Project 1

Josephus West

School or Institution Name (University at Place or Town, State)

**Introduction:**

Open data is referred to as the data related to various fields of life made available to general public by the government. Such information made available to masses can create value and enable the delivery of services to the public more efficient. Although the concept of providing confidential data for public domain research and development the initiative has proved its potential in various fields of life. Researchers are able to consult the data made available by the government. Alongside the amazing benefits of making the data public there are growing concerns of information assurance (Dove, 2018). Information assurance deals with the confidentiality, integrity, availability, and non-repudiation of the data. It is inevitable for the government and executives to ensure the basic levels of information assurance for the open data. The paper describes the best practices for the executives of the government office to ensure the confidentiality, integrity, availability, and non-repudiation of the open data.

**Benefits of the open data:**

Open data made available to the public for research and development by governmental institutions has the potential to unlock $3 trillion to economic value across various sectors. Open data is being used by the crop scientists to understand the disease data over a large spectrum using big data analysis techniques. It has enabled the scientists and businesses to not only analyze the available data but to prepare future trends as well. Scientists can predict future disease patterns and can prepare cure for those diseases. Businesses are harnessing the power of the open data to provide customized services to their clients adding value to their existing product lines. As an example to the beneficial use of the open data is that electric power supply companies are now able to advise their users for energy saving tips based on the analysis of the big data available to them by the open data initiative (Lynskey, 2018). There are endless possibilities that the open data can add value to businesses across the spectrum. Healthcare providers are able to provide patients and general public with the ability to track their medical bills. They are even able to suggest future trends for the medical bills based on the similarities and correlation patterns of the available open data. A major breakthrough has been developed in the area of securities and exchange commissions because companies are able to investigate and suggest investment patterns to their potential clients. Analyzing the massive amounts of data and machine learning capabilities they are able to predict future market trends and investment growths for their clients and investors. They are able to build better relations with the investors and industry as well.

**Security issues with the open data:**

Alongside the very benefits of the making data available to the public there are growing security concerns as well. The initiative has placed a burden of ensuring the confidentiality, integrity, availability, and non-repudiation of the data. As the targeted attacks on large-scale organizations are not only growing in numbers but in complexity too it is inevitable to protect the data against criminal actors (Kounadi, Resch, & Petutschnig, 2018). Third parties having access to the open data can create ethical dilemmas by forging the data trends and misinterpreting the results if the analysis. It is difficult to ensure the confidentiality of the data. Once, data is obtained it can be transmitted or copied over insecure channels making it a potential target for malicious actors.

Data centers must have enough protective measure to ensure the confidentiality of the data. Adding layers of the confidentiality can hinder the availability of the data. Data sets containing personally identifiable information can be misused easily for nefarious purposes by the criminals. It would not be possible for the obtaining party to validate the authenticity of the data because it may be forged in transit. Digital channels are highly unpredictable therefore, the issuing authority may show reluctance to take any responsibility of forging of the open data results.

**Best practices to protect the open data:**

Given the potential of the open data for business value creation, it can be the critical asset of the state. Sophisticated encryption algorithms must protect the confidentiality of the data so, that it can be obtained and accessed by the intended recipients only. The attackers and malicious actors will not be able to understand the trends and patterns of the data due to sophisticated encryption even if they are aware of the algorithm as well (Palm, Mann, & Metzger, 2018). It will be true until the key to encryption is kept secret with the authorities and participating agencies. To ensure the authenticity and non-repudiation of the open data, a public key infrastructure will be made available as well. Public key infrastructure will ensure the integrity of the data in transit and there will be no modifications in the data unless authorized. Certificate-based public and private key pairs will be used for the access and authorization to the open data. It will ensure non-repudiation of the data as well because the executives in the government office will be able to authorize the data use by the authorized parties such as designated business.

**Conclusion:**

Open data is a valuable initiative by the government. However, protecting the confidentiality, integrity, availability, and non-repudiation of this data is also inevitable. Several steps must be applied as layers of the security to accomplish the basic goals of the information assurance including the encryption of the data sets and the public key infrastructure. It will protect the data in transit as well.

References

Dove, E. (2018). Collection and Protection of Personal Health Data.

Kounadi, O., Resch, B., & Petutschnig, A. (2018). Privacy Threats and Protection Recommendations for the Use of Geosocial Network Data in Research. *Social Sciences*, *7*(10), 191.

Lynskey, O. (2018). *At the crossroads of data protection and competition law: time to take stock*. Oxford University Press.

Palm, A., Mann, Z. Á., & Metzger, A. (2018). Modeling Data Protection Vulnerabilities of Cloud Systems Using Risk Patterns. In *International Conference on System Analysis and Modeling* (pp. 1–19). Springer.