Name: Aristotle Buenaventura  
Student No: 2013752  
Program: BSIT

1.What are the main areas of security? this is most commonly known as CIA triad. briefly explain each of the area;

The CIA triad and information security mean confidentiality, integrity, and availability. It’s an organizational model designed to guide information storing policies. Its three elements are considered the three most crucial components of security.

Confidentiality is a set of rules that limits access to information, it’s comparable to privacy. Ensuring confidentiality means that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access. This can be accomplished through methods like data encryption, two-factor authentication, and biometric verification. As an example, the only authorized teacher should have access to the students’ grade information. Another example, customers expect that the personal information they provide to a store such as credit card information or contact number will be protected in a way that prevents unauthorized people to access it.

Integrity is the assurance that the information is trustworthy and accurate, it involves maintaining data consistency and accuracy over its entire lifecycle. Integrity is about ensuring that data has not tampered so, data can be trusted. It is correct, authentic, and reliable. As an example, banking customers expect that their banking information and account balances have not tampered. Data must not change and must be protected from alteration by unauthorized people. User access controls must be in place and backups must be available for restoring affected data. Some risks involved with not protecting the integrity of data are fraud and information that is no longer reliable or accurate.

Availability is the guarantee of reliable access to the information that can be accessed only by authorized people and make sure that the services of an organization are always available. Availability measures protect timely and uninterrupted access to the system. Its countermeasures to protect system availability are as far-ranging as the threats to availability. Systems that have a high requirement for continuous uptime should have significant hardware redundancy with backup servers and data storage immediately available.

2. As an aspirant application developer, can you list some design considerations of a secured application/information system? you may suggest at least 3 design considerations.

As a future web developer, I will enforce a strong password policy to my future website to avoid the account to be easily hacked. Users need to use a strong password because hackers utilize software that uses force to crack passwords. Passwords should be complex, containing an uppercase letter, lowercase letters, numerals, and special characters. The user’s password should be at least 10 characters long.

Furthermore, encryption of login data is a must for my future website so that sensitive information such as usernames, passwords, credit card numbers, and other personal information to be transmitted securely. All information that entered in the website will be encrypted so that it is meaningless to any third party who may try to breach the page. This helps to prevent hackers from accessing your login credentials or other private data.

Finally, my future website will have automatically back up the important files regularly. So, in case my website become inaccessible or data is lost, I will have the backup files for it. Web host providers should provide backups of their servers, but I should still backup my files regularly.