Assignment: 4

Sub: Cyber Security

Name : Shivam Sagpariya

Enroll : 91800103191

Question 1: Definitions

1) **Computer Forensics:** Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media.

2) **Digital Forensics:** Digital Forensics in Cyber Security Defined, They're the people who collect, process, preserve, and analyze computer-related evidence. They help identify network vulnerabilities and then develop ways to mitigate them. They go deep inside networks, computers, and smartphones in search of evidence of criminal activity.

3) **Information Security Management System (ISMS):** An information security management system (ISMS) is a framework of policies and controls that manage security and risks systematically and across your entire enterprise—information security.

4)Electronic record : The **electronic record** meaning is best described in the legal recognition of **electronic records**, digital signatures, and associated topics, for which the following provisions of the IT Act, 2000 was formulated. For any important point to become a law, it is needed to be written, printed, or typewritten.

5)Intellectual Property Rights (IPR) : Intellectual Property Rights (**IPRs**) are legal **rights** that protect creations and/or inventions resultingfrom **intellectual** activity in the industrial, scientific, literary or artistic fields. The most common **IPRs** include patents, **copyrights**, marks and trade secrets.

Question 2: Write a short note.

1) Draw the process model for understanding a seizure and handlingof forensics evidence. The main task of any digital forensics investigation is to acquire, preserve, examine and present digital evidence to be used in the court of law, so what is meant by the term digital evidence? Digital evidence (also known as electronic evidence) is any information stored or transmitted in digital format, this includes data found on computers, laptops, cell phones, tablet, PDA hard drives, and all data stored using various storage device media such as USB thumb drive, SD cards, external hard drive, CD/DVD. Data transmitted via computer networks is also considered a part of digital evidence in addition to op;erating systems and database logs.

Digital evidence should be acquired in a Forensically Sound manner. "Forensically Sound" is a term used by digital forensics examiners to describe the process of acquiring digital evidence while preserving its integrity to be admissible in a court of law. **Evidence Handling:**

Different jurisdictions have different requirements for digital evidence handling procedures; some of these are defined in Chapter 1, Section 1.1.6. This is not a definitive list. In Europe, the Budapest Convention on Cybercrime was the first international treaty seeking to address computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. This has met with success, and while it is an European initiative, a number of other nations have ratified it, and as at the time of writing, these are given in Appendix 1.

Search and Seizure:

Once the scene is secured and thoroughly documented, investigators work to seize evidence. But the goal of seizing evidence is not to seize everything at the scene. Through the knowledge and experience of trained investigators, educated decisions can be made about what

evidence need to be seized and then documenting the justifications for doing so.

Digital evidence comes in many forms, such as application logs, network device configurations, badge reader logs, or audit trails. Given that these are only examples and depending on the scope of the investigation, there are potentially significantly more relevant evidence forms. Identifying and seizing all evidence can prove to be a challenging task to which technical operating procedures will provide guidance and support. However, from time to time, investigators might encounter situations where these technical operating procedures do not address collecting a specific evidence source. In these situations, the importance of having trained a digital forensic professional is essential in having the knowledge and skills necessary to apply the fundamental principles, methodologies, and techniques of forensic science in seizing the evidence.

2) Explain How the "Chain of Custody" Concept applies in computer/digital Forensics.

Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases. Each step in the chain is essential as if broke, the evidence may be rendered inadmissible. Thus we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.

What the Chain of Custody entails in Digital Cyber Forensics?

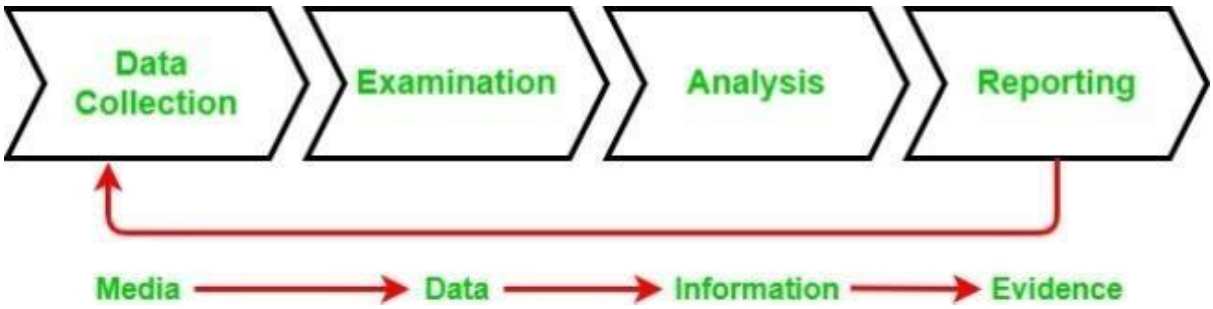
If you are in the field of Cyber

Security, you will be at one point in your career will be involved in Digital Forensics. One of the concepts that is most essential in Digital Forensics is the Chain of Custody.

The chain of custody in digital cyber forensics is also known as the paper trail or forensic link, or chronological documentation of the evidence.

Chain of Custody Process

In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.



1. Data Collection: This is where the chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.
2. Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
3. Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are

used to derive useful information to address questions posed in the particular case.

4. Reporting: This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:

    - Statement regarding Chain of Custody.
    - Explanation of the various tools used.
    - A description of the analysis of various data sources.
    - Issues identified.
    - Vulnerabilities identified.
    - Recommendation for additional forensics measures that can be taken.

3) Briefly explain the role of computer forensics investigator. As the name implies, forensic computer investigators and digital forensic experts reconstruct and analyze digital information to aid in investigations and solve computer-related crimes. They look into incidents of hacking, trace sources of computer attacks, and recover lost or stolen data.

The job of a forensic computer investigator or digital forensic expert often includes:

Recovering data from damaged or erased hard drives
Tracing hacks
Gathering and maintaining evidence
Writing and reviewing investigative reports
Working with computers and other electronic equipment
Working closely with other police officers and detectives

Forensic computer investigators and

digital forensic experts may conduct internal or external investigations. In fact, in many cases, they may be called upon more often to investigate in-house personnel.

Private companies and government organizations may hire forensic computer investigators full time, or they may contract for their services. The investigators will likely be involved in looking for violations of company policies regarding computer use as much as they will be involved in crime-solving. They work closely with other investigators and attorneys.

4) What is Trap and Trace? trap and trace security system is designed to trap a cybercriminal when he/she intrudes unauthorized into a network system and trace his identity and inform the necessary official authority to deal with the data theft or unauthorized entry.

The trap features a Honeypot or a padded cell along with an alarm to notify the security professionals that the cybercriminal has compromised the security and has made his entry onto the network system.

While the trace feature works similar to the caller ID feature where the ID of the caller is traced and located, similarly its traced and validated whether the criminal is an outsider or an insider.

Question 3: Give the answer in detail.

1) Explain Phase of Computer Forensics/Digital Forensics

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. The term digital forensics was first used as a synonym for computer forensics. Since then, it has expanded to cover the investigation of any devices that can store digital data. Although the first computer crime was reported

in 1978, followed by the Florida computers act, it wasn't until the 1990s that it became a recognized term. It was only in the early 21st century that national policies on digital forensics emerged.

Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.

1. **Identification**
   - First, find the evidence, noting where it is stored.
   - The first stage identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.
2. **Preservation**
   - Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.
   - the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.
3. **Analysis**
   - Next, reconstruct fragments of data and draw conclusions based on the evidence found.
   - an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.
4. **Documentation**

- Following that, create a record of all the data to recreate the crime scene.
- collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.

5. **Presentation**

- Lastly, summarize and draw a conclusion.
- firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.

2) What is ISMS? Lis out benefits of ISO 27001.

"Information Security Management System" is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. ISMS always follows Plan-Do-CheckAct methodology.

The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.

The Do phase involves implementing and operating the controls.

The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.

In the Act phase, changes are made where necessary to bring the ISMS back to peak performance

ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS)

FEATURES OF ISMS:

Adopted PDCA (PLAN – DO – CHECK – ACT) Model

Adopted a Process Approach

Identify – Manage Activities – Function Effectively

Stress On Continual Process Improvements

Scope covers Information Security not only IT Security

Focused on People, Process, Technology

Resistance to intentional acts designed to cause harm or damage to the Organisation.

Combination of Management Controls, Operational Controls and Technical Control.

Overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information security.

BENEFITS OF ISMS CERTIFICATION:

Certifying your ISMS against ISO/IEC 27001 can bring the following benefits to your organization:

Independent framework that will take account of all legal and regulatory requirements.

Gives the ability to demonstrate and independently assure the internal controls of a company (corporate governance)

Proves senior management commitment to the security of business information and customer information

Helps provide a competitive edge to the company

Formalizes, and independently verifies, Information Security processes, procedures and documentation

Independently verifies that risks to the company are properly identified and managed

Helps to identify and meet contractual and regulatory requirements

Demonstrates to customers that security of their information is taken seriously

3)Define file system. Explain NTFS Disk and NTFS Encrypting File System. The **Encrypting File System** (**EFS**) on Microsoft Windows is a feature introduced in version 3.0 of NTFS[1] that provides filesystemlevel encryption. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.

When an operating system is running on a system without file encryption, access to files normally goes through OS-controlled user authentication and access control lists. However, if an attacker gains physical access to the computer, this barrier can be easily circumvented. One way, for example, would be to remove the disk and put it in another computer with an OS installed that can read the filesystem; another, would be to simply reboot the computer from a boot CD containing an OS that is suitable for accessing the local filesystem.

The most widely accepted solution to this is to store the files encrypted on the physical media (disks, USB pen drives, tapes, CDs and so on).

In the Microsoft Windows family of operating systems EFS enables this measure, although on NTFS drives only, and does so using a combination of public key cryptography and symmetric key cryptography to make decrypting the files extremely difficult without the correct key.

However, the cryptography keys for EFS are in practice protected by the user account password, and are therefore susceptible to most password attacks. In other words, the encryption of a file is only as strong as the password to unlock the decryption key.

EFS works by encrypting a file with a bulk symmetric key, also known as the File Encryption Key, or FEK. It uses a symmetric encryption algorithm because it takes less time to encrypt and decrypt large amounts of data than if an asymmetric key cipher is used. The symmetric encryption algorithm used will vary depending on the version and configuration of the operating system; see Algorithms used by Windows version below. The FEK (the symmetric key that is used to encrypt the file) is then encrypted with a public key that is associated with the user who encrypted the file, and this encrypted FEK is stored in the $EFS alternative data stream of the encrypted file.[5] To decrypt the file, the EFS component driver uses the private key that matches the EFS digital certificate (used to encrypt the file) to decrypt the symmetric key that is stored in the $EFS stream. The EFS component driver then uses the symmetric key to decrypt the file. Because the encryption & decryption operations are performed at a layer below NTFS, it is transparent to the user and all their applications.

Folders whose contents are to be encrypted by the file system are marked with an encryption attribute. The EFS component driver treats this encryption attribute in a way that is analogous to the inheritance of file permissions in NTFS: if a folder is marked for encryption, then by default all files and subfolders that are created under the folder are also encrypted. When encrypted files are moved within an NTFS volume, the files remain encrypted. However, there are a number of occasions in which the file could be decrypted without the user explicitly asking Windows to do so.

Files and folders are decrypted before being copied to a volume formatted with another file system, like FAT32. Finally, when encrypted files are copied over the network using the SMB/CIFS protocol, the files are decrypted before they are sent over the network. The most significant way of preventing the decryption-on-copy is using backup applications that are aware of the "Raw" APIs. Backup applications that have implemented these Raw APIs will simply copy the encrypted file stream and the $EFS alternative data stream as a single file. In other words, the files are "copied" (e.g. into the backup file) in encrypted form, and are not decrypted during backup.

4)Explain the offences and penalties under the Copyright Act 2000?

The Government of India enacted its Information Technology Act 2000 with the objectives stating officially as:

“to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the

Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

What does IT Act 2000 legislation deals with?

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Why did the need for IT Amendment Act 2008 (ITAA) arise?

The IT Act 2000, being the first legislation on technology, computers, ecommerce and ecommunication, the was the subject of extensive debates, elaborate reviews with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some obvious omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the IT Act also being referred in the process with the reliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the **Information**

Technology Amendment Act 2008 was placed in the Parliament and passed at the end of 2008 (just after Mumbai terrorist attack of 26 November 2008 had taken place). The IT Amendment
Act 2008 got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

5) Discuss Section 65, 66B, 66C, 66D, 66E,66F with Punishment under ITA 2000.

Section 65 – Tampering with Computer Source Documents
Related Case: Syed Asifuddin and Ors. Vs. The State of Andhra PradeshIn this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocomm.
Verdict: *Court held that tampering with source code invokes Section 65 of the Information Technology Act.* **Section 66 – Computer Related offenses**
Related Case: Kumar v/s Whiteley In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.

Verdict: *The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G*
Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Section 66A – Punishment for sending offensive messages through communication service

Relevant Case #1: ***Fake profile of President posted by imposter*** On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President

Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook.The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Relevant Case #2: Bomb Hoax mail In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1p.m. on May 25, the news channel received an email that read: "I have planted five bombs in Mumbai; you have

two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

Section 66C – Punishment for identity theft *Relevant Cases:*

The CEO of an identity theft protection company, Lifelock, Todd Davis's social security number was exposed by Matt Lauer on NBC's Today Show. Davis' identity was used to obtain a $500 cash advance loan.

Li Ming, a graduate student at West Chester University of Pennsylvania faked his own death, complete with a forged obituary in his local paper. Nine months later, Li attempted to obtain a new driver's license with the intention of applying for new credit cards eventually.

Section 66D – Punishment for cheating by impersonation by using computer resource

Relevant Case: Sandeep Vaghese v/s State of Kerala

A complaint filed by the representative of a Company, which was engaged in the business of trading and distribution of petrochemicals in India and overseas, a crime was registered against nine persons, alleging offenses under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code. The company has a web-site in the name and and style `www.jaypolychem.com' but, another web site `www.jayplychem.org' was set up in the internet by first accused Samdeep Varghese @ Sam, (who was dismissed from the company) in conspiracy with other accused, including Preeti and Charanjeet Singh, who are the sister and brotherinlaw of `Sam'

Defamatory and malicious matters about the company and its directors were made available in that website. The accused sister and brother-inlaw were based in Cochin and they had been acting in collusion known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.

Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to malign the name and image of the Company and its Directors. The defamation campaign run by all the said persons named above has caused immense damage to the name and reputation of the Company.

The Company suffered losses of several crores of Rupees from producers, suppliers and customers and were unable to do business.

Section 66E – Punishment for violation of privacy *Relevant Cases:*

Jawaharlal Nehru University MMS scandal In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university.Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.

Nagpur Congress leader's son MMS scandal On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

Section-66F Cyber Terrorism

Relevant Case: The Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case.The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday.The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo framemaker in Patna,'' said an officer.

Status: *The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act.*

Section 67 – Punishment for publishing or transmitting obscene material in electronic form

Relevant Case:This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the lady's complaint, the police nabbed the accused.Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through internet.

Verdict: *The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000. He is convicted and sentenced for the offence as follows:*

As per 469 of IPC he has to undergo rigorous imprisonment for 2 years and to pay fine of Rs.500/-

As per 509 of IPC he is to undergo to undergo 1 year Simple imprisonment and to pay Rs
500/-

As per Section 67 of IT Act 2000, he has to undergo for 2 years and to pay fine of Rs.4000/

Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Relevant Case: *Janhit Manch & Ors. v. The Union of India 10.03.2010*
Public Interest Litigation: The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

6)Discuss the powers and functions of Controller of Certifying Authorities under the Information Technology Act, 2000?

The Controller may perform all or any of the following function, namely:-

(a) exercising supervision over the activities of Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authority shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key; (g) specifying the form and content of a Digital Signature Certificate and the key;

(h) specifying the form the manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data-base containing the disclosure record of ever Certifying Authority containing such particulars as may be specified by regulations which shall be accessible to public.