Laboratory Exercise
Data Security VS Data Privacy

Objective:

At the end of the exercise, the students should be able to:

- Compare data security and data privacy.

Materials:

- Internet connection
- MS Office

Procedures:

1. Read the blog post entitled “Data Security Vs Data Privacy: An Imperative Distinction to Protect Data” by StealthLabs below.

   In the present digital world, organizations face a multitude of challenges related to the privacy and security of employee, consumer, and client data. The sheer volumes of data that enterprises handle and store is growing and drive a greater need for data protection practices. In addition, computing environments have become highly complex, routinely spanning the cloud, the enterprise data center, and numerous devices ranging from IoT sensors to remote servers.

   This complexity proliferates the attack surface, making it more challenging for organizations to monitor and secure data. Thus, it has become crucial for organizations to incorporate data security and data privacy policies into a sound data governance strategy to prevent data breaches and achieve legal compliance. Unfortunately, many organizations believe that their data security policy covers data privacy and vice versa. They often use data security and data privacy interchangeably.

   Data Security is commonly referred to as confidentiality, availability, and integrity of information. It is all about the practices and procedures that focus on protecting personal information from unauthorized access, data breaches, cyberattacks, and accidental or intentional data loss. Data security ensures that data is accurate and reliable and is available for authorized users. A data security plan includes resilient data storage technologies, encryption solutions, data erasure, data masking, physical and logical access controls, breach response, and multi-factor authentication.

   Whereas Data Privacy is concerned with the procedures and policies that govern the collection, storage, sharing, and usage of Personally Identifiable Information (PII) and proprietary corporate information. It refers to the rules and regulations that ensure personal or private information is being controlled on par with the preferences of the concerned individual(s).

   The best way to understand the distinction between data security and data privacy is to consider the mechanisms used in both cases. An organization may have effective and robust data security, yet the procedure or process by which information was collected and handled might violate the privacy policy. For instance, an organization might ensure data security by encrypting, masking, and properly accessing the data. But if it gathers that information

improperly, for instance, without any proper consent from the concerned individual, the organization has violated data privacy requirements even though data security remains unbreeched. Therefore, organizations must understand that data security can be achieved without data privacy. However, data privacy cannot be achieved without data security.

2. Answer the following questions:
    a. What is the article all about?
    b. Why do you think it is important to know the difference between data security and data privacy based on the article?
    c. Do you agree with the article? Why or why not?
3. Place your answer on MS Word. Once done, save your work with the filename <**Last name_First name_Lab1**> (ex. San Juan_Ariel_Lab1) and call the attention of your instructor. Have it saved on his/her FTP account.

GRADING RUBRIC:

Criteria/Scoring	0 – 35	36 – 70	71 – 100	Score
Procedure Execution	No output is done.	Explained the article and gave some examples.	Provided examples and explained the article clearly.	/100
			TOTAL	**/100**

Reference:

StealthLabs (2020, October 1). *Data Security Vs Data Privacy: An Imperative Distinction to Protect Data.* Retrieved from https://www.stealthlabs.com/blog/data-security-vs-data-privacy-an-imperative-distinction-to-protect-data/ on January 28, 2021