files or locks users out of their systems, demanding payment (ransom) in exchange for decryption keys or restoring access. Ransomware infections typically occur through malicious email attachments, compromised websites, or exploit kits. They can cause significant data loss, financial losses, and operational disruptions.

v. **Spyware**: Spyware is software that secretly gathers information about a user's browsing habits, keystrokes, or personal data without their consent. It can monitor online activities, capture sensitive information (e.g., login credentials, financial details), and transmit it to remote servers controlled by attackers. Spyware often accompanies other malware infections or is bundled with legitimate software downloads.

**14.**

a) **Types of Computer Security Testing:**

i. **Vulnerability Assessment**: Identifies and evaluates security vulnerabilities and weaknesses in systems, networks, and applications to assess their susceptibility to attacks. It involves scanning for known vulnerabilities, misconfigurations, and outdated software versions using automated tools and manual techniques.

ii. **Penetration Testing**: Simulates real-world cyber attacks to assess the effectiveness of security defenses and identify exploitable vulnerabilities in systems, networks, or applications. Penetration testers attempt to breach defenses, gain unauthorized access, and escalate privileges to uncover weaknesses and recommend remediation measures.

iii. **Security Auditing**: Conducts comprehensive reviews and assessments of security controls, policies, and procedures to ensure compliance with regulatory requirements and industry standards. Security auditing examines the implementation and effectiveness of security measures, identifies gaps or deficiencies, and provides recommendations for improvement.

iv. **Security Code Review**: Analyzes the source code of software applications to identify security vulnerabilities, coding errors, or design flaws that could be exploited by attackers. Security code reviews involve manual inspection and automated analysis techniques to detect potential weaknesses and provide developers with guidance on secure coding practices.

v. **Security Architecture Review**: Evaluates the overall security architecture of systems, networks, or infrastructures to assess their resilience against cyber threats and attacks. Security architecture reviews examine the design, configuration, and deployment of security controls, identifying architectural weaknesses and recommending enhancements to strengthen defenses.

b) **Ways to Prevent Identity Theft:**

i. **Use Strong Authentication**: Implement strong authentication mechanisms, such as biometrics, multi-factor authentication, or hardware tokens, to verify users' identities and prevent unauthorized access to accounts and sensitive information.

ii. **Regularly Monitor Financial Accounts**: Monitor financial accounts, credit reports, and online transactions regularly for any suspicious or unauthorized activity. Report any discrepancies or fraudulent charges to financial institutions immediately.

iii. **Secure Personal Information**: Safeguard personal information, such as social security numbers, birthdates, and financial data, by avoiding sharing it unnecessarily and securely storing it in encrypted files or password-protected databases.

iv. **Be Cautious Online**: Exercise caution when sharing personal information online, especially on social media platforms or unfamiliar websites. Avoid clicking on suspicious links or downloading attachments from unknown sources to minimize the risk of phishing attacks and malware infections.

v. **Shred Sensitive Documents**: Dispose of sensitive documents containing personal information, such as bank statements, bills, or credit card statements, securely by shredding them before discarding to prevent dumpster diving and identity theft.

vi. **Use Secure Connections**: Use secure and encrypted connections (e.g., HTTPS) when accessing websites or transmitting sensitive information online to protect against interception and eavesdropping by attackers.

vii. **Stay Educated**: Stay informed about the latest identity theft trends, scams, and security best practices by regularly reading security blogs, news articles, and resources provided by reputable sources.

**c) Cyber Security Risks in the Banking Industry and Mitigation:**

i. **Data Breaches**: Data breaches pose significant risks to banks, leading to unauthorized access, theft, or exposure of sensitive customer information. Banks can minimize this risk by implementing robust data encryption, access controls, and monitoring mechanisms to detect and respond to suspicious activities promptly.

ii. **Fraudulent Transactions**: Fraudulent transactions, such as account takeovers or unauthorized fund transfers, can result in financial losses and damage to the bank's reputation. Banks can mitigate this risk by implementing transaction monitoring systems, fraud detection algorithms, and multi-factor authentication for online banking transactions.

iii. **Phishing Attacks**: Phishing attacks target bank customers and employees with deceptive emails, messages, or websites to trick them into disclosing sensitive information or login credentials. Banks can educate customers and employees about phishing risks, implement email filtering and anti-phishing tools, and enforce strict authentication measures to prevent unauthorized access.

iv. **ATM Skimming**: ATM skimming involves installing malicious devices on ATM machines to capture card details and PINs, enabling criminals to clone cards and withdraw funds fraudulently. Banks can mitigate this risk by regularly inspecting ATMs for tampering, implementing physical security measures, and deploying anti-skimming technologies to detect and prevent skimming attacks.

**15.**

**a) Terms in Computer Security:**

i. **Firewall**: A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between trusted internal networks and untrusted external networks, filtering traffic to prevent unauthorized access, malicious attacks, and unwanted communication. Firewalls can be implemented as hardware appliances, software applications, or cloud-based services and are essential for enforcing network security policies and protecting against various cyber threats.

ii. **Hacking**: Hacking refers to the unauthorized or illegitimate access, manipulation, or exploitation of computer systems, networks, or data by individuals or groups (hackers) with malicious intent. Hacking techniques can range from exploiting software vulnerabilities and weak passwords to social engineering and phishing attacks. While hacking can be used for criminal activities, such as stealing sensitive information, disrupting services, or causing financial harm, it can also be employed for ethical purposes, such as identifying security weaknesses and improving defenses (ethical hacking).

iii. **Threat**: In the context of computer security, a threat refers to any potential danger, risk, or malicious event that could compromise the confidentiality, integrity, or availability of information, systems, or networks. Threats can include various forms of cyber attacks (e.g., malware infections, hacking attempts, denial-of-service attacks), natural disasters (e.g., floods, earthquakes), human errors, or insider threats. Understanding and mitigating threats are essential for protecting against security breaches and minimizing the impact of security incidents.

iv. **Vulnerability**: A vulnerability is a weakness or flaw in a system, application, or network that could be exploited by attackers to compromise security, gain unauthorized access, or cause damage. Vulnerabilities can arise due to programming errors, misconfigurations, software bugs, or outdated software versions. Exploiting vulnerabilities often involves attackers exploiting weaknesses to execute malicious code, escalate privileges, or bypass security controls. Vulnerability management involves identifying, prioritizing, and remediating vulnerabilities to reduce the risk of exploitation and strengthen security posture.

v. **Risk**: Risk refers to the potential for loss, harm, or damage resulting from the occurrence of threats exploiting vulnerabilities. In computer security, risk encompasses the likelihood of security incidents occurring and their potential impact on the organization's assets, operations, and reputation. Risk management involves identifying, assessing, mitigating, and monitoring risks to minimize their impact and ensure business continuity. It involves balancing the trade-offs between security measures, business objectives, and resource constraints to effectively manage and mitigate risks.

**b) Objectives of Information Security:**

i. **Confidentiality**: One of the primary objectives of information security is to ensure the confidentiality of sensitive information by preventing unauthorized access, disclosure, or exposure. Confidentiality measures, such as encryption, access controls, and data classification, protect sensitive data from unauthorized disclosure or interception, preserving privacy and confidentiality.

ii. **Integrity**: Information security aims to maintain the integrity of data and systems by safeguarding against unauthorized modifications, alterations, or corruption. Integrity measures, such as data validation, checksums, and digital signatures, ensure that data remains accurate, complete, and reliable throughout its lifecycle, preventing unauthorized tampering or manipulation.

iii. **Availability**: Another key objective of information security is to ensure the availability of information, systems, and services to authorized users when needed. Availability measures, such as redundancy, backup and recovery, and fault-tolerant systems, minimize disruptions, downtime, or denial-of-service attacks, ensuring uninterrupted access to critical resources and operations.

**c) Rules for Legal Compliance with Data and Information:**

i. **Data Protection Laws Compliance**: Ensure compliance with relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), to safeguard the privacy and security of personal and sensitive data.

ii. **Intellectual Property Rights Protection**: Respect and uphold intellectual property rights, including copyrights, trademarks, and patents, when using, sharing, or distributing copyrighted materials or proprietary information to avoid infringement and legal consequences.

iii. **Confidentiality Agreements and Non-Disclosure Policies**: Adhere to confidentiality agreements and non-disclosure policies when handling confidential or proprietary information belonging to individuals, organizations, or clients, ensuring that sensitive information is not disclosed or shared without proper authorization.

iv. **Lawful Use of Information**: Ensure that data and information are used lawfully and ethically, adhering to legal and regulatory requirements and avoiding activities that could lead to unauthorized access, misuse, or exploitation of information for illicit purposes.

**16.**

a) **Measures to Protect Against Cyber-Attacks:**

i. **Implement Strong Access Controls**: Enforce robust authentication mechanisms, access controls, and user permissions to restrict unauthorized access to systems, networks, and sensitive data.

ii. **Regular Security Updates and Patch Management**: Keep software, applications, and systems up-to-date with the latest security patches, updates, and fixes to address known vulnerabilities and mitigate the risk of exploitation by attackers.

iii. **Deploy Intrusion Detection and Prevention Systems (IDPS)**: Implement IDPS solutions to monitor network traffic, detect suspicious activities, and block or mitigate potential cyber threats, including malware infections, intrusion attempts, and denial-of-service attacks.

iv. **Data Encryption and Secure Communications**: Encrypt sensitive data both at rest and in transit using strong encryption algorithms and secure communication protocols (e.g., SSL/TLS) to protect against unauthorized access, interception, or tampering.

v. **Employee Training and Awareness**: Provide regular cybersecurity training and awareness programs to employees to educate them about security risks, best practices, and procedures for identifying and responding to cyber threats effectively.

vi. **Incident Response and Disaster Recovery Planning**: Develop and maintain incident response and disaster recovery plans to facilitate swift and coordinated responses to security incidents, minimize the impact of cyber-attacks, and restore operations quickly.

b) **Ways to Prevent Piracy with Regard to Data and Information:**

i. **Use Digital Rights Management (DRM)**: Implement DRM technologies and solutions to control and manage access to digital content, enforce licensing agreements, and prevent unauthorized copying, distribution, or reproduction of copyrighted materials.

ii. **Implement Access Controls and Authorization Mechanisms**: Employ access controls, authentication mechanisms, and user permissions to restrict access to proprietary software, databases, or online resources to authorized users only, preventing unauthorized use or duplication.

iii. **Anti-Piracy Measures and Enforcement**: Deploy anti-piracy measures, such as copyright notices, watermarks, or digital signatures, to deter piracy and enforce copyright protection laws. Work with law enforcement agencies and intellectual property rights holders to identify and take legal action against pirates and infringers.

iv. **Educate Users About Copyright Compliance**: Raise awareness among users about the importance of copyright compliance and the legal implications of piracy. Provide information and resources on obtaining licensed software, digital content, or media legally and ethically.

c) **Distinguishing Data Security and Data Integrity:**

* **Data Security**: Data security refers to the protection of data against unauthorized access, disclosure, or alteration to ensure its confidentiality, integrity, and availability. It involves implementing security measures, such as access controls, encryption, and authentication, to safeguard sensitive information from unauthorized access or misuse.
* **Data Integrity**: Data integrity, on the other hand, refers to the accuracy, consistency, and reliability of data over its entire lifecycle. It ensures that data remains unchanged and uncorrupted during storage, transmission, or processing and reflects the

**Section A 2023**

1. Definitions: i. Asset: In cybersecurity, an asset refers to any valuable resource or component within a system that requires protection from potential threats. This could include hardware such as servers and computers, software applications, data, intellectual property, and even human resources. ii. Threat: A threat in cybersecurity is any potential danger or risk to an asset or system that could exploit vulnerabilities and cause harm. Threats can come in various forms, including malware, hackers, natural disasters, human error, and more. iii. Logic bomb: A logic bomb is a type of malicious code or software that is intentionally inserted into a system to execute a harmful action when specific conditions are met. Unlike viruses or worms, logic bombs remain dormant until triggered by a predefined event, such as a particular date or action. iv. Vulnerability: A vulnerability refers to a weakness or flaw in a system's design, implementation, or configuration that could be exploited by attackers to compromise the integrity, availability, or confidentiality of the system or its data.
2. Ethical Penetration Testing: Ethical penetration testing, also known as ethical hacking, is a proactive approach to evaluating the security of a system or network by simulating cyber attacks from the perspective of a potential adversary. Ethical penetration testers use authorized techniques and tools to identify vulnerabilities and weaknesses in a system's defenses, helping organizations improve their security posture.
3. Ways to prevent brute force attacks: i. Implement account lockout policies: After a certain number of failed login attempts, lock the account temporarily or permanently to prevent further unauthorized access attempts. ii. Use strong authentication methods: Require the use of complex passwords or passphrase policies, multi-factor authentication, or CAPTCHA to increase the difficulty of brute force attacks. iii. Implement rate limiting: Restrict the number of login attempts within a specific time frame to make brute force attacks less feasible by slowing down the attack process.
4. Differentiation: i. Vulnerability Assessment vs. Penetration Testing:
   * Vulnerability Assessment involves identifying, quantifying, and prioritizing vulnerabilities in a system or network. It typically doesn't involve exploitation of vulnerabilities but focuses on discovering and reporting them.
   * Penetration Testing, on the other hand, goes a step further by actively attempting to exploit vulnerabilities to assess the effectiveness of existing security measures and identify potential weaknesses in the system's defenses.

ii. Update vs. Overhaul of security systems:

* + Update refers to the process of applying patches, fixes, or upgrades to existing security systems, software, or hardware components to address known vulnerabilities or improve functionality without fundamentally changing the underlying architecture.
  + Overhaul involves a more comprehensive and significant change to the security infrastructure, such as replacing outdated systems or implementing new technologies, policies, or procedures to enhance overall security posture.

1. Ways attackers may use to identify an individual password: i. Dictionary attacks: Attackers use lists of commonly used passwords or dictionary words to systematically guess passwords. ii. Brute force attacks: Attackers try all possible combinations of characters until they find the correct password. iii. Social engineering: Attackers gather personal information about the target individual from social media or other sources to guess or reset passwords based on common knowledge or security questions.
2. Symptoms of malware infection in a computer system: i. Slow performance: The infected system may experience sluggishness or unresponsiveness due to the malware consuming system resources. ii. Pop-up advertisements: Malware often generates unwanted pop-up ads or redirects users to malicious websites. iii. Unusual behavior: The system may exhibit unexpected behavior, such as files disappearing or new programs appearing without user intervention. iv. Security alerts: Antivirus or anti-malware software may detect and alert users to the presence of malicious files or activities on the system.
3. SQL injection: SQL injection is a type of cyber attack where an attacker exploits vulnerabilities in a web application's input fields to inject malicious SQL code into the application's backend database. This allows the attacker to manipulate the database, steal data, modify records, or execute arbitrary commands.
4. Secure Socket Layer (SSL): SSL is a cryptographic protocol designed to provide secure communication over a computer network, particularly the internet. It ensures data confidentiality, integrity, and authenticity by encrypting data transmitted between a web server and a client browser, thus protecting sensitive information from interception or tampering by unauthorized parties.
5. Common categories of ICT security threats: i. Malware: Malicious software such as viruses, worms, Trojans, ransomware, and spyware designed to disrupt, damage, or gain unauthorized access to computer systems or networks. ii. Phishing: Cybercriminals use deceptive emails, websites, or messages to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal data. iii. Denial of Service (DoS) attacks: Attackers flood a system, network, or server with excessive traffic or requests to overwhelm its resources and disrupt normal operations, rendering it inaccessible to legitimate users.
6. Categories of computer hackers: i. White Hat Hackers: Ethical hackers who use their skills to improve cybersecurity by identifying vulnerabilities and helping organizations strengthen their defenses. ii. Black Hat Hackers: Malicious hackers who exploit vulnerabilities for personal gain, financial profit, or malicious intent, such as stealing data, disrupting systems, or spreading malware. iii. Grey Hat Hackers: Hackers who operate between white hat and black hat hackers, sometimes engaging in activities that may be considered illegal or unethical but not necessarily with malicious intent, often motivated by curiosity or personal agenda.

**Section B 2023**

**11.**

**a) Six steps of setting up a firewall:**

1. **Identify Network Requirements:** Determine the network's topology, traffic patterns, and security needs to design an effective firewall configuration.
2. **Choose Firewall Type:** Select the appropriate type of firewall based on the organization's requirements and budget, such as packet-filtering, stateful inspection, proxy-based, or next-generation firewalls.
3. **Design Firewall Rules:** Create rulesets that define how traffic should be allowed or denied based on criteria such as source/destination IP addresses, ports, protocols, and application types.
4. **Implement Firewall Configuration:** Deploy the firewall hardware or software and configure it according to the predefined rulesets and security policies.
5. **Test Firewall Configuration:** Conduct thorough testing to ensure that the firewall is functioning as intended and effectively filtering network traffic without causing disruptions.
6. **Monitor and Maintain:** Regularly monitor firewall logs, update rule sets as needed to address emerging threats or changes in network requirements, and apply patches or firmware updates to maintain the firewall's security and performance.

**b) Functions of information security:**

1. **Confidentiality:** Ensuring that sensitive information is accessible only to authorized individuals or entities, preventing unauthorized access, disclosure, or theft of data.
2. **Integrity:** Safeguarding the accuracy and reliability of data by preventing unauthorized tampering, modification, or destruction, maintaining data consistency and trustworthiness.
3. **Availability:** Ensuring that information and resources are consistently accessible and usable by authorized users whenever needed, minimizing downtime and disruptions to operations.
4. **Authentication and Authorization:** Verifying the identity of users and entities accessing the system, and granting appropriate levels of access based on their roles, privileges, and permissions to prevent unauthorized access or misuse of resources.

**12.** *(Measures to protect government services from future attacks)*

1. Implement Strong Access Controls: Enforce strict user authentication mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC) to prevent unauthorized access.
2. Regular Vulnerability Assessments and Patch Management: Conduct frequent vulnerability assessments to identify and mitigate security weaknesses, and promptly apply security patches and updates to all systems and software.
3. Network Segmentation: Segment the network into distinct zones with different levels of trust, and implement firewalls and access controls to restrict lateral movement of attackers within the network.
4. Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS solutions to monitor network traffic and detect suspicious activities or intrusion attempts, and automatically block or mitigate threats in real-time.
5. Employee Training and Awareness: Provide comprehensive cybersecurity training to all government personnel to raise awareness about common threats, phishing attacks, and best practices for maintaining security hygiene.
6. Data Encryption: Encrypt sensitive data both in transit and at rest to protect it from unauthorized access or interception, using strong encryption algorithms and secure key management practices.
7. Incident Response Plan: Develop and regularly update an incident response plan outlining procedures for detecting, responding to, and recovering from security incidents, with clear roles and responsibilities assigned to relevant stakeholders.
8. Continuous Monitoring and Auditing: Implement robust logging and monitoring mechanisms to track user activities, network traffic, and system events for detecting anomalies or suspicious behavior, and conduct regular security audits to ensure compliance with security policies and regulations.
9. Vendor Risk Management: Assess and monitor the security posture of third-party vendors and service providers, and establish contractual agreements outlining security requirements and responsibilities.
10. Cybersecurity Collaboration and Information Sharing: Foster collaboration and information sharing among government agencies, law enforcement, and cybersecurity organizations to exchange threat intelligence, insights, and best practices for enhancing collective security posture.

**13.**

**a) Goals of ICT security:**

1. **Confidentiality:** Protecting sensitive information from unauthorized access, disclosure, or interception to maintain privacy and confidentiality.
2. **Integrity:** Ensuring the accuracy, reliability, and trustworthiness of data and systems by preventing unauthorized tampering, alteration, or corruption.
3. **Availability:** Ensuring that information and resources are consistently accessible and usable by authorized users whenever needed, minimizing disruptions and downtime.

**b) Elements of an Information Security Policy:**

1. **Access Control Policy:** Defines rules and procedures for granting and revoking access rights to users, systems, and data based on the principle of least privilege.
2. **Data Classification Policy:** Establishes guidelines for categorizing and labeling data based on its sensitivity level, and defines appropriate security controls and handling procedures for each classification.
3. **Acceptable Use Policy (AUP):** Sets forth rules and guidelines for acceptable and prohibited uses of organizational assets, including computers, networks, and internet resources, to mitigate risks associated with misuse or abuse.
4. **Incident Response Plan (IRP):** Outlines procedures for detecting, responding to, and recovering from security incidents, including roles and responsibilities of stakeholders, communication protocols, and escalation procedures.
5. **Security Awareness Training Policy:** Mandates cybersecurity awareness training programs for all employees to educate them about common threats, security best practices, and organizational security policies.
6. **Physical Security Policy:** Defines measures for safeguarding physical assets, facilities, and infrastructure from unauthorized access, theft, vandalism, or damage, including access controls, surveillance, and environmental controls.
7. **Compliance and Regulatory Policy:** Ensures that the organization complies with relevant laws, regulations, and industry standards pertaining to information security, privacy, and data protection, and defines procedures for compliance monitoring and reporting.

**14.**

**a) Steps of system testing plan:**

1. **Planning:** Define the objectives, scope, and resources required for testing, and develop a test plan outlining the testing approach, methodologies, and timelines.
2. **Test Design:** Create test cases and scenarios based on system requirements, functional specifications, and use cases, covering both positive and negative test scenarios to validate system behavior under different conditions.
3. **Test Execution:** Execute the test cases according to the test plan, record test results, and identify any deviations from expected outcomes, documenting defects and issues for resolution.
4. **Defect Tracking and Management:** Track and prioritize identified defects using a defect tracking system, and collaborate with development teams to investigate and resolve issues in a timely manner.
5. **Regression Testing:** Perform regression testing to ensure that changes or fixes do not introduce new defects or regressions in previously tested functionalities.
6. **User Acceptance Testing (UAT):** Involve end users or stakeholders in UAT to validate that the system meets business requirements and expectations before deployment.

**b) Types of logical security control measures:**

1. **Access Control Lists (ACLs):** Define rules or policies that specify which users or systems are granted or denied access to resources based on predefined criteria such as IP addresses, ports, or protocols.
2. **Encryption:** Protect sensitive data by converting it into an unreadable format using cryptographic algorithms, ensuring that only authorized parties with the proper decryption keys can access or decipher the information.
3. **Authentication Mechanisms:** Verify the identity of users or entities accessing the system, such as passwords, biometrics, smart cards, or multi-factor authentication (MFA), to prevent unauthorized access or impersonation.
4. **Digital Signatures:** Provide a means for verifying the authenticity and integrity of digital documents or messages by using cryptographic techniques to create unique digital signatures that can be validated by recipients.
5. **Intrusion Detection and Prevention Systems (IDPS):** Monitor network traffic and system activities for signs