March-April 2020
ISSN: 0193-4120 Page No. 12006 - 12016

Information Security Policy in the Indonesia Corruption Eradication Commission to Establish Indonesia Free of Corruption

[1]Ridwan, [2]Safril Hidayat, [3]Samsul Rizal, [4]Haposan Simatupang

[1]Subang University, Indonesia
[2,4]Indonesia Defence University
[3]Doctoral Student of Public Administration, Brawijaya University, Malang, Indonesia

Article Info
Volume 83
Page Number: 12006 - 12016
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 17 April 2020*

Abstract:

In era of globalizing information, the existence of the internet has accompanied the life pattern of the sectoral people to the global community. The positive side makes it easy for the public, but there is a negative side that needs serious attention, namely information tapping. The Indonesia Corruption Eradication Commission as an institution to eradicate corruption must synergize its performance with all components of the nation, executive, legislative and judiciary including the private elements. The synergy of the Indonesia Corruption Eradication Commission with all components will facilitate Indonesia Corruption Eradication Commission in creating Indonesia free of corruption. However, there are several cases of information leakage owned by the Indonesia Corruption Eradication Commission in doing so the Indonesia Corruption Eradication Commission needs to build a reliable and unbreakable information security system. Information security systems must be reliable both from hardware aspects that are resistant to all terrain and weather, as well as software aspects that are unbreakable so that it is not easily hacked and infiltrated and that is not less important is the manware aspect where the Indonesia Corruption Eradication Commission must have human resources who have high integrity and sense of information security towards commitment to eradicate corruption in the effort to make Indonesia clean of corruption.

Keywords: *Information Security, Synergy, Tapping.*

I. INTRODUCTION

In the current era of globalizing information, the existence of the internet has accompanied the life pattern from sectoral to a global community that is connected in a global network of "e-world", especially e-Government and e-Commerce. Information and communication technology is the fastest growing technology in line with the development of science. Human activity in general is almost inseparable from information and communication technology. Even everything that touches the lives of many people continues to be arranged by using information technology for efficiency and effectiveness. In line with the development of communication technology,

information becomes a very important commodity. The race to obtain and provide information quickly, precisely, and accurately becomes very important for every organization.[1]

The high needs of the community for the informations availability, requires information transparency, in other words freedom and ease in obtaining information. Transparency is an important agenda in the implementation of good governance. Transparency forces openness in the administration of government to open up access as much information as possible for the public, so that there is no opacity and secrecy in the implementation of government policy. [2] However, not all informations can be opened to the public, according to Law number 14 of 2008 concerning Openness of Public Information, there are excluded informations or confidential informations, that cannot be accessed by the public. Such informations, if opened, can result in obstruction of the law enforcement process; interfere with the interests of protecting intellectual property rights and protection from unfair business competition; failure of capturing criminal actors *(OTT/Operasi Tangkap Tangan)*, endangering national defense and security such as information on strategy, intelligence, operations, tactical and technical matters relating to the implementation of defense and security systems; an investigation warrant; state coding system; intelligence system, and so on. Due to the importance of the existence of information, especially excluded information, it is necessary to secure it, so that the validity and values contained therein are not utilized by unauthorized parties.

Excluded information must be secured from unauthorized parties. So that the excluded information is protected and safe from parties who are not authorized to know it by making information security policy. With this policy, various methods can be used by the government to secure the excluded information such as using steganography or cryptology methods.[3] The steganography method is hiding a message or information in a way so that besides the sender and the recipient no one can know it. The cryptological method is to change the message to be meaningless and only the sender and the recipient can process it back into meaningful messages. Cryptology as a science is not only a theoretical concept, but can be applied in various applications of information and communication security technology.

Furthermore, the development of information systems is so rapid but also turned out and causing various problems of leakage, theft, and destruction of information, so that information to the destination is not timely, and not even received at all to the destination address. According to Stallings there are several possible types of attacks on information such as interception (unauthorized parties succeeded in accessing assets or information, an example of this attack is wiretapping); Modification (unauthorized parties not only succeed in accessing information but can change information), an example is changing the content of the website with messages and information that harm the owner); interruptions (system devices become damaged or not available; attacks are directed at the availability of the system); and fabrication (unauthorized parties insert fake objects or fake messages/news into the system such as entering fake messages/e-mails/videos on a network computers and various other types of attacks on excluded information security.[4] Thus, the government's information security policy for excluded information is very urgent to be applied at all levels of government. Excluded information security threats can be explained in Figure 1 below:

March-April 2020
ISSN: 0193-4120 Page No. 12006 - 12016

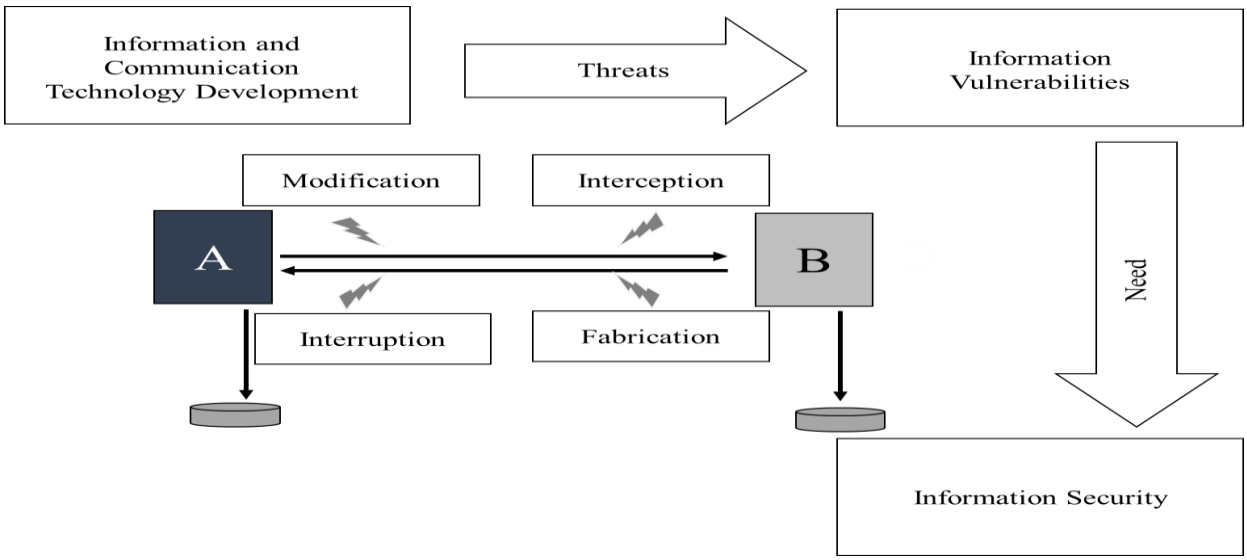

Figure 1 Information Vulnerability of Excluded Informations

From Figure 1 can be seen that the development of communication and information technology is vulnerable to raise threats (modification, interception, interruption, and fabrication). The information received probably is not complete, has undergone changes, and is not in accordance with the initial information sent. To overcome information vulnerability, information security technology is needed. It would be dangerous if an information technology infrastructure that is in contact with the lives of many people is not protected by an appropriate information security policy, such as population data networks and banking networks. If the data is damaged by irresponsible or unauthorized parties, the information contained in it becomes chaotic and damaged. It will harm the public who come in contact with the validation of the data.

Numbers in regular manner are just a series of writings, but the numbers as data or information is very sensitive, for example banking data. Disorder or damage to these figures can be detrimental to society, can damage economic and financial traffic, and can have an impact on the political life and security of a nation, as well as disorder in society. Information technology infrastructure is also vulnerable such as aviation, defense, oil and gas, electricity, etc., because those facilities can be used as a means of terror by terrorist groups. It is possible that terrorists will make information technology networks as a means to create chaos and terror in the community.

Nowadays. information security policy is a must to establish, because information technology networks that are public and global are inherently insecure. When data is sent from a public network, it will provide an opportunity for other parties to tap or change the data. In the traffic of the data, it allows others to participate in "listening". Terrorist attacks on information security policies can be carried out using one or more information technology networks as a means of terror. Broad invasion of an attack that is set automatically can also threaten the information network infrastructure. This attack can cause a large part of the information network not to be functioned properly. In the early 1990s the infiltration was still carried out openly. Most intrusions often exploit security weaknesses of the system that are quite simple, for example passwords with a combination of characters that are less secure. Once an intruder can exploit a weakness to get access that is already known but not fixed, then he will be able to use the system as he/she wishes.

Some examples of leakage, wiretapping, theft and tampering government informations sites such as Election Commission's website, Ministry of Defense, Ministry of Foreign Affairs, Cases of

wiretapping of the Indonesian President's conversation by Australia, intercepting talks between President BJ Habibie and the Attorney General (Andy Ghalib) in 1998. Oenetration by the KGB (Russian intelligence) into the USA representative office through electronic emissions to the United States Communication Program Unit. Between April 1990 to May 1991, five Dutch hackers were able to penetrate the American communication system on 34 military sites. The hackers managed to obtain information about the location of American troops, weapons, missile capabilities and movement of American warships in the Arabian Gulf, and other cases of wiretapping (Stalling, 2007:19). [5]

No matter how perfect the information security policy is made to design a strong security system, it can be understood that no information and communication system can be secure totally. What can be done is to make it difficult for others to disrupt the existing system. For example, avoiding the risk of intrusion, reducing the risk of threats, protecting the system from vulnerabilities, and so on. That, the safer the system is built, the more uncomfortable it is, and conversely, the more comfortable the system is built, the more insecure it is.

The Indonesia Corruption Eradication Commission was formed based on Law Number 30 in 2002 concerning the Corruption Eradication Commission that was given the mandate to eradicate corruption in a professional, intensive, and sustainable manner. According to Law Number 19/2019 which is the second amendment to Law Number 30/2002 concerning the Corruption Eradication Commission explains that the Indonesia Corruption Eradication Commission is an independent governmental institution, which in carrying out its duties and authorities is free from any authority. In carrying out its duties and functions in eradicating corruption, the Indonesia Corruption Eradication Commission has also experienced in reducing leakage and fabrication of information. The Chief Secretary of the Indonesia Corruption Eradication Commission in the era of Abraham Samad was declared by the Indonesia Corruption Eradication Commission Ethics Committee as the person who leaked documents (warrants of investigation) that were supposed to be secret for public consumption. The leak of classified information eventually led to speculations on the reputation of the Indonesia Corruption Eradication Commission as an organization accused of acting under the pressure of power to launch political agendas for the authorities. Another case is the former Mayor of Bandung, Dada Rosada, who came to the Indonesia Corruption Eradication Commission office to fulfill the Indonesia Corruption Eradication Commission summons based on an official letter received. However, the Indonesia Corruption Eradication Commission has never made a letter as demonstrated by Dada Rosada [6].

This information security issue is interesting to discuss because it is the main key in supporting the successful implementation of corruption eradication. Information leaks that occur have the potential to interfere with the eradication of corruption process in Indonesia. It needs specific solutions in overcoming the problems mentioned above. But of course, it is understood that solving the problem is not as easy. Major and fundamental changes must be made, along with the government's commitment to make Indonesia clean of corruption. So how far is the KPK's effort to strengthen information security policy to support efforts to eradicate corruption in Indonesia?

II. CONCEPTUAL FRAMEWORK

A large number and more and more studies in comparative, public policy politics and international relations have paid attention to how the policy spread between states, states or federal cities, that is, how policies are one unit is affected by other unit policies [7]. Policy implementation is a dynamics activity which are political decisions, in the form of regulations and programs involving not only “street level bureaucracy” to the top leadership

apparatus, but also community. Activities create opportunities for the community to involve themselves in accessing and achieving the interests of policy makers. The implementation of the policy according to Grindle (1980) is not merely related to the mechanism of translating political decisions into routine procedures through the bureaucracy, more than that it involves the problem of conflict, decisions and who gets what from a policy.[8] But consistency in a policy must be clear and measurable from planning to the policy being implemented, as stated by Presmann and Wildavsky (1979:21), that policy implementation is a process of interaction between established goals and actions taken to realize the goals referred to. [9]

Presmann and Wildavsky (1979) see policy implementation as a link connected starting point "setting of goals" to end point "achievement them". On the other hand, humans as individuals or groups determines of the success of a policy must have strong ethics and commitment in implementing policies as expressed by Winarno (2012:102), the implementation of policies as actions carried out by individuals or groups in government and the private sector that is directed to achieve the goals set in decisions. [10] The complexity in the implementation of public policy is because it involves various forms of activities, various actors or parties, related to the environment, and context in which the policy will be applied to achieve the objectives.[11] Thus, the success of public policy is not only based on economic, efficiency and administrative principles, but ethical and moral consequences are at stake in reflecting apparatus behavior in relation to the interests of the people, mainly information security.

Every policy carries a risk of failure. There are two categories of policy failure, namely non-implementation or program failures and unsuccessful implementation because they do not produce the desired benefits. Non-implementation policy occurs the parties involved in the implementation do not want to cooperate or have worked together inefficiently, work half-heartedly, or they do not fully understanding the problem, or the problem is solved beyond the scope of their power.[12] Unsuccessful implementations usually occur when a policy has been implemented in accordance with the plan but given the external conditions turned out to be unprofitable, the policy was not successful in realizing the desired impact or outcome.

Edward III (1980) asked 2 main questions, what are the prerequisites for a successful implementation? What are the main obstacles to the successful implementation of the program? Based on these two questions, four factors or variables are formulated as the most important conditions for the successful implementation, which are communication, resources, disposition or tendency of the executor and organizational structure, and the work flow of the implementing bureaucracy.[13] Of the four factors, communication is placed at the top position for implementing policy effectively. Communication relates to the interrelation and interaction between policy makers (decision makers) with implementors, as well as communication among policy implementors and target group.

Resources are authority. Authority is the power to make decisions in guiding other individuals. Thus, authority is intended to produce compliance for both the actors implementing the policy, as well as the people or organizations as the object of policy. Edwards III said that the disposition / attitude of executors provides guidings among implementors, if the implementation is carried out effectively. Implementors must not only know what they should do, but they must have the ability to implement policies. Implementor has a large role and determines the success of a policy in its implementation. Regarding this Edward III stated, "If implementators are well disposed to the administration of particular policy policies, they are more likely to carry out as the original decision makers intended. But when implementators' attitudes or perspectives differ from the decision

March-April 2020
ISSN: 0193-4120 Page No. 12006 - 12016

makers, the process of implementing a policy becomes infinitely more complicated."

The description shows the need for a common perception or attitude between decision makers orchestrated with implementors. Implementors in general have the possibility of deviating attitudes and perspectives on policy, and this can be a major obstacle to the policy implementation effectiveness. The information itself is data that has been processed so that it has a meaningful and beneficial form for the recipient so that it can be used in decision making. [14] It means, information is data that has been processed. Data processing is done in such a way that the data that has been processed can increase the knowledge of people who receive and use it. Before reform we rarely heard the term public information. Society is difficult to know the performance of the government, participate in government systems and make public information expensive items as if not allowed to know. Information is controlled by the authorities, especially information relating to public policy and the state budget. This causes the role of the community in development to be very weak due to limited information. After the reform, freedom in expressing aspirations and knowing information seems to be something that must be known by the public. The guarantee of the right to information brings a fresh breath of new life for democracy in Indonesia, where the second amendment to the second const itution of 2000 added a guarantee of the right for every citizen to obtain information.[15] Public information is information generated, stored, managed, sent and / or received by a public body that relating to the organizer and state administration and / or organizer and organization other appropriate public bodies with the Commission Law Public Information and other information related to interests public [16].

The communication that is built must follow the information exchange process. According Soemarkidjo (2006) that the process of exchanging information as complex as any has the following context: Information - sender - communication media - recipient. Schematically the information exchange process is described as follows:

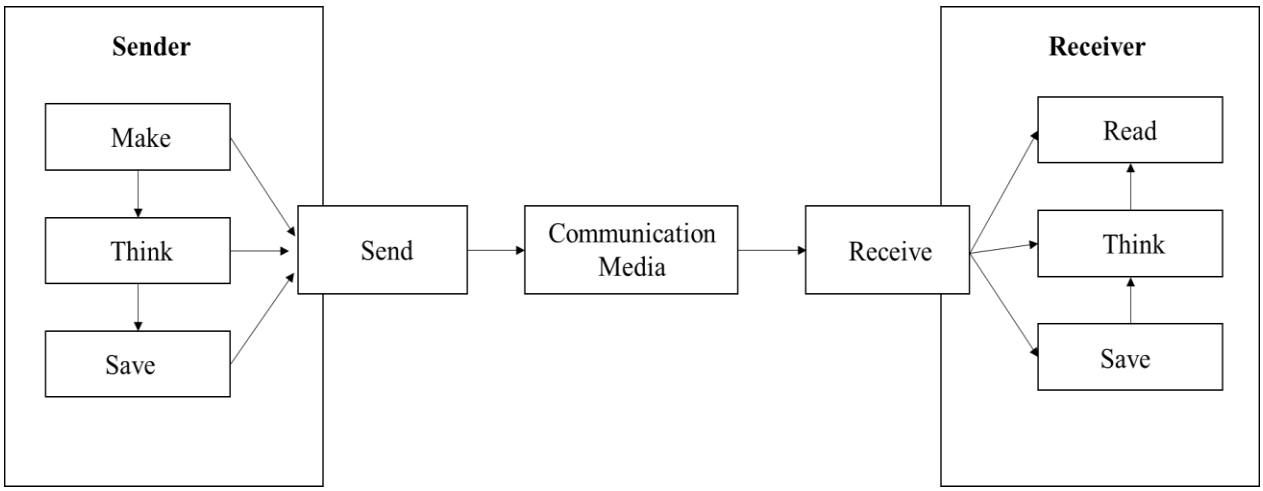

Figure 2. Information Exchange Process
Sources: Soemarkidjo (2006:319)

Figure 2 above explains that the information created and processed by the sender then stores and sends it through the communication media. Recipients get information to process and store it then read to get data from the information obtained. In general, the purpose of information security is to

March-April 2020
ISSN: 0193-4120 Page No. 12006 - 12016

guarantee availability, that is, information is always available when needed and is easy to obtain, integrity means ensuring that data is not altered by unauthorized parties or by other things unknown instances of poor transmission data, confidentiality, maintaining the confidentiality of information from all parties, except those with authority. Information security is of great importance and interest to everybody in the world of technology today, whether you are a mobile phone or a personal computer user, this is why information security is of the most importance in our everyday life, and in the IT fields [17]

Based on the description above, the threat of information leakage caused by individual negligence or wiretapping can occur to Indonesia Corruption Eradication Commission and causing public antipathy to the performance of the Indonesia Corruption Eradication Commission to eradicate corruption. Policies on information security can be established by synergizing policy makers and implementors. Referring to the simple model in the policy implementation by Van Meter and Van Horn (1975), implementation process is an abstraction or performance of a policy manifestation which is intentionally carried out to achieve high performance policy implementation with various variables.[18] This model presupposes that policy implementation runs linearly from policy that can influence political decisions, implementor, and performance. One variable is communication, therefor goals should be understood by each implementor. Communication means delivering information to policy implementors that standards and objectives consistency and uniformity from various sources of information. Communication requires the ability of human resources to interact properly, there is no deviation between policy maker and implementor in executing the policy to achieve the expected performance to secure Indonesia Corruption Eradication Commission information system. Thus, quality of Human Resources becomes the main factor to maintain the Indonesia Corruption Eradication Commission in combating corruption by maintaining confidential information. The conceptual framework is as follows:

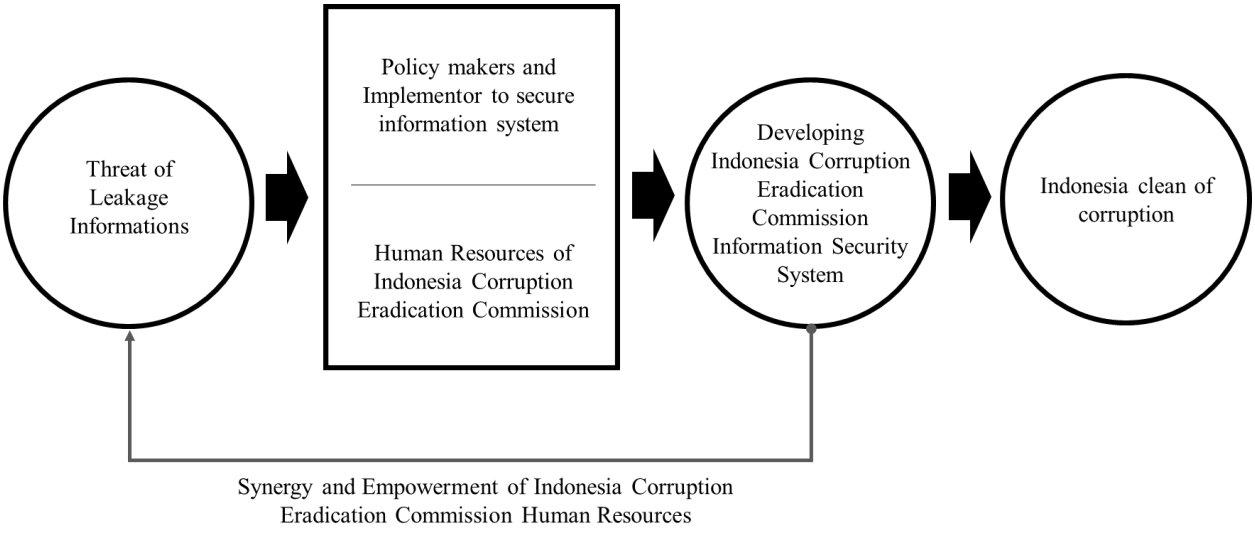

Figure 3 Conceptual Framework

III. METHOD

The research was conducted by a qualitative research design using literature review. This paper

basically wants to provide an overview of the ability to secure and manage information coupled with the ability to build human resources with integrity in supporting the realization of information security policy. To obtain data and information related to this paper, data collection is done through literature and document studies. Validity and reliability of the data was executed by using triangulation technique.

IV. RESULT AND DISCUSSION

4.1 Communication synergy between Policy Makers and Implementor

Information security is related to three requirements: confidentiality, integrity, and availability. The policy compiled by Indonesia Corruption Eradication Commission in ensuring the confidentiality, integrity and availability are often tarnished by individuals who publish information unilaterally on behalf of the Indonesia Corruption Eradication Commission. As the consequences, Indonesia Corruption Eradication Commission poor performance is breaking by certain individual without legal authority to disseminate classified information. It means that there is a communication gap between policy makers in formulating information security policy and implementors. However, The Indonesia Corruption Eradication Commission has modern and sophisticated hardware and software to be able to hack people suspected of committing corruption. However, the actions of a handful of people who lack integrity often tarnish the achievements that have been inscribed by the Indonesia Corruption Eradication Commission in combating corruption in Indonesia.

In order to synergize communication between policy makers and relevant stakeholders, optimizing performance of human resources or man ware is a must. Synergy is a process in which the interaction of two or more agents or forces will produce a combined effect that is greater than single organization.[19] Considering that communication becomes very important in policy implementation, because although the policies produced are of good quality and aim to fulfill the interests of the community, if the implementors do not have a clear, complete, and broad understanding of the meaning and purpose of the policy, then implementors will convey it vaguely, narrowly and in a limited way. As a result, it is possible that a priori attitudes occur, and even there is a refusal of policies from the target group. In other words, a desire arises to leak, distort, or change the information provided to the public, and causing confusion.

Efforts to implement the eradication process of anti corruption starts from prevention to enforcement requires synergy of cross-sectoral communication within all components of the nation, both executives in central government to regional or local governments, legislatures, judiciary, and private sector. According to Corning (1995) synergy is part of self-awareness to be able to work together with others.[20] In essence, existing organization contains humans as social creatures who cannot live alone *(zoon politicon)*. To be able to survive, humans must interact and relate to other people in different organizations or places. Likewise, in the context to make Indonesia that is free from corruption, the synergy of all state stakeholders is an absolute requirement to develop communication synergy so that the policy in line with leadership to secure information in the Indonesia Corruption Eradication Commission.

Synergy relationship by Indonesia Corruption Eradication Commission with external stakeholders are very important in order to prevent corruption. While the internal synergy of the Indonesia Corruption Eradication Commission harmonizes policy makers and implementors so as to minimize the occurrence of irregularities on the grass root. As an institution, that is expected by the community for Indonesia Corruption Eradication Commission independence and integrity to eradicate corruption. Indonesia Corruption Eradication Commission needs synergy with all components of the nation so

that the implementation, function and tasks can run optimally in order to create an Indonesia that is free of corruption.

The Indonesia Corruption Eradication Commission synergy is able to double eradicating corruption, this is in line with Deardorff and Williams that synergy is a multiplier effect that allows exponential multiplication through joint efforts (Deardorff and Williams, 2006). Synergy between components of the nation requires the participation of relevant stakeholders so that goodwill and political will are needed synchronously between the Indonesia Corruption Eradication Commission, the Ministry of Communication and Information, and the National Police so that unauthorized cannot disseminate classified informations to public. This synergy is carried out with positive instincts, empowering, and using by Indonesia Corruption Eradication Commission members as unified state organization. Synergy of all stakeholders can achieve: Firstly, Socialization of anti-corruption as well as information security can be well maintained; Secondly, facilitate the prevention of corruption by Indonesia Corruption Eradication Commission with the accuracy of the news and accuracy arrested of suspects who is alleged committing corruption; Thirdly, the realization of synergy in information security can be established; and Fourth, execution of anti corruption eradication will raise significant result in combating corruption.

Developing information security through synergic communication can reduce failures or non-implementation policy and unsuccessful implementation in the Indonesia Corruption Eradication Commission. All implementors work together efficiently and master problems according to their respective tasks and functions. Even unsuccessful implementation can be avoided because of the solidity of internal communication with an information security system, that is guaranteed with legal aspects and independent process.

4.2 Developing Information Security System of the Indonesia Corruption Eradication Commission

In general, the purpose of information security is to guarantee availability, that is, information is always available when needed and is easy to obtain. Integrity ensures that data is not altered by the unauthorized apparatus. Disruption to integrity causes the information received by the recipient to be incompatible with the information that should be. The warrant letter leak case and the fake invitation letter of Indonesia Corruption Eradication Commission in the past, are a form of attack on the integrity of information. Although the Indonesia Corruption Eradication Commission has clarified that it did not send any information, but the information was created by an irresponsible party on behalf of the Indonesia Corruption Eradication Commission. Thus, confidentiality is only to those who have the authority.

Developing information security system is not an instant process but it is a process that is carried out continuously. To protect the exempt information belonging to the Indonesia Corruption Eradication Commission of wiretapping, theft, fabrication need reliable information security system in terms of hardware, software and manware. Equipment (hardware) that is reliable, strong in various fields and weather already owned by the Indonesia Corruption Eradication Commission. Secure software is protected with unbreakable encryption, not easily hacked. Thus the logical consequence is updating by sophisticated and layered information security system. Last but not least, human resources with a high integrity and capacity is always needed to prevent corruption.

The Indonesia Corruption Eradication Commission needs to adjust with global information security standards and enforce consistently with high political will of the ISO 27001 [21], through a Plan-Do-Check-Act (PDCA) cycle, accordingly improvements are made continuously. The internal information security policy makers require good

communication in developing security policies; organization for information security functions; asset management; security of human resources; physical and environmental safety; communication and operational management; access control; information system acquisition, development and maintenance; information security incident management; business process management; and compliance. At least the political will and goodwill by policy makers towards implementor must be strong on four aspects: human resources, access control, management of information security incidents, and integrity of human resources to avoid information leakage.

Indeed, the development and implementation of information security system can be done gradually, but the determination of the scope and phasing must be determined based on a clear risk analysis. Risk analysis is preceded by an inventory of assets related to information managed by the organization so that it can be known which parts are vulnerable to information leakage. The Indonesia Corruption Eradication Commission information security policy formulation needs to measure the level of risk exposure for the possibility of information leakage based on previous experience. Policy makers in information security can then give authority to the implementor to just accept the situation, control the situation (mitigate), reject, or transfer to other parties or stakeholders while maintaining authority of each institution. It must be clear which part has the authority so it does not become an “overlapping territory".

The last and very decisive point is humans as executors should have high integrity. As strong and sophisticated hardware and software but if manned by people who do not have integrity, the information will be leaked by humans, vice versa. The Indonesia Corruption Eradication Commission is the foundation of citizen in combatting corruption. The Indonesia Corruption Eradication Commission ensures information security in its organization. Comprehensive and holistic improvements must be made by policy makers who are "guaranteed" by the information security policy implementor in all parts of the organization within individual entities and sub-organizations of the Indonesia Corruption Eradication Commission.

V. CONCLUSION

Policy implementation is a dynamic activities which are the implementation of political decisions, in the form of law, programs, and activities involving not only the implementor up to the level of street level bureaucracy, but also involving the community. Community involve themselves in accessing their interests and achieving the interests of policy makers. Indonesia will be free from corruption if the synergy of all components of the state stakeholders by building synergistic communication. Relationships in the form of external synergies by the Indonesia Corruption Eradication Commission are very important in order not to prevent corruption. Meanwhile, the internal synergy of the Indonesia Corruption Eradication Commission harmonizes policy makers with implementors so as to minimize the occurrence of irregularities and leakage informations.

The purpose of information security is to guarantee availability, information is always available when it is needed and easy to obtain it. Integrity ensures data does not change by unauthorized person or poor data transmission. Confidentiality means maintaining the confidentiality of information from all parties, except those who have the authority. To build a reliable and unbreakable information security system, the Indonesia Corruption Eradication Commission must have hardware, software, and manware that are reliable.

REFERENCES

[1] Ridwan. (2016). *Information Security Policy Implementation in Central Sulawesi Provincial Government*¸ Bandung: Padjadjaran University.

[2] Michael Lenon dan Gary Berg-Cross. (2010). *Toward a High Performing Open Government.* The Public Manager 39, No. 10 (Winter 2010).
[3] Soemarkidjo. (2006). *Jelajah Kriptologi.* Jakarta: Lembaga Sandi Negara.
[4] William Stallings. (2007). *Data Computer and Communications. Eighth Edition.* Upper Saddle River, New Jersey: Pearson Prentice Hall.
[5] *Ibid.* Stalling, 2007. p.19
[6] *Pembuat Surat Palsu KPK untuk Dada Rosada Terancam 6 Tahun Penjara.* Source: https://news.detik.com/berita/d-2212375/pembuat-surat-palsu-kpk-untuk-dada-rosada-terancam-6-tahun-penjara, Accessed 04/02/2020.
[7] Maggetti, Martino and Gilardi, Fabrizio. (2016). *Problems (and solutions) in the measurement of policy diffusion mechanisms.* Journal of Public Policy / Volume 36 / Issue 01 / March 2016, pp.87 - 107
[8] Grindle, Merilee S. (1980). *Politics and Policy Implementation in the Third World.* Princeton, New Jersey: Princeton University Press.
[9] Presmann, J and Wildavsky. (1979). *Implementation.* Berkeley: University of California Press.
[10] Winarno, Budi. (2002). *Teori dan Proses Kebijakan Publik.* Yogyakarta: Media Pressinda.
[11] Rusli, Budiman. (2013). *Kebijakan Publik: Membangun Kebijakan Publik yang Responsif.* Bandung: Publishing
[12] Brian W, Hogwood, and Lewis A. Gun. (1984). *Policy Analysis for The Real Word.* London: Oxford University Press.
[13] Edward III, G.C. 1980. *Implementing Public Policy.* Washington D.C: Congressional Quarterly Press.
[14] Davis, William, S. (1981). *Sistem Pengolahan Informasi.* New York: Wesley Publishing.
[15] Tyasmara, Nuritan C. (2016). *Kebijakan Informasi dan Pelaksanaan Undang-Undang No. 14 Tahun 2008 Keterbukaan Informasi Publik.* Journal of Information Policy. pp. 2
[16] Zulaikha. (2017). *Implementasi Kebijakan Keterbukaan Informasi di Jawa Timur Tahun 2016.* Jurnal Studi Komunikasi. Vol 1 pp. 133
[17] Alhasan, Mahfouz M & Quaye Alexander. (2017). *Information Security in An Organization.* International Journal of Computer Vol. 24 No. 1 pp. 100-116
[18] Van Meter, Donal and Carl E. Van Horn. (1975). *The Policy Implementation Process Conceptual Frame Work.* Journal Administration & Society, 6(4), pp. 445-488.
[19] D.S. Deardorff & G. Williams. (2006). *Synergy Leadership in Quantum Organizations.* Lake Lure, NC: Fesserdorff Consultants.
[20] Corning, Peter A.(1996). *Synergy, Cybernetics and the Evolution of Politics.* International Political Science Review Vol. 17, No. 1 (Jan., 1996), pp. 91-119
[21] *ISO/IEC 27001 Information security management.* Source: https://www.iso.org/isoiec-27001-information-security.html, accessed 04/02/2020.