Implementation Of Electronic-Based Government System In Jakarta: The Case Of Cyber Attacks

[1]R. Fauzy, [2]Bahrullah Akbar, [3]Dadang Suwanda, [4]Sutiyo, [5]Mansyur Achmad, [6]Ika Sartika, [7]Juri Ardiantoro, [8]Andi Fitri Rahmadany

dip.11.687@ipdn.ac.id, bahrullah.akbar@ipdn.ac.id, kangdadang207@yahoo.co.id, sutiyo@ipdn.ac.id, mansyurachmad@ipdn.ac.id, ika_sartika@ipdn.ac.id, ardiantoro.juri@unusia.ac.id, afitri.rahmadany@ipdn.ac.id
[1,2,3,4,5,6,8]Sekolah Pascasarjana IPDN, [7]Univeristas Nahdlatul Ulama Indonesia
Email Correspondence: dip.11.687@ipdn.ac.id

Article Info

Received: 2024-10-22
Revised: 2024-12-23
Accepted: 2024-12-31

Keywords:
Policy Implementation, Cyber Attacks, DKI Jakarta Provincial Government

Abstract

Information security in the Electronic-Based Government System (SPBE) of the DKI Jakarta Provincial Government is not yet optimal. The study found that 682 applications are vulnerable to cyber attacks, including the JAKI application in 2023. The causal factors include inadequate security budgets, insufficient personnel with BSSN certification (only 14 out of 31), and infrastructure that does not meet the ISO 27001: 2022 standards. Additionally, Information Security Standard Operating Procedures (SOPs) are not yet available in every Regional Apparatus Organization (OPD), and support from the Regional Council (DPRD) is still minimal. This study aims to analyze the deficiencies in SPBE information security in DKI Jakarta and provide recommendations for improvement. The theoretical foundations used are Government Science, Information Security, and Public Policy Implementation. The research method employs a qualitative approach, using secondary data analysis from official reports and literature reviews on public policy implementation and information security standards. The study concludes that increased budgets, personnel training and certification, as well as infrastructure and SOP improvements are urgently needed. As a global city, Jakarta must improve its information security to protect its data and reputation, thereby enhancing the overall information security index. The recommendations include increasing the information security budget to 6-10% of the total SPBE budget, providing training and certification for all relevant personnel, updating the infrastructure to meet the ISO 27001:2022 standard, and developing and implementing Information Security SOPs in each OPD . Strong policy support from the DPRD is also crucial to strengthen these efforts and support Jakarta's position as a Global City.

I. Introduction

In the last decade, the phenomenon of electronic government (e-government) transformation has become an important part of global world development. E-government is a new paradigm in government that is driven by the use of Information and Communication Technology (ICT) to improve the quality of public services. The transformation of e-government in Indonesia has become an important milestone in the development of government administration since the early 2000s, with the publication of Presidential Instruction No. 6 of 2001 concerning the need to improve government efficiency and effectiveness and Presidential Decree no. 95 of 2018 concerning Electronic-Based Government Systems (SPBE) (Suwardana, Achmad &Sutiyo, 2023).

The SPBE Presidential Decree was designed as a legal basis for implementing a system that utilizes information and communication technology in the government administration process. The implementation of this Presidential Decree has a significant impact on various aspects of government administration, such as data management, provision of public services, and government-society interactions. This changes the government paradigm to a more open, integrated and technology-based system (Indrawati et al., 2022).

Implementation of the SPBE Presidential Decree faces challenges, such as data security, technology accessibility, and changes in organizational culture. The Special Capital Region (DKI) Province of Jakarta responded by issuing DKI Jakarta Governor Regulation (Pergub) No. 68 of 2022 concerning Implementation of SPBE (Pergub SPBE DKI Jakarta) which actualizes the implementation of SPBE in 42 Regional Government Organizations (OPD).

The DKI Jakarta SPBE Gubernatorial Regulation is the legal basis for the implementation of e-government in the local government environment, with the aim of realizing clean, effective, transparent and accountable government governance as well as quality public services (Lukman and Suwanda, 2021). The policies and strategies regulated in this Gubernatorial Regulation include increasing government transparency and accountability, efficiency, quality of public services and community participation. In order to realize this, the Gubernatorial Regulation emphasizes the development and use of ICT, increasing the capacity of Human Resources (HR), budget support, and inter-agency cooperation in implementing SPBE.

The implementation of the DKI Jakarta SPBE Gubernatorial Regulation is a strategic step towards modern and efficient government in the DKI Jakarta region. This Gubernatorial Regulation provides a strong foundation for the transformation of electronic-based government systems in the DKI Jakarta region in accordance with the goals and principles mandated in Presidential Decree No. 95 of 2018. Based on the Decree of the Minister for Administrative Reform and Bureaucratic Reform (PANRB) No. 108 of 2023 concerning the results of SPBE monitoring and evaluation in central and government agencies. In 2022, the DKI Jakarta Provincial Government received the highest SPBE index with a score of 3.67 with a Very Good predicate as seen in table 1 below:

Table1.SPBE Ranking Scoring in 2022

No	Provincial Level SPBE Evaluation Results	SPBE Index	Predicate
1	DKI Jakarta Provincial Government	3.67	Very good
2	West Kalimantan Provincial Government	3.42	Good
3	West Java Provincial Government	3.37	Good
4	Lampung Provincial Government	3.37	Good
5	NTT Provincial Government	3.35	Good

Source:DKI Jakarta Provincial Government SPBE Tauval Year 2023

DKI Jakarta Province has 47 SPBE monitoring and evaluation value indicators in 2022 which are grouped into four domains, namely SPBE Policy Domain, SPBE Governance Domain, SPBE Management Domain, and SPBE Service Domain. In the SPBE Policy Domain, the Internal Information Security Management (IMKI) Policy indicator in DKI Jakarta Province is still not optimal, with a score of 3 out of target 5. This shows that the internal information security management policy in DKI Jakarta Province is still at the basic stage, where the organization already has information security policies and procedures, but they have not been effectively implemented and monitored.

In the 2023 SPBE evaluation ratified by the Ministry of PANRB, the DKI Jakarta Provincial Government received a score of 4.21, occupying second place, with a satisfactory predicate. The DKI Jakarta Provincial Government's SPBE index managed to increase by 0.54 points compared to 2022. Meanwhile, the highest points were achieved by the Central Java Provincial Government with 4.26 points, followed by the West Java Provincial Government with 4.14 points, the Bali Provincial Government with 4.07 points. , and the East Nusa Tenggara Provincial Government 3.83 points. Details of the 2023 SPBE evaluation results can be seen in table 2 below:

Table 2. SPBE Ranking Scoring in 2023

No	Provincial Level SPBE Evaluation Results	SPBE Index	Predicate
1.	Central Java Provincial Government	4.26	Satisfying
2.	DI Yogyakarta Provincial Government	4.22	Satisfying
3.	DKI Jakarta Provincial Government	4.21	Satisfying
4.	West Java Provincial Government	4.14	Very good
5.	Bali Provincial Government	4.07	Very good

Source: DKI Jakarta Provincial Government SPBE Tauval 2023

In 2023, the SPBE evaluation will involve 30 universities as external assessors. The evaluation process includes independent assessment by agencies, document assessment, interviews, direct visits, and preparation of reports. The SPBE evaluation implementation guidelines refer to PANRB Ministerial Regulation No. 59 of 2020 concerning Monitoring and Evaluation of SPBE and PANRB Ministerial Guidelines No. 6 of 2023 concerning Procedures for Monitoring and Evaluation of SPBE. The assessment was carried out on 47 indicators including the SPBE Policy Domain, Governance Domain, Management Domain and SPBE Service Domain. The DKI

Jakarta Provincial Government is in third place.

In the SPBE Policy Domain, the IMKI Policy indicator in DKI Jakarta Province has reached the maximum score of 5. However, in the SPBE Management Domain, the SPBE Risk Management Implementation Maturity Level indicator in DKI Jakarta Province is still not optimal, with a score of 2 from the maximum target of 5. This shows that the organization has policies and procedures related to SPBE risk management, but they have not been implemented effectively. Organizations need to have strong information security policies and procedures to protect data and information systems. (Akbar, 2013). In table 3 below, efforts to increase SPBE implementation in the DKI Jakarta Provincial Government are illustrated by the increased budget allocation, from IDR 74,626,099,197 in 2022 to IDR 337,724,774,087 in 2023.

Table 3. SPBE Implementation Budget at Diskominfotik DKI Jakarta Province

Informatics Application Program	2022	2023
Domain Name/Subdomain Management	IDR 271,864,796,288	IDR 175,719,437,716
Management e-Government/ Jakarta Smart City	IDR 274,626,099,197	IDR 337,724,774,087

Source: Jakarta.go.id 2022-2023

The Cyber and Crypto Division of the Communications, Informatics and Statistics Service (Diskominfotik) has allocated a special budget for cyber and password security activities. The budget has increased from IDR 12,162,776,900 in 2022 to IDR 14,843,503,664 in 2023, this shows the DKI Jakarta Provincial Government's commitment to strengthening information security, as seen in table 4:

Table 4. Cyber and Crypto Agency Budget for DKI Jakarta Province

Year	No	Details	Amount
2022	1.	Needs Analysis and Management of Information Security Resources	IDR 9,009,721,362
	2.	Provision of Information Security Services	IDR 3,153,055,538
		Total	IDR 12,162,776,900
2023	1.	Information Security Governance Policy and Cipher Communication Networks	IDR 290,659,000
	2.	Needs Analysis and Management of Information Security Resources	IDR 11,318,672,524
	3.	Implementation of Network Security Software Procurement Work	IDR 3,234,172,140
		Total	IDR 14,843,503,664

Source: Jakarta.go.id 2022-2023

This budget is still insufficient if we use the 2020 Deloitte and the Financial Services Information Sharing and Analysis Center (DFSISAC) standards. Apart from that, human resources and cyber security infrastructure in the DKI Jakarta Provincial

Government are still not optimal.

The results of monitoring in 2022 show a lack of coordination between OPDs, where the focus of information security is still focused on the Cyber and Crypto Information Technology Sector. It is necessary to increase commitment, competence and capacity in each OPD to maintain information system security.

Economically, DKI Jakarta's economic growth in the second quarter of 2023 will increase, but the budget for ICT is still relatively small. The digital literacy level of the people of DKI Jakarta is also still ranked 8th nationally. Politically, the support of the DKI Jakarta Regional People's Representative Council (DPRD) for the implementation of information system security policies is also not optimal (Achmad, 2021).

The performance achievement of SPBE implementation in the DKI Jakarta Provincial Government is the highest nationally, but there are still challenges related to security standards that are not yet optimal. This causes cyber attacks to continue to occur within the DKI Jakarta Provincial Government. The details of these cyber attacks are explained in table 5, namely:

Table 5. Impact of Cyber Attacks

No	Type	Location	Year	Impact
1.	Ransomware	Mayor of North Jakarta	2022	Ransomware or data leak incidents can indicate low levels of cybersecurity, potentially damaging an agency's reputation and public trust
2.	Web Defacement	Pesanggrahan Regional Hospital	2022	Threatening the security of patient data and health information, it also has a serious impact on the reputation of health services
3.	Web Defacement	Sawah Besar District Hospital	2022	
4.	Web Defacement	Tanah Abang Regional Hospital	2022	
5.	Malware	ControllerWifi DHCP-37_49	2022	Malware on wifi controller and DHCP breaks functionality network, affecting device connectivity and IP address distribution. By infecting the WiFi controller, malware can spread to other devices on the network, causing service disruptions and disconnections
6.	Web Defacement	DKI Jakarta Personnel Management	2022	Threatening the security of data and information on personnel data for 54 thousand ASN in the DKI Jakarta Provincial

				Government
7.	Web Defacement	Mayor of Central Jakarta	2022	Reputation on Public Information will have a negative impact
8.	Malware	Data Communication Network Services	2022	Malware hampers network performance, causing connection disruptions between devices and public services in the DKI Jakarta Provincial Government
9.	Web Defacement	DKI Jakarta Archives	2022	Loss of Information Archives at the DKI Jakarta Provincial Government
10.	Web Defacement	Taman Sari Regional Hospital	2022	Threatening the security of patient data and health information, it also has a serious impact on the reputation of health services
11.	Web Defacement	Tourism and Creative Economy	2022	
12.	Web Defacement	Menteng Health Center, Central Jakarta	2022	
13.	Web Defacement	DKI Health Service Documentation Services	2023	Reputation on Public Information will have a negative impact
14	Web Defacement	DKI ASN Elearning	2023	The reputation of learning information for 52 thousand ASN DKI Jakarta is disrupted
15	Web Defacement	DKI Jakarta ASN Performance System	2023	Threatening the security of data and information on personnel data for 52 thousand ASN in DKI Jakarta
16	Web Defacement	Jatipadang Regional Hospital	2023	Threatening the security of data and information, it also has a serious impact on the reputation of public services
17	Web Defacement	Kalideres Regional Hospital	2023	
18.	Web Defacement	Matraman Regional Hospital	2023	
19.	Web Defacement	Menteng Health Center	2023	
20	Defacement	JAKI application	2023	

Source: CSIRT DKI Jakarta Provincial Government @2023

The analysis shows common patterns of cyber attacks that include web defacement, malware and ransomware, all of which have the potential to seriously impact data security, reputation and services. Strengthening cybersecurity, data recovery and transparency in dealing with incidents are important to reduce the impact and rebuild public trust. The increasing presence of cyber attacks indicates weaknesses in digital security standards. This requires the DKI Jakarta Provincial Government to strengthen its digital security system to protect government infrastructure and data. The DKI Jakarta Provincial Government has many critical service applications, such as e-KTP, e-Pajak, e-Health, SIMPEG, and SIMKEU, which are vulnerable to cyber attacks. Overall, this analysis emphasizes the importance of strengthening cyber security and transparency to address increasing threats and ensure the continuity of safe and reliable public services.

This research aims to explain the implementation of SPBE in DKI Jakarta Province, as well as analyze the impact of cyber attacks on electronic-based government systems. In this regard, this research will detail aspects such as resource allocation, communication, commitment, skills and abilities in implementing SPBE, as well as exploring the impact of cyber attacks on electronic government services. The hope is that this research can encourage positive changes in governance and information security in the government environment, so that the DKI Jakarta Provincial Government can provide superior and trustworthy public services.

In analyzing policy implementation, there are various theories and models that can be used to understand the complexity of the process. One model that is often quoted and used as a basis is the model used by Van Meter and Van Horn. This model highlights six dimensions that dynamically interact in the policy implementation process. (Hill and Hupe, 2002) as expressed in the following quote "The six variables (surely are in fact clusters of variables) are" are six dimensions or variables which are explained as follows:

1. Standards and Policy Objectives
2. Resources and Incentives
3. Quality of Inter - Organizational Relations
4. Characteristics of Implementing Institutions
5. Economic, Social and Political Environment
6. Disposition or Response of the Executors

By understanding these six factors comprehensively, a deeper understanding of the dynamics and complexity of policy implementation can be developed. This is key in formulating effective strategies to achieve policy objectives and overcome challenges that arise in the implementation process.

2. Research Method

This study used descriptive qualitative method. The unit of analysis in this research is the parties or stakeholders related to the implementation of the SPBE policy, namely the DKI Jakarta Provincial Government as the policy maker and the SKPD Unit (Regional Work Unit) with the target being the SKPD/UKPD Unit as the implementer and the wider community as the beneficiary of the policy implementation SPBE. The research was conducted qualitatively by revealing phenomena in depth

through the perceptions and interpretations of the subjects involved, as well as understanding the problem with relevant competencies (Creswel, 1994).

In this research, adopting a concept of understanding that is in accordance with a view that emphasizes:

1. Focus on process rather than results;
2. Examining meaning, how people understand experiences;
3. Using researchers as the main instrument;
4. Involves field work and observation;
5. Descriptive approach to exploring processes, meaning, and understanding;
6. An inductive approach to building abstractions and theories from details.

The policy implementation model from Van Meter & Van Horn (1975) applies a thinking framework with six dimensions contained in the following concept operational table:

Table 6. Operational Concept

No	Draft	Dimensions	Indicator
1	The Policy Implementation Process. Van Meter Van Horn	Standard policies and objective (Dimension standards and goals policy)	1. Standard clarity and objective. 2. Relevance of standards and objective.
		The resources and incentives (Dimen resources and incentive)	3. Human Resources. 4. Incentive Policy.
		The quality of interorganizational relationships (Dimensions relationship quality between organizations)	5. Coordination and Collaboration. 6. Trust.
		The characteristics of theimplementation agencies (Dimensions institutional characteristics executor)	7. Ability and Competent. 8. Institutional Readiness Executor.
		The economic, social and politics environment (Dimension economic environment, social and political)	9. Economic, Social and Political. 10. Community Attitude.
		The disposition or response of the	11. Commitment and Support

	implementers (Dimension of disposition or implementing response)	12.Awareness and understanding

Source: IPDN Researcher @2023

Based on the concept operational table, the data collection process was carried out by interviewing and observing informants who were determined according to the criteria. Information retrieval involves the process of collecting primary and secondary data in a study (Siregar, 2013).

The selection of sources as research informants was carried out based on the criteria of policy makers, policy implementers, policy recipients and also their involvement in research aspects related to SPBE Implementation and Cyber Attacks. The key informants in this research were the Head of the DKI Jakarta Provincial Government's Communication and Information Service and SPBE management officials at that Service. Activities carried out include interviews with informants, and Focus Group Discussion participants (FGD, observations, as well as literature studies such as books, journals, articles, legal regulations and government publication documents and documents related to the topic

After the data is obtained, the data is then processed through four stages, namely data collection, data presentation, data reduction, and drawing or validating conclusions (Sugiyono, 2008).

3. Results and Discussion

4. *Policy standards and objectives*

5. SPBE is a concept that combines the principles of clean, effective and transparent government with the use of information technology. Through SPBE, various public services can be accessed electronically, enabling Jakarta residents to carry out transactions and obtain information more quickly and easily. It is hoped that the use of digital platforms can simplify public administration processes, reduce bureaucracy and increase efficiency in service delivery.
6. In the DKI Jakarta Provincial Government there is Governor Regulation Number 68 of 2022 concerning the Implementation of an Electronic-Based Government System (SPBE) which marks a significant step in the transformation of government administration towards more efficient and digitally integrated governance. Clarity of standards and policy objectives must have an information security aspect so as to ensure that SPBE implementation is not only effective in providing services, but also safe from potentially damaging cyber attacks. This policy covers crucial aspects such as risk identification, information security management, response to security incidents, and regular security evaluations.
7. Quoted from DKI Jakarta Provincial Governor Regulation No. 68 of 2022 concerning the Implementation of SPBE that "That in order to realize clean, effective, transparent and accountable government governance as well as quality and trustworthy public services, an electronic-based government system that is integrated and coordinated within the government is needed area. SPBE services are an important milestone in efforts to realize digital transformation that improves government governance."
8. Success in managing information security depends not only on existing policies, but also on how effectively these policies are implemented in practice. The government already has policies governing information security, but if these

policies do not cover all relevant aspects or are not implemented consistently across government agencies, then the risk of hacking and data leakage remains. Threats to information security continue to grow and become more complex along with technological developments. Therefore, governments must continuously update their information security policies and practices in accordance with new developments in cyber threats.

9.

10. ***The resources and incentives***

11. Resources and incentives play an important role in implementing information security because they involve a number of key elements such as budget, human resources, infrastructure and incentives given to employees who excel.

12. This was conveyed by PLT. Head of the DKI Jakarta Province Communications and Information Department that "Overall, Resources and Incentives play a key role in strengthening information security in implementing SPBE policies. "By ensuring adequate budget allocation, developing skilled and trained human resources, updating infrastructure regularly, and providing incentives to employees who excel, the government can build a solid foundation for information security within the SPBE scope in DKI Jakarta Province."

13.

14. ***The quality of interorganizational***

15. ***relationships***

16. The importance of the quality of relationships between organizations cannot be doubted in policy implementation, especially in policy implementation that involves many stakeholders.

17. The Head of the Cyber, Crypto and Applications Division of the DKI Jakarta Provincial Communication and Information Department said "With the active involvement of various OPDs, it is not only Diskominfotics that is ready to respond in handling cyber attack incidents. All OPD levels in DKI Jakarta Province also participate in efforts to maintain cyber security. This is a very important step in ensuring that government systems and services remain safe and reliable amidst the growing era of digitalization."

18.

19. ***The characteristics of the implementation agencies***

20. Based on discussions from MTRI II Community FGD participants | YY1 stated "One of the reasons internal cyber attacks are so dangerous is because they are often difficult to detect. Employees have legitimate access to systems and data, so they can easily avoid detection when carrying out attacks. Apart from that, internal attacks can also take advantage of weaknesses or gaps in internal security policies that are not strict enough."

21. It is important for organizations to adopt a comprehensive security strategy to protect themselves from internal cyber attacks. These steps include implementing strict access policies, regularly monitoring user activity, providing security training to employees, and developing effective incident handling procedures.

22.

23. The economic, social and political environment

24. The support of the DKI Jakarta DPRD in information security regulations is very important in facing the threat of cyber attacks. The political situation also has a significant impact, as stated by the Secretary of the BSSN RI that "Synergy between society and government in maintaining data security in cyber space is the key to guaranteeing data sovereignty. With a good understanding of the threats that may threaten personal data, both governments and society can work together to prevent and respond to potential cyberattacks."

25.

26. The disposition or response of the implementers

27. Transparency in responding to cyber attacks is important. The government needs to provide clear and accurate information to the public about information security incidents that occur, including the steps that have been taken to address the incidents and the efforts that are being made to prevent recurrence of attacks in the future. Efforts to improve capabilities in responding to cyber attacks must be a priority for the government in maintaining information security in the current digital era and of course in accordance with existing regulations.

28. Ka. UP, Information and Communication Technology Services Manager for the DKI Jakarta Provincial Communications and Information Technology Service, is of the opinion "It must comply with existing regulations in the DKI Jakarta Provincial Government. Apart from that, in accordance with the SOP and based on regulations from the President of the Republic of Indonesia, we have issued Presidential Regulation (Perpres) No. 95 of 2018 concerning Electronic-Based Government Systems (SPBE) and Presidential Decree no. 132 of 2022 concerning National SPBE Architecture. These two regulations provide a framework and standards for the implementation of electronic-based government services with the aim of increasing efficiency, effectiveness, transparency and accountability in government."

29.

30. Collaborative Participatory Based Policy Implementation Model (KBKP)

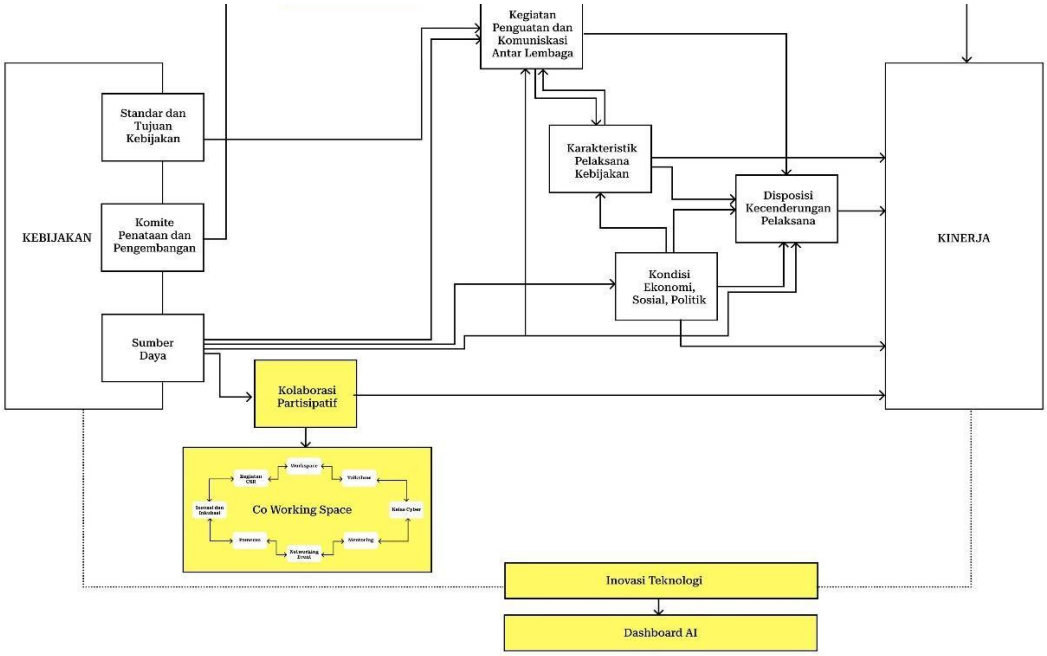
31. Based on the basic analysis previously explained, the researcher added three aspects as additional variables in developing the Van Meter and Van Horn models.

32. So, the researcher considers this variable model to be more appropriate in developing the Van Meter and Van Horn Models for Implementing SPBE Implementation Policies in the DKI Jakarta Provincial Government on Information Security Indicators.

33.

34. Figures1. Collaborative Participatory Based Policy (KBKP) on Implementation SPBE Implementation Policy in the DKI Jakarta Provincial Government:

35. Cyber Attack Case Study



36.

37. Source: Peneliti IPDN @2024

38.

39. Making the KBKP model using a Systems Thinking approach which focuses on management supervision and collaboration. By adopting the model developed by Van Meter and Van Horn, this research identifies two key aspects that are the main focus, namely management supervision and collaboration.

40. In the first keyword, Supervision in the management of Budget, Human Resources and Infrastructure is very important in anticipating cyber attacks and ensuring that the implementation of programs occurs according to predetermined plans.

41. Meanwhile, the second keyword, namely Participatory Collaboration, Optimizing the role of the JakartaProv-CSIRT Team in managing information security, can be done by Managing information security is a major challenge for many organizations and government entities in the current digital era.

4. Conclusion

The implementation of Governor's Regulation Number 68 of 2022 concerning the Implementation of Electronic-Based Government Systems (SPBE) in DKI Jakarta Province is good but improvements are still needed so that in order to increase resilience from cyber attacks, further efforts are needed to improve the information security indicators in this regulation.

The implementation of the new model prepared by researchers, namely the Collaborative Participatory Based Policy Model (KBKP) based on the Van Meter Van Horn model, is based on the principle that policies involving various stakeholders and the community can increase legitimacy and support for the policies produced.

References

Akbar, Bahrullah. 2013. Akuntansi Sektor Publik Konsep & Teori, Jakarta, CV. Bumi Metro Raya.

Instruksi Presiden Nomor 6 Tahun 2001 Pengembangan dan Pendayagunaan Telematika Indonesia

Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Gubernur DKI Jakarta Nomor 68 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik

Surat Keputusan Menteri PANRB Nomor 108 Tahun 2023 Tentang Hasil Pemantauan dan Evaluasi SPBE Pada Instansi Pusat dan Pemerintah Tahun 2022

Peraturan Menteri PANRB Nomor 59 Tahun 2020 Tentang Pemantauan dan Evaluasi SPBE

Pedoman Menteri PANRB Nomor 6 Tahun 2023 Tentang Tata Cara Pemantauan dan Evaluasi SPBE

Creswel, John. W, 1994, Research Design Qualitative & Quantitative Approaches. Sage Publication: New Delhi

Van Meter, Donald S. and Van Horn, Carl E.. 1975. "The Policy Implementation Process. A Conceptual Framework". Administration and Society, Vol.6 No.4. London: Sage Publications, Inc.

Siregar, Syofian. 2013. Statistik Parametrik untuk Penelitian Kuantitatif Dilengkapi dengan Perhitungan Manual dan Aplikasi SPSS Versi 17. Jakarta: PT. Bumi Aksara.

Denzim, Norman, K dan Yvonna S. Lincoln. 1994. Handbook of Qualitative Research. California: Sage Publications Inc.

Bungin, H. M. Burhan. 2007. Penelitian Kualitatif: Komunikasi, Ekonomi, Kebijakan Publik, dan Ilmu Sosial Lainnya, Jakarta: Kencana Penada Media, 2007.

Sugiyono, 2008. Metode Penelitian Kuantitatif, kualitatif dan R&D, Alfa Beta, Bandung.

Indrawati, L., Shafrullah, F., Akbar, Bahrullah., Effendy, K., Lukman, S., Kurniawati, L., ... Gunawan, R. (2022). Implementation of Education Operational Costs for Good Governance in DKI Jakarta

Peraturan Gubernur Nomor 68 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik

Hill, Michael and Peter Hupe. 2002. Implementing Publik Policy, London: SAGE Publications Ltd. Gutmnan

Lukman, Sampara and Suwanda, Dadang. 2021. Penyusunan Standar Pelayanan Publik, Jawa Barat: PT Remaja Rosdakarya

Suwardana Malik, S., Achmad, M., & Sutiyo, S. (2023). Penerapan E-Government Melalui Sistem Pelayanan Daring Administrasi Kependudukan Subang (Sipedas) Pada Dinas Kependudukan Dan Pencatatan Sipil. *Edusaintek: Jurnal Pendidikan, Sains Dan Teknologi*, *10*(2), 704-717. https://doi.org/10.47668/edusaintek.v10i2.826

Achmad, Mansyur. 2021. Implementasi Kebijakan Sistem Elektronik Surat dalam Mewujudkan Electronic Government