**Assignment for Lesson 1 – Security Basics and Mindsets**

**TRUE/FALSE QUESTIONS (6 points each):**

T F 1. Computer security is protection of the integrity, availability, and

confidentiality of information system resources.

T F 2. Computer security is essentially a battle of wits between a perpetrator

who tries to find holes and the administrator who tries to close them.

T F 3. Many security administrators view strong security as an impediment to

efficient and user-friendly operation of an information system.

T F 4. The first step in devising security services and mechanisms is to

develop a security policy.

**MULTIPLE CHOICE QUESTIONS (6 points each):**

1. \_\_\_A\_\_\_\_ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

A. System Integrity C. Data Integrity

B. Availability D. Confidentiality

2. A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy is a(n) \_\_\_\_\_\_C\_\_\_.

A. countermeasure C. vulnerability

B. adversary D. risk

3. A(n) \_\_\_\_A\_\_\_ is an attempt to learn or make use of information from the system that does not affect system resources.

A. passive attack C. inside attack

B. outside attack D. active attack

4. Masquerade, falsification, and repudiation are threat actions that cause \_\_\_\_\_\_\_\_\_\_ threat consequences.

A. unauthorized disclosure C. deception

B. disruption D. usurpation

5. The \_\_\_\_\_\_\_\_\_ prevents or inhibits the normal use or management of communications facilities.

A. passive attack C. traffic encryption

B. denial of service D. masquerade

6. The assurance that data received are exactly as sent by an authorized entity is \_\_\_D\_\_\_\_.

A. authentication C. data confidentiality

B. access control D. data integrity

**SHORT ANSWER QUESTIONS (8 pointe each):**

1. Confidentiality, Integrity, and Availability form what is often referred to as the \_CIA\_\_.

2. A(n) \_\_\_attack\_\_\_ is a threat that is carried out and, if successful, leads to an undesirable violation of security, or threat consequence.

3. Misappropriation and misuse are attacks that result in \_\_\_\_\_\_\_\_ threat consequences.

4. Release of message contents and traffic analysis are two types of \_\_\_\_\_\_\_\_\_ attacks.

5. Security implementation involves four complementary courses of action: prevention, detection, response, and \_recovery and remediation\_\_\_.