Gelila Gossa
CYSE 200

1. Briefly define each of the three members of the information security triad.
    - The three members are **Confidentiality**; being able to restrict people from seeing given information. **Integrity**, the assurance that the Information accessed cannot be altered. **Availability** meaning the information can be accessed and modified by anyone authorized.

2. What does the term authentication mean?
    - Is a process of verifying a user's identity through a device that prevents unauthorized access to a program.

3. What is multi-factor authentication?
    - It is used to assure online users to have at least two verifying evidence to prove their identity

4. What is role-based access control?
    - It prevents network access based on the individuals position with an organization. It has levels of access.

5. What is the purpose of encryption, and fundamentally how does it work?
    - The main purpose of encryption is to protect confidential information over the internet. It uses the internet to scramble or encrypt data.

6. What is pretexting and how does it represent a threat in the Cyber Security landscape?
    - Pretexting is like a cyber-attack (scam) that involves an attacker and the victim. This is a threat to cyber security because you because the attacker uses personal information convincing you to get access to sensitive data.

7. What's the point in backups & what are the components of a good backup plan?
    - Backups are used to copy, save and recover data. A good backup plan is having at least saving three copies of the data that is stored on different devices.

8. What is a firewall?

- Is a security network that helps traffic malicious activity based on the organization's security guidelines?

9. Discuss various types of Firewalls.
    - Cloud firewall
    - Hardware firewall
    - Next-gen firewall
    - Packet filtering firewall
    - Proxy firewall

10. What does the term physical security mean and how does it apply to Cyber Security?
It's the protection of important data, confidential information and equipment. It denies access to facilities. i.e. using an office ID to access the office building.