**Assignment 8 – Database Security Review Questions (100 points)**

**Instructions: *Use the readings from Database Systems Chapter 16*** *to**answer each of the following questions. Submit your complete assignment in Blackboard.*

1. **Define the below key terms (25 points)**
   1. Security threat: attacks that threaten the security of a system, database, or program.
   2. Security Breach: Incident that leads to the exposure of sensitive information. Can be purposeful or accidental.
   3. Audit log: A chronological record of any activity within a database, system, program, etc. Keeps track of access or any
   4. Authorization management: Certain roles or people may have access to information or data, but authorization management will control the access given.
   5. Security vulnerability: Potential risks or issues that could happen given a specific incident or underlying issue.
2. **What are the three database security goals? (15 points)**
   1. **Confidentiality, Integrity, Availability**
3. **How do you normally define security? How is your definition similar to or different from the definition of database security in this chapter? (15 points)**
   1. **I define security as protections in place to keep something or someone safe. It is similar to database security as in this chapter, database security is described as rules and constraints in place to ensure the security of the data. Both definitions ensure security of an entity, but database security is primarily about data.**
4. **What are the levels of data confidentiality? (15 points)**
   1. **People, workstation and servers, operating system, applications, network, data**
5. **What are security vulnerabilities? What is a security threat? Give some examples of security vulnerabilities in different information system components. (15 points)**
   1. **A security threat is defined as “imminent security violation”; something that can threaten the security of a database. A security vulnerability is something that a security threat can take advantage of; potentially user errors or weaknesses within the database. A potential security vulnerability is simply leaving your computer unlocked and unattended. Potential attackers could easily gain access by just sitting at the computer. Within the system, another security vulnerability would be easy to guess passwords like birthdays or important names. Attackers would easily be able to hack and gain significant information that could potentially never be recovered.**
6. **What is a security policy? How does it contribute to system security? (15 points)**
   1. **A security policy is a constraint or rule set in place to ensure consistency and protect against any potential threats. It contributes to system security as these policies are specifically set in place to defend the information and catch any issues earlier before they could arrive.**