|  |  |  |
| --- | --- | --- |
| animatedLOGO |  **Assignment No. 01 Semester: Fall 2019****CS205: Information Security** | **Total Marks: 15****Due Date: 14/11/2019** |
| **Instructions:**Please read the following instructions carefully before submitting assignment:You need to use MS word document to prepare and submit the assignment on VU-LMS.It should be clear that your assignment will not get any credit if:* The assignment is submitted after due date.
* The assignment is not in the required format (doc or docx)
* The submitted assignment does not open or file is corrupt.
* Assignment is copied (partial or full) from any source (websites, forums, students, etc)

**Objectives:**To enhance the learning capabilities of the students about: * Security model
* OSI security architecture
 |
| **Assignment**  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Question No.1:**Carefully study the scenarios given below with respect to C.I.A triangle and identify the C.I.A. security component associated with each scenario. You are required to provide your answer in table given below:1. Student’s grade information is considered very important and it should be available only for that specific student rather than other students.
2. Information of heart patient is stored in hospital’s database. The doctor trusts on that stored information and then suggests medicine according to this information. Another employee who has also legal rights to access this database, unintentionally changes this information that can misguide the patient treatment.
3. VU-LMS is not accessible due to which students are not able to submit their assignments on time.
4. An ATM machine is not responding due to general processing error.
5. Employee’s salary slip in an organization should not be visible to any other employee.
6. Product price and specification available on online shopping store is changed by unauthorized person.
7. You are replying to an email of your friend then it should be received in original form as it is sent by you.
8. Your academic marks are posted on social media website by some unauthorized person.
9. A student is checking his/her result online but website is not responding.
10. A multinational company makes a plan for launching a new product for capturing customers in a market but this plan leaked to its competitor.

**Solution:**

|  |  |
| --- | --- |
| **Scenario. No** | **Associated C.I.A security component** |
| 1 | Confidentiality  |
| 2 | Integrity  |
| 3 | Availability  |
| 4 | Availability |
| 5 | Confidentiality  |
| 6 | Integrity  |
| 7 | Integrity  |
| 8 | Confidentiality  |
| 9 | Availability  |
| 10 | Confidentiality  |

**Question No.2:**OSI architecture was developed as an international standard to define the requirements for security and characterizing the way to satisfy that requirements. You are required to carefully study the OSI security architecture then identify and relate the following scenarios with security services provided by OSI. You are required to provide your answer in table given below:1. A person, transferring money to his friend using online banking service. Both the bank and the user should be guaranteed in identities of each other.
2. In online banking application a user may be allowed to see his profile, but not allowed to make any changes in his profile information.
3. A user withdraw money from his bank account, but later denied that. How the bank can handle such situation?
4. A user wants to pay his electricity bill using online banking service but website of that bank is down in that time.
5. A user sends a query to bank head office to know about his closing balance and he should receive same balance amount as sent by bank authorities.

**Solution:**

|  |  |
| --- | --- |
| **Scenario. No** | **Security Service by OSI** |
| 1 | Authentication  |
| 2 | Access control  |
| 3 | Non repudiation |
| 4 | Data confidentiality  |
| 5 | Data integrity  |

 |