CSC 2735
Dipesh Tha Shrestha
Third Semester

Programme Name: **BCS HONS**

Course Code: **CSC 2735**

Course Name: **Network And Data Security**

Assignment / Lab Sheet / Project / Case Study No. **1**

Date of Submission: **2020/6/12**

Submitted By:

Student Name**: Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester**: Third Semester**

Intake**: September 2019**

Submitted To:

Faculty Name**: Manoj Gautam**

Department**: LMS**

CSC 2735
Dipesh Tha Shrestha
Third Semester

1. **Explain Term Information Security, Network Security, and Internet Security.**

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

CSC 2735
Dipesh Tha Shrestha
Third Semester

2. Explain the concept of CIA Triad.

Answer:

The **CIA triad** is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure. The model has nothing to do with the U.S. Central Intelligence Agency; rather, the initials stand for the three principles on which infosec rests:

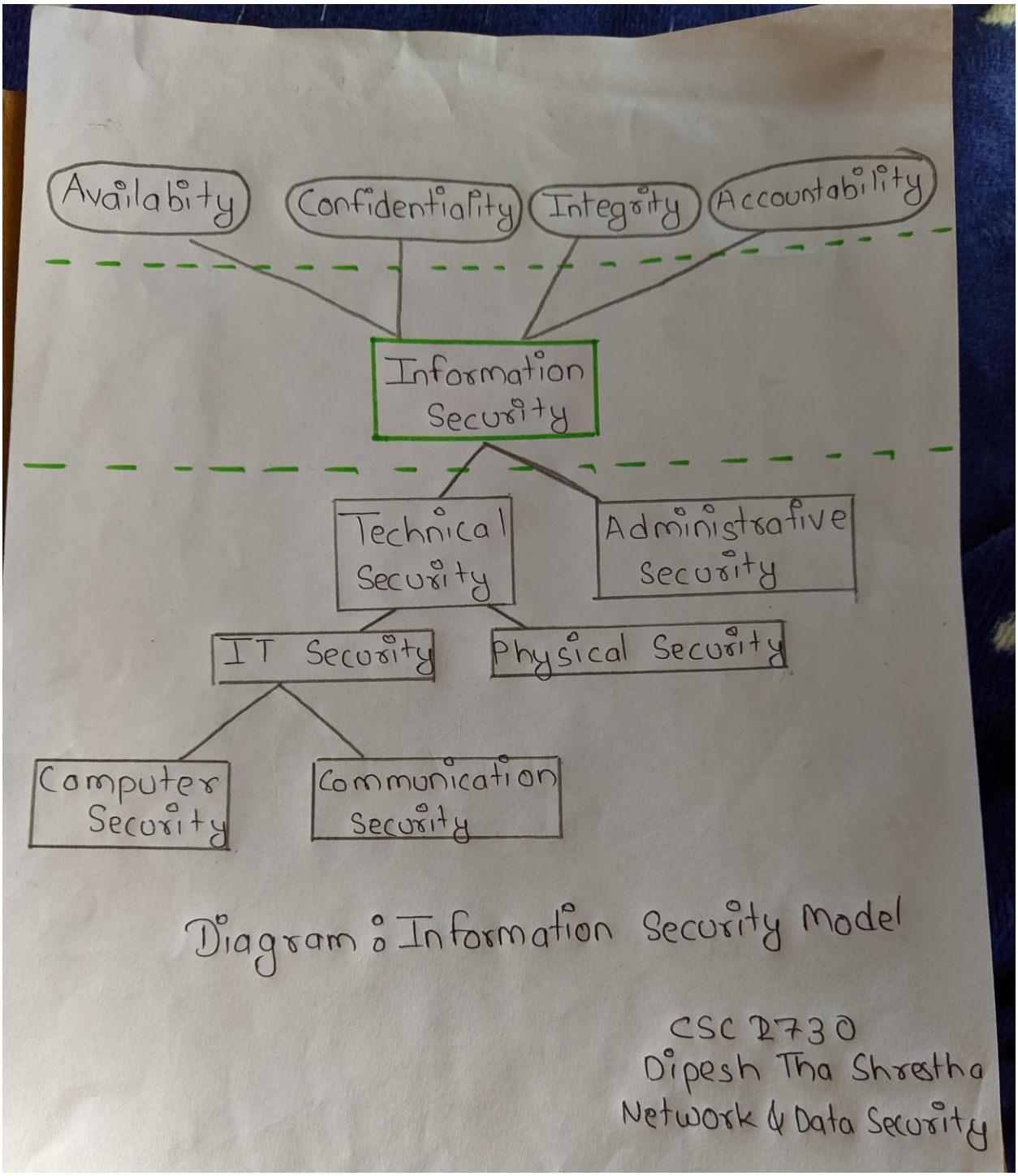
- **Confidentiality**: Only authorized users and processes should be able to access or modify data.
- **Integrity:** Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously.
- **Availability**: Authorized users should be able to access data whenever they need to do so.

Chances are you have noticed a trend here - the CIA Triad is all about information. While this is considered the core factor of the majority of IT security, it promotes a limited view of the security that ignores other important factors. For example, even though availability may serve to make sure you don't lose access to resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

CSC 2735
Dipesh Tha Shrestha
Third Semester

3. Draw a labelled diagram of Information Security Model.



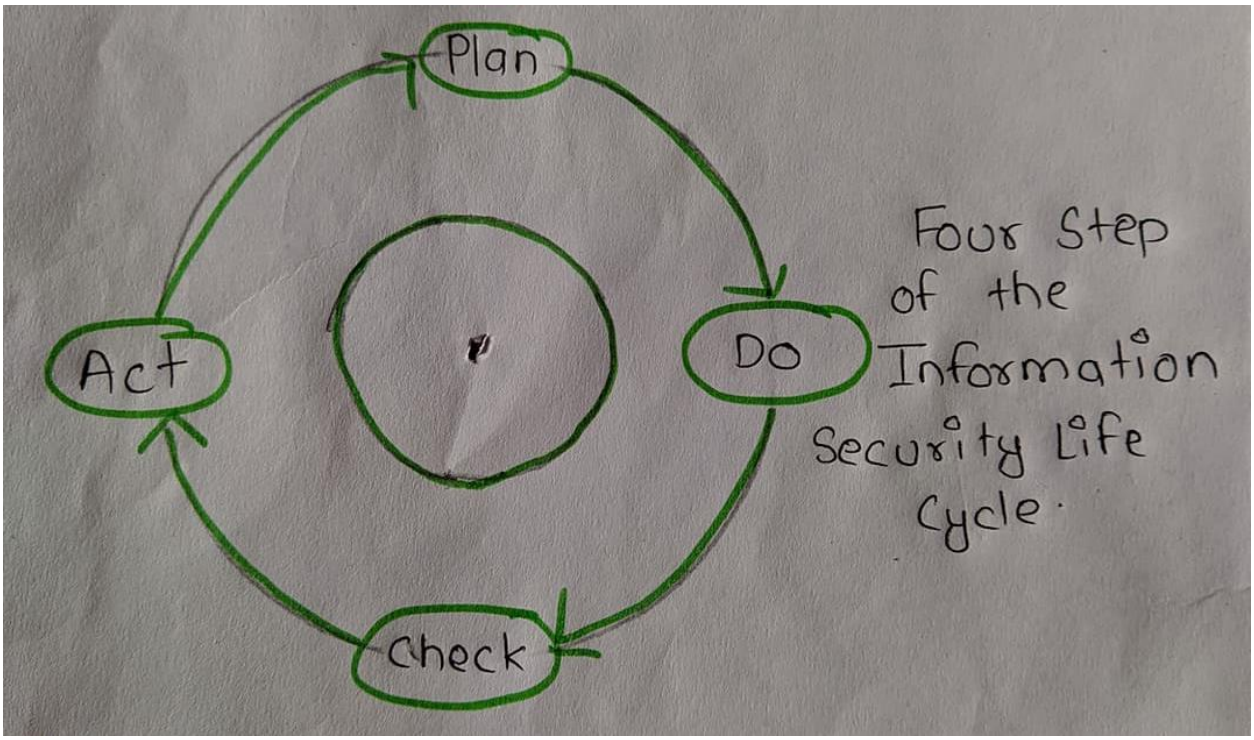
CSC 2735
Dipesh Tha Shrestha
Third Semester

4. **Explain Information security life cycle with neat and clean diagram.**

Answer:

Information security is a living, breathing process that's ongoing, it's a life cycle. Without a life-cycle approach to information security and its management, organizations typically treat information security as just another project. Projects have a beginning and ending date. Once completed, resources are shifted to the next hot initiative and focus shifts away from security. Information Security is a business decision after all and who makes business decisions for organizations? Hint – it's NOT the good folks in IT. Understanding and managing risk for an organization is a critical component of information security. Once Executive Management is informed of an identified risk they can decide how they will address the risk so the information security life cycle can begin. This will eliminate the "information security is just another IT project" mentality and help give direction and support so that the focus can be on the organizational goals.

CSC 2735
Dipesh Tha Shrestha
Third Semester



Step one – Plan

Involve senior management as well as stake holders and department managers. Information security is not just an IT issue, the whole organization needs to be on board in order to have a strong information security program. Form a committee and establish agreed on direction.

Step two – Do

Assign specific responsibility to individuals, determine timelines and desired results. Develop a “cookbook” that lays out policies, standards, procedures, and guidelines that can be followed to maintain a strong information security program. Just as parts of “recipes” may change over time, parts of your information security program may change as well.

Step three – Check

After solutions are implemented, review the audit findings to determine if the desired results are being achieved.

CSC 2735
Dipesh Tha Shrestha
Third Semester

Step four – Act

These actions should be based on your audit results, with adjustments made as needed. Circle back to the Planning step and run through the process again until the threat is reduced to an acceptable level.

5. **List and explain four types of Active attacks**.

An **active attack**, in computing security, is an attack characterized by the attacker attempting to break into the system. During an active attack, the intruder may introduce data into the system as well as potentially change data within the system.

Types of active attacks include:

- Denial of service (DoS)
- Distributed Denial of Service (DDoS)
- Session replay
- Masquerade
- Message modification
- Trojans

Denial-of-service attacks prevent the normal use or management of communication services, and may take the form of either a targeted attack on a particular service or a broad, incapacitating attack. For example, a network may be flooded with messages that cause a degradation of service or possibly a complete collapse if a server shuts down under abnormal loading. Another example is rapid and repeated requests to a web server, which bar legitimate access to others. Denial-of-service attacks are frequently reported for internet-connected services.

Masquerade attacks, as the name suggests, relate to an entity (usually a computer or a person) taking on a false identity in order to acquire or

modify information, and in effect achieve an unwarranted privilege status. Masquerade attacks can also incorporate other categories.

Message replay involves the re-use of captured data at a later time than originally intended in order to repeat some action of benefit to the attacker: for example, the capture and replay of an instruction to transfer funds from a bank account into one under the control of an attacker. This could be foiled by confirmation of the freshness of a message.

Message modification could involve modifying a packet header address for the purpose of directing it to an unintended destination or modifying the user data.

6. Explain Interruption, Interception and DOS attack.

Interruption: This type of attack is due to the obstruction of any kind during the communication process between one or more systems. So the systems which are used become unusable after this attack by the unauthorized users which results in the wastage of systems. In an interruption, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.

Interception: The phenomenon of confidentiality plays an important role in this type of attack. The data or message which is sent by the sender is intercepted by an unauthorized individual where the message will be changed to the different form or it will be used by the individual for his malicious process. So the confidentiality of the message is lost in this type of attack.

Dos Attack: A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks

accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.