ARSIP NASIONAL
REPUBLIK INDONESIA

KAJIAN KEAMANAN ARSIP ELEKTRONIK

PUSAT PENGKAJIAN DAN PENGEMBANGAN
SISTEM KEARSIPAN
DEPUTI BIDANG INFORMASI DAN
PENGEMBANGAN SISTEM KEARSIPAN
TAHUN 2022

DAFTAR ISI

ARSIP NASIONAL
REPUBLIK INDONESIA

SAMBUTAN

DR. Andi Kasman, SE.,MM

Deputi Bidang Informasi dan Pengembangan SIstem Kearsipan

Bismillahirrahmanirrahim
Assalamualaikum Wr. Wb.

Puji syukur senantiasa kita panjatkan kehadirat Allah SWT. karena atas Rahman dan Rahim-Nya, kita senantiasa diberikan kesehatan sehat walafiat untuk terus menjalankan tugas pemerintahan kita dengan baik.

Sebagaimana yang tertuang dalam Rencana Strategis Arsip Nasional Republik Indonesia Tahun 2020-2024, upaya percepatan tranformasi digital bidang kearsipan, peningkatan keterbukan dan kemudahan akses Arsip Negara, serta layanan berbasis digital merupakan suatu keniscayaan yang harus kita laksanakan sebagai bagian dari konsekuensi terhadap perkembangan Revolusi Industri 4.0 dan *Society* 5.0 di era digital yang begitu masif.

Transformasi digital, dalam hal ini, seperti dua sisi mata uang yang saling berlawanan. Konsekuensi dari keterhubungan jaringan, pada satu sisi, membawa kemudahan dan kecepatan sementara pada sisi lain akan meningkatkan kerentanan terhadap ancaman siber. Oleh karena itu, keamanan siber menjadi salah satu isu penting dan strategis yang senantiasa menyertai dalam proses transformasi digital kearsipan. Penerapan kebijakan keamanan siber kearsipan ini sejalan dengan amanat Pasal 3 huruf f Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, yang menjelaskan bahwa *"penyelenggaraan kearsipan bertujuan untuk menjamin keselamatan dan keamanan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara"*. Sejalan dengan hal tersebut, penyusunan kajian terkait dengan Keamanan Arsip Elektronik merupakan upaya untuk menjaga agar Arsip Negara senantiasa terpelihara keauntetikannya.

Akhir kata, semoga kajian terkait dengan Keamanan Arsip Elektronik yang telah disusun dapat bermanfaat.

Wassalamualaikum wr.wb.

KATA PENGANTAR

Dalam rangka memenuhi amanat Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, Deputi Bidang Informasi dan Penyelenggaraan Sistem Kearsipan melalui Pusat Pengkajian dan Pengembangan Sistem Kearsipan melaksanakan penyusunan kebijakan terkait dengan keamanan arsip elektronik.

Penyusunan kebijakan terkait dengan keamanan arsip elektronik merupakan upaya dalam mendukung pelaksanaan transformasi elektronik bidang kearsipan. Urgensinya, bahwa pembangunan sistem , dalam hal ini sistem kearsipan elektronik, sangat bergantung kepada teknologi dan jaringan. Sementara teknologi dan jaringan ini sangat rentan terhadap serangan yang dapat menyebabkan hilangnya informasi arsip. Oleh karena itu, kesadaran untuk penerapan keamanan baik dari perangkat fisik dan jaringan sangat diperlukan guna pengelolaan arsip agar tetap autentik, utuh dan dapat dipercaya.

Tentunya dalam proses penyusunan kebijakan ini, kami menyadari masih banyak kekurangan baik dari segi materi muatan maupun pelaksanaan kegiatan. Namun, besar harapan kami agar kebijakan yang disusun dapat menjadi masukan bagi penyusunan kebijakan utamanya penyusunan kebijakan keamanan arsip elektronik. Saran dan masukan yang membangun senantiasa kami harapkan bagi seluruh pemangku kebijakan kearsipan untuk mewujudkan transformasi elektronik bidang kearsipan.

Jakarta, Desember 2022

Kepala Pusat Pengkajian dan Pengembangan Sistem Kearsipan

Dr. Muhammad Sumitro, S.H.,M.AP

DAFTAR TABEL DAN GAMBAR

RINGKASAN EKSEKUTIF

Berdasarkan Pasal 3 huruf f Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan mengamanatkan bahwa salah satu tujuan penyelenggaraan kearsipan adalah menjamin keselamatan dan keamanan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara.Melalui amanat tersebut, keamanan arsip meliputi 2(dua) aspek yaitu aspek fisik dan aspek informasi.

Aspek fisik, dalam hal ini, meliputi situs perimeter, bangunan, dan penggunaan perangkat keras (laptop dan media penyimpanan). Sementara aspek informasi meliputi keterpenuhan informasi arsip yaitu kerahasiaan, keutuhan, keautentikan, dan ketersediaan informasi.

Adapun secara struktur, dalam penyusunan kebijakan ini terdiri dari 6(enam) bab. Bab I menjelaskan tentang latar belakang perlunya kebijakan ini disusun beserta identifikasi masalah, tujuan dan kegunaan serta metode penyusunan kebijakan . Sementara Bab II menjelaskan tentang kajian teoritis dan praktik empiris yang terkait dengan penyusunan kebijakan. Adapun kajian teoritis menekankan pada definisi arsip, keamanan serta penjabaran keamanan fisik dan keamanan informasi.

Bab III menjabarkan tentang evaluasi dan analisis kebijakan perundang -undangan terkait. Adapun evaluasi ini terkait dengan kebijakan internal yang disusun oleh Arsip Nasional Republik Indonesia terkait keamanan arsip serta kebijakan eksternal yang merupakan kebijakan nasional Sistem Pemerintahan Berbasis Elektronik serta Standar Manajemen Keamanan Informasi.

Bab IV menjabarkan tentang landasan fisiologis, sosiologis dan yuridis terkait dengan peran kearsipan dalam konteks transformasi elektronik. BAB V menjabarkan tentang jangkauan, arah pengaturan, dan ruang lingkup dari materi muatan kebijakan.

BAB I
PENDAHULUAN

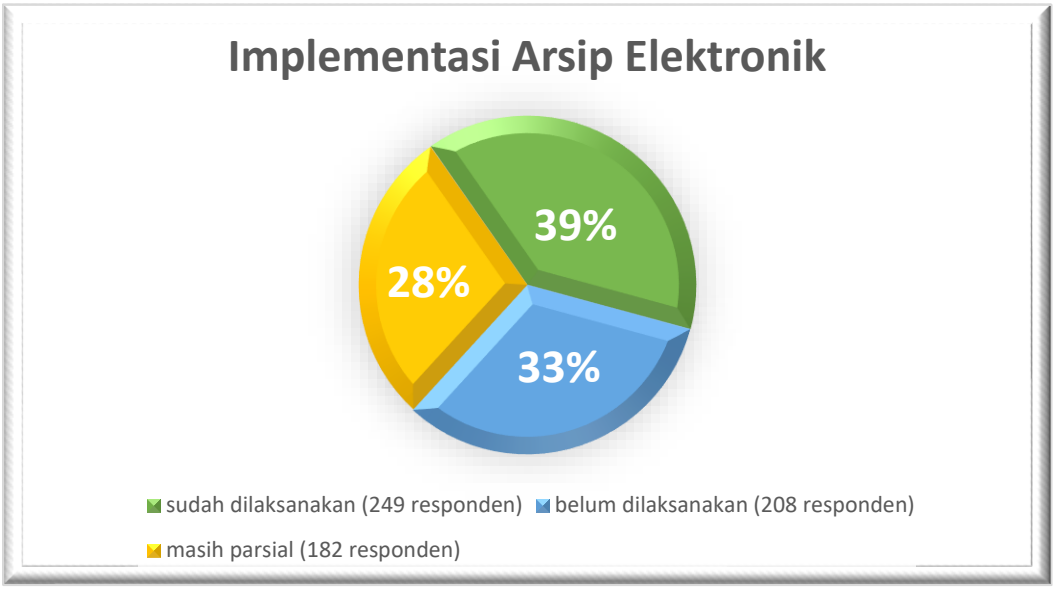
A. LATAR BELAKANG

Pasal 1 angka 2 Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan menjelaskan bahwa pengertian arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa dan bernegara. Berdasarkan penjabaran definisi arsip tersebut, proses transformasi arsip elektronik sejatinya menjadi kebijakan yang sejalan dengan kebijakan kearsipan. Pernyataan tersebut dapat dilihat dalam konteks arsip diciptakan sesuai dengan perkembangan teknologi informasi dan komunikasi. Artinya dalam pengertiannya, pengelolaan arsip sudah melingkupi konvensional maupun arsip elektronik.

Berdasarkan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) semakin memperkuat bahwa transformasi arsip elektronik di bidang kearsipan, sekaligus memberikan landasan bagi Arsip Nasional Republik Indonesia dalam melaksanakan kebijakan tersebut. Sebagai buktinya, pada pasal 63 huruf f Peraturan Presiden Nomor 95 Tahun 2018, mengkategorikan arsip sebagai salah satu bidang dalam aplikasi umum Sistem Pemerintahan Berbasis Elektronik. Impelementasinya, dapat dilihat dari aplikasi Sistem Informasi Kearsipan Dinamis terintegrasi yang saat ini lebih dikenal dengan SRIKANDI. Aplikasi Sistem Kearsipan Dinamis terintegrasi dilaksanakan pengembangan dari aplikasi Sistem Inforrmasi Kearsipan Dinamis (SIKD) yang telah dibangun dan dikembangkan sejak tahun 2009 melalui Kebijakan Kepala ANRI Nomor 15 Tahun 2009 tentang Aplikasi Sistem Informasi Kearsipan Dinamis dan Aplikasi Sistem Informasi Kearsipan Statis. Artinya, pelaksanaan transformasi kearsipan elektronik setidaknya telah diimplementasikan selama 14 (empat belas) tahun.

Namun selama kurun waktu tersebut, tentunya, selain keberhasilan juga banyak hambatan dan permasalahan yang dihadapi. Salah satunya terkait dengan implementasi kebijakan arsip elektronik. Berdasarkan hasil survey[1] dapat dilihat bahwa K/L/Daerah yang menyatakan telah melaksanakan kebijakan arsip elektronik sebesar 38% sementara 31,8% menyatakan belum melaksanakan implementasi kebijakan arsip elektronik dan 27,8% responden menyatakan bahwa kebijakan arsip elektronik masih dilaksanakan secara parsial sebagaimana dijabarkan dalam gambar berikut ini :

Gambar 1



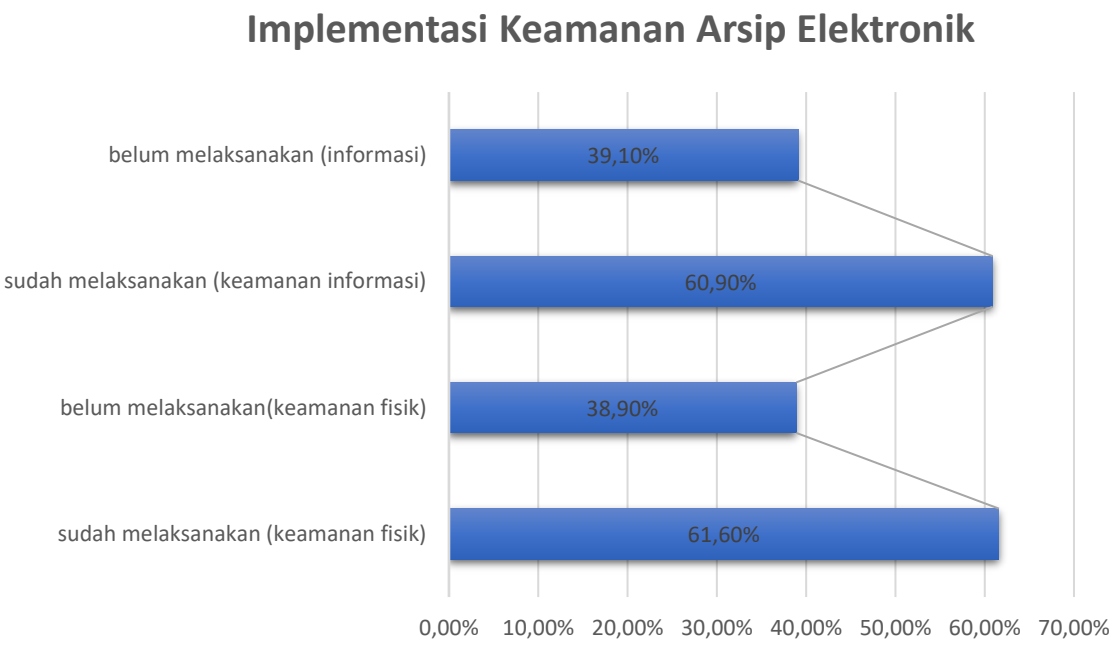
sumber: hasil survey uji publik keamanan arsip elektronik

Tentunya, melalui survey tersebut, dapat menjadikan gambaran urgensi percepatan implementasi arsip elektronik di Indonesia. Selanjutnya, salah satu aspek yang harus diperhatikan dalam implementasi kebijakan arsip elektronik adalah terkait dengan keamanan arsipnya. Sebagaimana yang kita ketahui, dalam beberapa bulan belakangan, isu terkait dengan keamanan arsip elektronik mengemuka karena adanya kebocoran data pelanggan dari PLN maupun 1,3 Miliyar data simcard di Indonesia[1]. Kebocoran tersebut membuktikan bahwa faktor

[1] Kompas. 2022. 1.3 Milyar Data SIM Card diduga bocor, begini respon 3 Opsel dan Kominfo. (Online)(1,3 Miliar Data SIM Card Diduga Bocor, Begini Respons 3 Opsel dan Kominfo (kompas.com) diakses 11 April 2022

keamanan menjadi penting untuk disusun kebijakannya. Hal tersebut karena proses transformasi arsip elektronik mewajibkan setiap proses kerja terkoneksi dalam sistem yang saling terhubung dalam jaringan internet. Pun sama halnya dengan transformasi arsip elektronik dalam penyelenggaraan kearsipan. Keamanan harus menjadi salah satu prioritas yang kebijakannya harus disusun. Terkait dengan implementasi keamanan dalam penyelenggaraan arsip elektronik, sebagaian besar K/L/D masih belum menerapkan kebijakan sebagaimana hasil survey berikut ini[2]:

Gambar 2



berdasarkan hal tersebut, urgensi kebijakan keamanan arsip elektronik penting untuk dilaksanakan sebagai aspek yang mendukung proses transformasi arsip elektronik kearsipan.

B. IDENTIFIKASI MASALAH

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah yang dapat diidentifikasi adalah bagaimana substansi materi muatan dalam keamanan arsip elektronik yang perlu untuk dilaksanakan. Lebih lanjut identifikasi masalah dapat dijelaskan sebagai berikut:

[2] Survey dilaksanakan dalam acara Uji Publik Keamanan Arsip Elektronik tanggal 28 Desember 2022. Survey dilakukan terhadap 655 peserta dari Kementerian/Lembaga/Pemerintah Daerah di Indonesia.

1. Apakah landasan filosofis, sosiologis, dan yuridis terkait dengan substansi materi dalam keamanan arsip elektronik
2. Apakah sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan dan arah pengaturan yang akan diwujudkan dalam substansi materi muatan keamanan arsip elektronik

C. TUJUAN DAN KEGUNAAN

Tujuan dari penyusunan kebijakan ini adalah untuk memberikan rekomendasi terkait dengan substansi materi muatan keamanan arsip elektronik berdasarkan pertimbangan landasan filosofis, sosiologis, dan yuridis.

D. METODE PENYUSUNAN

Metode penyusunan dilakukan menggunakan pendekatan yuridis normatif. Metode ini dilaksanakan melalui studi pustaka dan referensi lainnya yang berkaitan dengan masalah yang diidentifikasi. Selain itu untuk mempertajam substansi materi muatan metode ini dilengkapi dengan konsultasi kebijakan berupa *Focus Grup Discussion,* rapat koordinasi dengan stakeholder terkait serta dengan uji petik implementasi keamanan di instansi pemerintah.

Secara garis besar proses penyusunan kebijakan ini meliputi tiga tahapan yaitu:

1) Penyusunan desain kebijakan;
2) Pelaksanaan konsultasi kebijakan;
3) Pembahasan hasil konsultasi kebijakan
4) Pelaksanaan uji publik; dan
5) Finalisasi kebijakan

Pengolahan data dalam rumusan kebijakan ini dilaksanakan secara kualitatif dengan melaksanakan analisis dari referensi yang ada yang dikomparasikan dengan informasi yang didapatkan dari narasumber sehingga dapat menjawab permasalahan yang ada.

BAB II
KAJIAN TEORITIS

A. ARSIP ELEKTRONIK

Sebagaimana yang dijelaskan sebelumnya, berdasarkan Pasal 1 angka 2 Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan menjelaskan bahwa pengertian arsip adalah:

> rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa dan bernegara.

Sementara, Duranti dalam buku Encyclopedia of Archival Science (2016:165) menjelaskan bahwa arsip elektronik adalah :

> *"…that an electronic record, just like every traditional record, is comprised of medium (the physical carrier of the message), form (the rules of representation that allow for the communication of the message), persons (the entities acting by means of the record), action (the exercise of will that originates the record as a means of creating, maintaining, changing, or extinguishing situations), context (the juridical administrative framework in which the action takes place), archival bond (the relationship that links each record to the previous and subsequent one and to all those which participate in the same activity), and content (the message that the record is intended to convey). However, with electronic records, those components are not inextricably joined one to the other, as in traditional records: they, and their parts, exist separately, and can be managed separately, unless they are consciously tied together for the purpose of ensuring the creation of reliable records and the preservation of authentic records. Strictly speaking, it is not possible to preserve an electronic record. It is always necessary to retrieve from storage the binary digits that make up the record and process them through some software for delivery or presentation. (Duranti and MacNeil 1996, 41)"*

Berdasarkan kedua penjelasan tersebut, hal yang dapat digarisbawahi adalah arsip elektronik, sama seperti arsip konvesional, bergantung pada medium, bentuk, maupun orang. Artinya secara substantif, definisi arsip pada Undang-Undang Nomor 43 Tahun 2009 tentang kearsipan masih relevan dengan definisi arsip elektronik yang dikemukakan oleh Luciana Duranti dalam bukunya *Encyclopedia of Archival Science*, hanya saja, yang perlu untuk ditekankan selanjutnya adalah pada proses pengelolaan arsip elektronik.

B. KEAMANAN ARSIP ELEKTRONIK

Salah satu tujuan penyelenggaraan arsip elektronik berdasarkan Pasal 3 huruf f Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan adalah menjamin keselamatan dan keamanan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Selanjutnya, pada lampiran penjelasan, yang dimaksud dengan menjamin keselamatan dan keamanan arsip adalah bahwa arsip baik secara fisik dan informasinya harus dijaga keselamatan dan keamanannya, sehingga tidak mengalami kerusakan atau hilang. Dalam hal ini aspek keamanan dan keselamatan arsip terdiri dari 2 (dua) yaitu aspek keamanan fisik dan informasi arsip yang dapat dijelaskan sebagai berikut:

a. Keamanan fisik arsip elektronik

Keamanan fisik arsip elektronik sangat berhubungan dengan bangunan yang digunakan sebagai ruang simpan arsip. Namun ruang simpan itu bukan lagi berupa rak arsip, akan tetapi menjadi server dan storage yang dalam bidang informasi dan teknologi dikenal dengan nama data center atau dalam bidang kearsipan dikenal dengan nama depot arsip.

Struktur keamanan fisik pada data center dibagi kedalam 4(empat) tier atau kategori yaitu[3] :

Tier I

Tingkatan pada data center ini merupakan tingkatan paling rendah pada data center. Pada tingkatan ini infrastruktur harus mampu menyediakan 1(satu) sumber daya dan kapasitas pendingin untuk mendukung berjalannnya sistem. Infrastruktur ini memiliki jalur distribusi tunggal dan tidak ada backup data saat terjadi darurat. Persyaratan dari tier I ini meliputi :

1) tersedianya UPS;
2) tersedianya ruang yang didesain untuk sistem teknologi informasi;
3) mesin generator;
4) pendingin yang berjalan di luar jam kerja

Lebih lanjut batas toleransi gangguan maksimal 28 jam per tahun

[3] *Andreja Velimirovic. 2021. (Online) Data Center Tier Explained. Data Center Tiers Classification Explained: (Tier 1, 2, 3, 4) (phoenixnap.com)*

Tier II

Tingkatan pada infrastruktur ini termasuk di dalamnya yang meliputi Tier I dengan opsi backup data. Penambahan pada pusat data ini menawarkan perlindungan yang lebih baik terhadap gangguan yaitu:

1) mesin generator tambahan
2) penyimpanan daya
3) pendingin
4) lantai yang lebih tinggi
5) tersedianya UPS modules
6) pompa
7) pumps
8) heat rejection equipment
9) fuel tanks and cells
10) extra cooling unit

Lebih lanjut batas toleransi gangguan maksimal 22 jam per tahun

Tier III

Pada tingkatan ini, data center tingkat 2 masuk ke dalam katagori dengan persyaratan bahwa seluruh peralatan fasilitas data center tier 3 harus memiliki lebih dari 1 sumber daya listrik dan jaringan (multi network link) sehingga tidak terjadi mati pada sistem. Sementara toleransi gangguan dalam setahun maksimal hanya 1,5 jam.

Tier IV

Pada tingkatan ini, data center tier 3 masuk dalam kategori dengan persyaratan gangguan dalam setahun hanya 30 menit.

b. Kemanan informasi arsip elektronik

Keamanan informasi menjadi aspek yang penting untuk melindungi implementasi transformasi arsip elektronik. Mengutip dari International Organization for Standardization ISO/IEC 27000 – *Overview and Vocabulary (Ali Ismail Awad dan Michael Fairhurst (2018: 14) – Information Security: Foundations, Technologies, and Application* menjelaskan bahwa :

Information security: Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Lebih lanjut terkait dengan hal ini, aspek dalam keamanan informasi dapat dijelaskan sebagai berikut :

Tabel 1

Istilah	***Definisi ISO***	***Definisi NIST***
Confidentiality	*Property that information is not made available or disclosed to unauthorised including means for protecting individuals, entities or processes.*	• *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary processes information.* • *The property that sensitive information is not disclosed to unauthorised individuals, entities or processes.* • *The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorised to access the information*
Integrity	*Property of accuracy and completeness*	• *Guarding against improper information, modification or destruction, and includes ensuring information nonrepudiation and authenticity.* • *The property that sensitive data has not been modified or deleted in an unauthorised and undetected manner.*

		• *The property whereby an entity has not been modified in an unauthorised manner*
Availabilitiy	*Property of being accessible and usable upon demand by an authorised entity*	• *Ensuring timely and reliable access to and use of information* • *The property of being accessible and usable upon demand by an authorised entity*
Authenticity	*Property that an entity is what it claims to be*	• *The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message or message originator*
Accountability		• *The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non repudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action.* • *Principle that an individual is entrusted to safeguard and control equipment, keying material and information and is answerable to proper authority for the loss or misuse of that equipment or information*
Non-repudiation	*Ability to prove the occurrence of a claimed event or action and its originating entities*	• *Assurance that the sender of information is provided with proof of the sender's identity, so neither can later deny having processed the information* • *Protection against an individual falsely denying having performed a particular*

		action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving and information receiving a message. • *Is the security service by which the entities involved in a communication cannot deny having participated. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin), and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).* • *A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e. the signatory).*
Reliability	*Property of consistent – intended behaviour and results*	

BAB III
EVALUASI DAN ANALISIS KEBIJAKAN PERUNDANG-UNDANGAN TERKAIT

A. ANALISA TERKAIT DENGAN KEBIJAKAN BIDANG KEARSIPAN

Sebagaimana yang telah disebutkan pada Bab II, bahwa berdasarkan pasal 3 huruf f bahwa salah satu tujuan penyelenggaraan kearsipan adalah untuk menjamin keselamatan dan keamanan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa dan bernegara. Lebih lanjut, pada penjelasannya, yang dimaksud dengan menjamin keselamatan dan keamanan arsip adalah bahwa arsip baik secara fisik maupun informasinya harus dijaga keselamatan dan keamanannya, sehingga tidak mengalami kerusakan atau hilang. Dalam hal ini, dapat disimpulkan bahwa keamanan arsip terdiri dari 2(dua) aspek utama yaitu keamanan fisik arsip dan keamanan informasi arsip.

Terkait dengan keamanan arsip elektronik, ANRI juga telah menetapkan Kebijakan Kepala ANRI Nomor 7 Tahun 2016 tentang Petunjuk Pelaksanaan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis di Lingkungan ANRI. Substansi dalam kebijakan tersebut merupakan amanat dari Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, dengan menitikberatkan pada keamanan pengelolaan arsip dinamis sebagaimana gambar berikut ini:

Gambar 3

Selain kebijakan tersebut, ANRI juga telah menetapkan Kebijakan Kepala ANRI Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia. Substansi materi muatan terkait dengan Manajemen Keamanan Informasi meliputi:

a. manajemen pengelolaan;
b. kebijakan umum yang dijabarkan sebagai berikut:
    - pengendalian kontrol akses
    - pengendalian kontrol akses;
    - pengendalian pengelolaan gangguan keamanan informasi;
    - pengendalian keamanan informasi dalam pengadaan, pengembangan,dan pemeliharaan sistem informasi;
    - pengendalian keamanan fisik dan lingkungan;
    - pengendalian pengelolaan aset informasi;
    - pengendalian pengelolaan komunikasi dan operasional;
    - pengendalian keamanan sumber daya manusia;
    - pengendalian organisasi keamanan informasi; dan pengendalian umum.

adapun hubungan terkait hal tersebut diatas dapat dijabarkan melalui gambar 4.

Gambar 4

Kebijakan Kepala Arsip Nasional Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi

Sesuai dengan penjabaran tersebut, setidaknya ada beberapa hal yang penting yaitu:

a. berdasarkan Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan setidaknya ada 2(dua) aspek yang berkaitan dengan keamanan (dan keselamatan) arsip yaitu aspek fisik arsip dan aspek informasi arsip. Kedua aspek ini dapat menjadi landasan dalam penyusunan materi muatan terkait dengan keamanan arsip
b. lebih lanjut, pada Kebijakan Kepala ANRI Nomor 7 Tahun 2016 tentang Petunjuk Pelaksanaan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis di Lingkungan ANRI, dijabarkan secara lebih lengkap bagaimana cakupan keamanan fisik dan keamanan informasi arsip. Meskipun ruang lingkup implementasi Kebijakan ini adalah arsip dinamis namun dapat dijadikan landasan dalam penyusunan substansi materi muatan kebijakan. Apabila arsip dinamis memiliki kategori keamanan berdasarkan sifatnya yaitu biasa/terbuka, terbatas, rahasia, dan sangat rahasia maka untuk keperluan akses klasifikasi arsip juga bisa diklasifikasikan sebagai arsip terbuka dan tertutup.
c. Kebijakan Kepala Arsip Nasional Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi disusun berdasarkan *International Organization for Standardization ISO/IEC 27000.* Keamanan fisik dan keamanan informasi menjadi bagian dalam manajemen keamanan informasi. Ditambah lagi materi muatan juga fokus kepada pengelolaan sistem informasi dimana proses manajerial dan penjabaran tugas fungsi masing-masing unit kerja dijabarkan.

B. ANALISA TERKAIT DENGAN KEBIJAKAN NASIONAL BIDANG TEKNOLOGI INFORMASI

Sehubungan dengan keamanan arsip elektronik, tentunya tidak lepas dari Kebijakan Presiden 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Pada Pasal 2 dijelaskan bahwa salah satu prinsip Sistem Pemerintahan Berbasis Elektronik adalah keamanan yang mencakup kerahasiaan, keutuhan, ketersediaan, keaslian dan kenirsangkalan. Selanjutnya sebagai amanat dari kebijakan Sistem Pemerintahan Berbasis Elektronik, Badan Siber dan Sandi Negara yang memiliki fungsi teknis terkait dengan keamanan

siber, menetapkan Kebijakan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik. Pada Kebijakan tersebut, setidaknya terdapat 5 cakupan dalam keamanan yaitu aspek keamanan data dan informasi, standar teknis dan prosedur keamanan aplikasi, standar teknis keamanan jaringan intra, standar teknis keamanan pusat data nasional, serta standar teknis keamanan sistem penghubung layanan sebagaimana gambar berikut ini:

Gambar 5

Tentunya dalam penyusunan substansi kebijakan keamanan arsip elektronik harus dapat dilakukan adaptasi terhadap setiap ketentuan yang telah disusun. Artinya bahwa arsip memiliki keunikan dan kebutuhan khusus dalam pelaksanaan pengamanannya namun tidak terlepas dari ketentuan umum yang telah disusun.

BAB IV
LANDASAN FISIOLOGIS, SOSIOLOGIS, DAN YURIDIS

A. LANDASAN FILOSOFIS

Landasan filosofis dalam pembentukan kebijakan terkait dengan keamanan arsip elektronik merujuk pada cita- cita hukum (*Reichtsidee*[4]) yang tercantum pada Undang-Undang Dasar 1945 serta Pancasila. Sesuai dengan tujuan negara yang tercantum dalam Pembukaan Undang-Undang Dasar 1945 yaitu:

> "untuk membentuk suatu Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasar kemerdekaan, perdamaian abadi dan keadilan sosial…"

Berdasarkan tujuan tersebut, dapat dijabarkan salah satu hal yang ingin dicapai melalui penyelenggaraan pemerintahan adalah untuk melindungi segenap rakyat yang ada di dalamnya. Lebih lanjut, berdasarkan Pasal 28G Undang-Undang Dasar 1945 bahwa setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia. Artinya bahwa Undang-Undang Dasar 1945 menjamin hak asasi rakyat Indonesia dalam melaksanakan kehidupan dan negara memiliki tugas untuk melindungi agar hak-hak rakyat tersebut dapat terpenuhi dan dilindungi sesuai dengan kebijakan yang telah ditetapkan.

Melalui penyusunan kebijakan tentang Keamanan Arsip Elektronik, dalam hal ini negara hadir (dalam bidang kearsipan) untuk melindungi dan menjamin

---

[4] Sebagaimana penjelasan pada Undang-Undang Dasar 1945 bahwa Undang-Undang menciptakan pokok-pokok pikiran yang terkandung dalam pembukaan dalam pasal pasalnya. Pokok-pokok pikiran tersebut meliputi suasana kebatinan dari Undang-Undang Dasar Negara Indonesia. Pokok-pokok pikiran ini mewujudkan cita cita hukum (*Reichtsidee*) yang menguasai hukum dasar negara, baik hukum yang tertulis maupun huum yang tidak tertulis

keamanan dalam penyelenggaraan arsip elektronik sementara masyarakat memiliki hak untuk dapat membuat, mengelola, dan mengakses arsip elektronik sesuai dengan kebijakan yang telah disusun. Oleh karenanya kebijakan yang disusun harus berdasarkan prinsip dan kaidah kearsipan.

Sementara itu, pengaturan terhadap keamanan arsip elektronik juga menjadi relevan dengan nilai nilai yang terkandung dalam Pancasila. Pada Sila Pertama, Ketuhanan yang Maha Esa, bahwa dengan terjaminnya Keamanan Arsip Elektronik, potensi penyalahgunaan arsip, penyebaran arsip yang tidak autentik dan tidak berdasarkan fakta yang ada, akan dapat dihindari. Penyalahgunaan dan penyebaran arsip yang tidak autentik dan tidak berdasarkan fakta yang ada dapat menyebabkan mengancam kerukunan umat beragama yang lebih lanjut dapat menyebabkan disintegrasi dan perpecahan bangsa.

Pada Sila Kedua Pancasila, Kemanusiaan yang Adil dan Beradab, apabila dihubungkan dengan penyusunan kebijakan keamanan arsip elektronik, bahwa materi muatan dalam kebijakan ini juga mengadaptasi dari berbagai peraturan internasional bidang kearsipan yang sedang berlaku saat ini. Selain itu kebijakan ini juga disusun dengan memperhatikan berbagai kebijakan nasional bidang keamanan siber. Sehingga dalam hal ini adanya kolaborasi antara berbagai kebijakan yang berlaku. Sementara pada Sila Ketiga Pancasila, Persatuan Indonesia, bahwa kebijakan keamanan arsip elektronik bertujuan untuk melindungi arsip elektronik dari penyalahgunaan yang dapat memecah kesatuan, persatuan, kepentingan dan keselamatan bangsa dan negara.

Pada Sila Keempat Pancasila, Kerakyatan yang dipimpin oleh hikmat Kebijaksanaan dalam permusyawaratan perwakilan adalah bahwa materi muatan yang disusun telah melalui hasil diskusi dengan para pemangku kepentingan terkait. Melalui proses diskusi ini dihasilkan suatu kesepakatan yang tercantum dalam materi muatan kebijakan. Sementara pada Sila terakhir, Keadilan Sosial bagi Seluruh Rakyat Indonesia, penyusunan kebijakan tentu diarahkan pada terwujudnya penyelenggaraan kearsipan elektronik yang sesuai dengan kaidah dan prinsip kearsipan. Selain itu dengan adanya pengaturan terhadap keamanan arsip elektronik, maka diharapkan akan terwujud keadilan merata dalam pemanfaatan arsip elektronik untuk kemajuan bangsa dan negara.

B. LANDASAN SOSIOLOGIS

Pembentukan suatu kebijakan memerlukan landasan sosiologis agar masyarakat dapat mengetahui dan memberikan masukan terkait dengan penyusunan kebijakan tersebut. Hal ini penting untuk menjamin "legalitas" kebijakan yang disusun bukan hanya dari aspek hukum namun juga dalam aspek sosial. Penetapan kebijakan harus memastikan bahwa nantinya tidak ada resistensi terhadapnya.

Indonesia merupakan negara yang dikenal dengan kemajemukan suku bangsa yang tersebar pada setiap provinsi maupun kabupaten kota. Menurut Laporan Badan Pusat Statistik[1], jumlah Provinsi di Indonesia adalah sebesar 34 Provinsi. Dari 34 Provinsi tersebut, jumlah kabupaten yang tercatat adalah sebanyak 416, dengan jumlah kota sebanyak 98. Tentunya dari masing masing Provinsi, Kabupaten, maupun Kota di Indonesia sendiri memiliki kebudayaan yang berbeda-beda.

Perbedaan ini menjadikan negara Indonesia merupakan negara yang kaya budaya namun juga tantangan bagi pengelolaannya. Pengelolaan di sini bukan hanya dalam hal pelestarian, namun juga merujuk pada aspek pelindungan terhadap kemajemukan ini. Potensi kehilangan budaya menjadi tinggi apabila arsip yang merupakan memori kolektif bangsa yang menjadi rujukan identitas dan jati diri bangsa tidak terkelola dengan baik.

Disisi lainnya, ancaman terhadap hilangnya memori kolektif bangsa ini, juga semakin tinggi seiring dengan dengan pesatnya perkembangan teknologi informasi. Menteri Komunikasi dan Informasi[5] bahkan mengungkapkan bahwa pada sepanjang tahun 2021 tercatat ada 888.711.736 ancaman siber yang terjadi di Indonesia. Artinya dengan tingkat kerentanan yang tinggi tersebut, keamanan terhadap arsip elektronik sangat perlu untuk diprioritaskan.

Oleh karena itu landasan sosiologis pembentukan kebijakan terkait dengan keamanan arsip elektronik ini adalah bahwa penyusunan standar keamanan arsip dalam konteks elektronik adalah upaya untuk melindungi identitas dan jati diri

---

[5] suara.com. 2021. Kominfo: Ada 888 Juta Ancaman Siber di Indonesia Sepanjang 2021 (Online) (Kominfo: Ada 888 Juta Ancaman Siber di Indonesia Sepanjang 2021 (suara.com) diakses 11 April 2022

bangsa dari berbagai macam serangan elektronik yang dapat mengancam kedaulatan negara. Apabila dirumuskan maka landasan sosiologis dari penyusunan kebijakan ini adalah:

> “ bahwa keamanan arsip dalam konteks arsip elektronik perlu ditetapkan sebagai bagian dari upaya pelindungan terhadap identitas dan memori bangsa sebagaimana amanat Pasal 32 Undang-Undang Dasar 1945 Negara Republik Indonesia”

C. LANDASAN YURIDIS

Landasan yuridis pembentukan kebijakan ini merupakan amanat dari Undang- Undang Nomor 43 Tahun 2009 tentang Kearsipan. Dalam Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan disebutkan bahwa (salah satu) tujuan penyelenggaraan kearsipan adalah menjamin keamanan dan keselamatan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa dan bernegara. Amanat ini menjadi tugas dan tanggung jawab Arsip Nasional Republik Indonesia untuk senantiasa memastikan bahwa arsip yang dikelola dapat dijamin keamanan dan keselamatannya.

Selanjutnya, hal ini juga diperkuat dengan ditetapkannya Peraturan Presiden Nomor 85 tentang Sistem Pemerintahan Berbasis Elektronik. Dimana dalam Peraturan Presiden tersebut, salah satu asas yang dipakai adalah dalam pembangunan arsitektur Sistem Pemerintahan Berbasis Elektornik adalah asas keamanan.

Tentunya dalam hal penyelenggaraan kearsipan konteks keamanan arsip elektronik harus disusun meskipun melalui Peraturan Presiden yang sama amanat terkait dengan keamanan menjadi tugas fungsi Badan Siber dan Sandi Negara. Namun Arsip Nasional harus menerapkan standar yang sesuai dengan prinsip-prinsip kearsipan untuk dapat dielaborasi dengan ilmu teknologi informasi

BAB V
JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP MATERI MUATAN

A. ARAH DAN JANGKAUAN PENGATURAN

Berdasarkan uraian pada Bab III, maka arah pengaturan dalam penyusunan kebijakan ini adalah bahwa keamanan arsip elektronik dilaksanakan berdasarkan prinsip kerahasiaan, keautentikan, keutuhan, kenirsangkalan dan ketersediaan. Selain itu arah dan jangkauan pengaturan tidak terlepas dari konteks, konten, dan struktur dari arsip elektronik. Substansi diharapkan mampu memberikan landasan hukum penyelenggaraan keamanan arsip elektronik, yang disusun berdasarkan pertimbangan filosofis, sosiologis, dan yuridis dalam penyelenggaraan kearsipan elektronik.

B. RUANG LINGKUP MATERI MUATAN

Ruang lingkup materi muatan dalam penyusunan kebijakan arsip elektronik dapat dijabarkan sebagai berikut:

1. Batasan Definisi

    a. Arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi poloitik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat berbangsa dan bernegara

    b. Keamanan arsip elektronik adalah upaya menempatkan arsip elektronik pada tempat yang aman untuk menjamin ketersediaan arsip elektronik

    c. Keamanan fisik arsip elektronik adalah keamanan yang meliputi perimeter, bangunan, dan perangkat keras pada penyelenggaraan kearsipan

    d. Keamanan informasi arsip elektronik adalah terjaganya kerahasiaan, keutuhan, keautentikan, dan ketersediaan informasi

e. Penerapan klasifikasi arsip: klasifikasi adalah pengkategorian/penggolongan arsip dinamis berdasarkan tingkat keseriusan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik, dan perorangan

2. Tujuan

Penyusunan kebijakan keamanan arsip elektronik bertujuan untuk

a. Menjamin ketersediaan arsip elektronik dalam penyeelnggaraan kearsipan

b. Menjamin terwujudnya pengelolaan arsip elektronik yang andal sesuai dengan ketentuan kebijakan perundang-undangan

c. Meningkatkan kualitas pelayanan publik dalam penyelenggaraan arsip elektronik

3. Kategori Penerapan

a. Penerapan keamanan arsip elektronik terbagi dalam 2(dua) katagori :

b. Keamanan fisik arsip elektronik yang meliputi keamanan perimeter, keamanan bangunan, dan keamanan perangkat keras

c. Keamanan informasi arsip elektronik yang meliputi kerahasiaan, keutuhan, keautentikan, dan ketersediaan informasi

4. Keamanan Fisik

a. Keamanan perimeter

Keamanan perimeter adalah sistem dan teknologi yang dibangun untuk melindungi tempat penyimpanan arsip elektronik dengan menghalangi intrusi fisik yang tidak sah di sekeliling area. Panduan terhadap keamanan perimeter arsip elektronik paling sedikit meliputi :

1. Pembangunan area penyimpanan server arsip elektronik yang terpisah dari ruang kerja

2. Pembangunan pagar menyeluruh disekeliling bangunan

3. Lokasi area jauh dari bencana alam seperti banjir gempa bumi atau kebakaran
4. Konstruksi bangunan mampu menahan goncangan minimal 8.5 SR
5. Akses keluar masuk 1 (satu) tempat
6. Pemasangan CCTV pada sekeliling bangunan yang dapat dipantau terus menerus
7. Pemasangan thermal detection dan metal detection pada area pintu masuk

b. Keamanan bangunan adalah sistem dan teknologi yang dibangun untuk melindungi bangunan dan menjaga keamanan peralatan yang ada di dalamnya. Panduan terhadap keamanan bangunan arsip elektronik meliputi:

1. Area bangunan terdiri dari bangunan utama serta ruang pusat kontrol dan akses keamanan terpisah
2. Pemilihan jenis rack server yang disesuakan dengan server dengan memperhatikan jarak peletakan (space)
3. Sistem kelistrikan terdiri berbagai sumber dan diberikan cadangan genset minimal 2 buah berkapasitas 1.5 MW yang dikontrol secara otomatis
4. *Dry bulb* dan *wet bulb temperature* 18-27 derajat celcius dengan kelembaban maksimal 60% (64,4 – 80,44 F)
5. Terpasangnya *rodent repellent system*
6. Terpasangnya water *cooling system* dan *water leakage detector*
7. Terpasangnya alarm kebakaran dan *smoke detector*
8. Terpasangnya sistem akses kontrol pintu dengan akses pintu masuk hanya dari 1(satu) tempat

9. Pemasangan thermometer minimal menggunakan thermohygrometer TH95 karena dapat menampilkan suhu, kelembaban, dan waktu serta adanya sensor suhu ruangan.
10. Jaringan kabel dipasang di lantai yang lebih tinggi untuk mengurangi kabel terlalu panas *(overheat cabling)* dan mengurangi panas di ruangan

c. Keamanan perangkat keras

Keamanan perangkat keras adalah perlindungan perangkat fisik dari ancaman yang memfasilitasi akses tidak sah ke sistem. Panduan terhadap keamanan perangkat keras meliputi:

1. Perangkat komputer atau laptop yang digunakan telah terdaftar sesuai ketentuan dan prosedur Barang Milik Negara (BMN)
2. Tidak menggunakan hard drives komputer untuk menyimpan informasi yang penting.
3. Secara berkala membersihkan sistem komputer dan lokasi jaringan dengan menghancurkan catatan yang digantikan atau using yang telah melewati masa retensi
4. Secara berkala melaksanakan backup terhadap arsip
5. Memastikan bahwa sistem komputer dikonfigurasi dengan sistem keamanan dengan minimal sebagai berikut:
6. Antivirus dipasang dan diupdate berkala;
7. Proteksi password dengan minimal verifikasi 2 langkah *(two step verification) saat* login akun
8. Mengaktifkan dinding api *(firewall)* untuk menyaring informasi dari internet
9. Mengosongkan cookies yang tidak diinginkan atau dibutuhkan dari peramban
10. Memastikan penggunaan https saat browsing dari internet
11. Memasang kunci otomatis untuk mencegah akses terhadap perangkat keras apabila sedang tidak digunakan

d. Keamanan Informasi

Keamanan informasi arsip elektronik dilaksanakan dengan memperhatikan aspek:

1. Kerahasiaan
2. Keutuhan,
3. Keautentikan, dan
4. ketersediaan informasi

Tabel 2

Aspek	Definisi	Persyaratan minimal :	Keterangan
Kerahasiaan	Informasi arsip tidak tersedia untuk orang yang tidak berwenang kecuali telah disetujui oleh pihak yang berwenang	1. Arsip diciptakan oleh pengguna berdasarkan format tata naskah dinas kearsipan elektronik 2. Arsip diklasifikasikan berdasarkan sistem klasifikasi keamanan dan akses arsip 3. Bagi arsip elektronik : a. Arsiparis melakukan alih media dan mencatat metadata yang dibutuhkan dan menyusun berita acara b. Pengguna yang memiliki hak akses memvalidasi arsip yang masuk ke dalam sistem c. Dalam tahapan penggunaan, enskripsi asimetris dengan fungsi HAS merupakan persyaratan wajib yang harus diterapkan untuk transaksi antar jaringan d. Penetapan hak akses untuk arsip statis : a. Arsiparis (admin); b. Pengguna c. Super admin (IT)	Telah dimuat dalam Perka 17/2011 tentang Pedoman Pembuatan Sistem dan Klasifikasi Arsip Dinamis

Keutuhan	Arsip yang akurat dan komplit	1. Arsiparis melakukan verifikasi dan validasi arsip elektronik secara berkala (minimal dilaksanakan per 3 bulan sekali) 2. Arsiparis memvalidasi bahwa struktur naskah sesuai dengan kebijakan terkait dengan tata naskah dinas elektronik	
Keautentikan	Arsip yang dapat dipercaya informasinya	1. Menerapan tanda tangan elektronik tersertifikat saat penciptaan arsip 2. Arsiparis memastikan bahwa tanda tangan elektronik tersebut sesuai dengan pengguna 3. melaksanakan *ingest* arsip untuk memastikan keamanan data saat proses *transmiting* data dari asli ke arsip dan merekam metadata *assurance* 4. memelihara arsip yang tersimpan dengan melakukan pengecekan secara berkala	Arsip elektronik dapat diautentikasi dengan tanda tangan elektronik tersertifikasi yang dapat diverifikasi oleh semua orang yang menggunakan arsip..
Ketersediaan informasi	Arsip elektronik tersedia sampai kapanpun	Melaksanakaan backup data 1. Data yang harus disimpan minimal asli, kopi master, kopi akses dan kopi backup.	Jenis backup data: 1. Asli : arsip asli disimpan bahkan jika file sudah dikonversi ke format pelestarian elektronik untuk

		2. Arsiparis memvalidasi metadata asli, kopi master, kopi akses dan kopi backup dan menyusun berita acara validasi arsip	penggunaan jangka Panjang 2. Kopi master : sama dengan aslinya dengan akses terbatas untuk arsiparis 3. Kopi akses : digunakan untuk publik dengan file format yang berbeda dan disunting untuk menyimpan informasi yang tertutup. Kopi backup: penyimpanan file di lokasi terpisah

e. Penanganan Insiden Keamanan Arsip Elektronik

Insiden keamanan arsip elektronik adalah gangguan pada sistem, pelayanan atau jaringan yang mengindikasikan kesalahan kebijakan keamanan,kegagalan pengamanan, maupun terjadinya keadaan yang tidak diinginkan yang mempengaruhi kinerja sistem elektronik kearsipan

Cara mendeteksi

Dilakukan pemeriksaan terhadap :

1. Histori log domain: membantu dalam mengidentifikasi upaya untuk memecahkan nama domain berbahaya atau alamat IP
2. Histori server email: membantu mendeteksi target pengguna yang dikirikan email yang tidak sesuai
3. Histori gateway : membantu mengidentifikasi lalu lintas anomali jaringan atau berbahaya
4. Histori sistem operasi dan aplikasi: dapat membantu mengidentifikasi aktivitas anomaly atau berbahaya
5. Histori akses jarak jauh: membantu mengidentifikasi sumber alamat yang tidak biasa, waktu untuk akses (log in maupun log off) yang mengindikasikan aktivitas mencurigakan
6. Histori web proxy: membantu mengidentifikasi Hypertext Transfer Protocol (HTP) dan lalu lintas jaringan yang mencurigakan
7. Berita acara registrasi arsip: membantu mengidentifikasi fungsi Has dan metadata file arsip

Penanganan

Apabila terjadi insiden keamanan maka perlu untuk dilakukan pendokumentasian dengan persyaratan sekurang kurangnya sebagai berikut:

1. Tanggal pelaksanaan kejadian
2. Tanggal temuan kejadian
3. Deskripsi insiden keamanan
4. Tindakan yang dilakukan
5. Penanggung jawab insiden

KESIMPULAN DAN REKOMENDASI KEBIJAKAN

A. KESIMPULAN

Berdasarkan hasil analisis kebijakan dapat disimpulkan hal-hal sebagai berikut:

1. Keamanan arsip elektronik sebagaimana diamanatkan dalam Undang-Undang 43 tahun 2009 terdiri dari keamanan fisik dan keamanan informasi. Keamanan fisik adalah upaya menjaga keberadaan arsip secara fisik melalui standar bangunan dan ruang penyimpanan. Keamanan informasi terkait dengan arsip yang harus memenuhi kriteria kerahasiaan, keautentikan, keutuhan dan ketersediaan informasi.
2. Keamanan fisik pada arsip sangat berhubungan dengan pengelolaan depot arsip elektronik yang terintegrasi. Mengingat bahwa dalam kondisi eksisting saat ini server dan storage penyimpanan arsip masih tersebar setidaknya di 3(tiga) tempat yaitu ANRI, Perpustakaan Nasional, dan Pusat Data Nasional.
3. Identifikasi terhadap ketentuan dalam pelaksanaan keamanan arsip elektronik, memberikan perspektif bagi tugas dan peran arsiparis dalam pengelolaan arsip elektronik. Sehingga arsiparis harus memiliki kemampuan dalam pengelolaan Informasi Teknologi.

B. REKOMENDASI KEBIJAKAN

1. Substansi materi muatan dalam kebijakan ini dapat menjadi masukan bagi Arsip Nasional Republik Indonesia dalam pembuatan Pusat Data Nasional Kearsipan. Mengingat bahwa arsip memiliki prinsip kearsipan yang menjadi landasan bagi penyelenggaraan arsip elektronik. Kolaborasi dengan informasi teknologi diperlukan namun tidak menghilangkan persyaratan fungsional yang harus dipenuhi dari segi kearsipan
2. Perlu adanya penyiapan Pendidikan dan Pelatihan bagi arsiparis dalam pelaksanaan transformasi digital bidang kearsipan yang dapat sekurang kurangnya memahami:
   a. metada dan fungsi has dalam proses verifikasi dan validasi arsip;
   b. melakukan *audit log* dalam proses pengelolaan arsip elektronik; dan
   c. memelihara arsip elektronik dalam masa inaktif maupun preservasi secara berkala

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Undang-Undang Republik Indonesia Tahun 1945

Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Kepala ANRI Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia

Peraturan Kepala Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik

Kebijakan Kepala ANRI Nomor 7 Tahun 2016 tentang Petunjuk Pelaksanaan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis di Lingkungan ANRI

Literatur

Awad, Ismail Ali dan Michael Fairhurst. 2018. *Information Security: Foundation, Technologies and Application: The Institution of Engineering and Technology*

Hefty, John Kingsley. 2013. *Physical Seurity Strategy and Process Playbook: The Security Executive Council*

Duranti, Luciana and Patricia C. Franks. 2015. *Encyclopedia of Archival Science*: Rowman & Littlefield

Mendel, Ronald L. 2007. *Document Security :* Charles C. Thomas Publisher. Ltd

Website

Kompas. 2022. 1.3 Milyar Data SIM Card diduga bocor, begini respon 3 Opsel dan Kominfo. (Online)(1,3 Miliar Data SIM Card Diduga Bocor, Begini Respons 3 Opsel dan Kominfo (kompas.com) diakses 11 April 2022

Andreja Velimirovic. 2021. (Online) Data Center Tier Explained. Data Center Tiers Classification Explained: (Tier 1, 2, 3, 4) (phoenixnap.com)

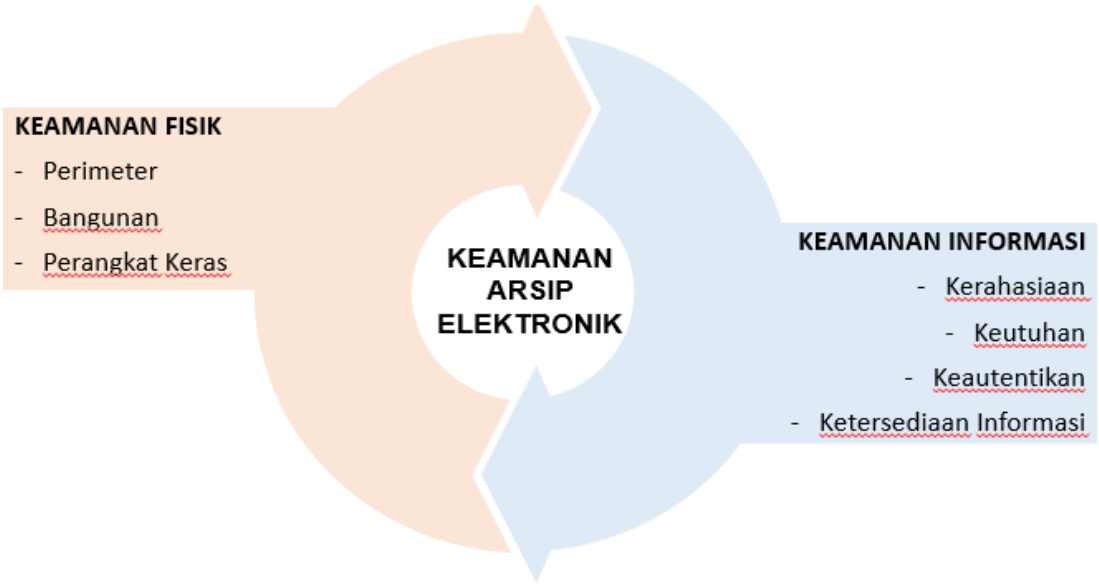
Gillialand-Swetland,Anne J dkk. 200. Preserving the Authenticity of Contingent Digital Objects. Preserving the Authenticity of Contingent Digital Objects: The InterPARES Project (dlib.org)

Bearman, David. Moment of Risk: Identifying Threats to Electronic Records

LAMPIRAN I

KERANGKA TEORI KEBIJAKAN

Berdasarkan landasan teori yang telah dikemukakan sebelumnya maka kerangka rancangan kebijakan terkait dengan keamanan arsip elektronik adalah sebagai berikut:



Kerangka desain kebijakan tersebut merujuk pada amanat pada Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan dimana keamanan (dan keselamatan) arsip merujuk pada fisik dan informasi arsip.

Selanjutnya, sebagaimana hasil uji publik yang dilaksanakan dengan mengundang narasumber (salah satunya) dari Kementerian Komunikasi dan Informatika, memberikan informasi bahwa Pusat Data Nasional nantinya akan menjadi media penghubung bagi lembaga dalam proses transaksi elektronik. Kondisi yang berjalan saat ini, Pusat Data Nasional berperan sebagai data center untuk seluruh Kementerian/Lembaga, namun ke depan, Kementerian/Lembaga berperan sebagai wali data bagi masing masing data yang dimiliki.

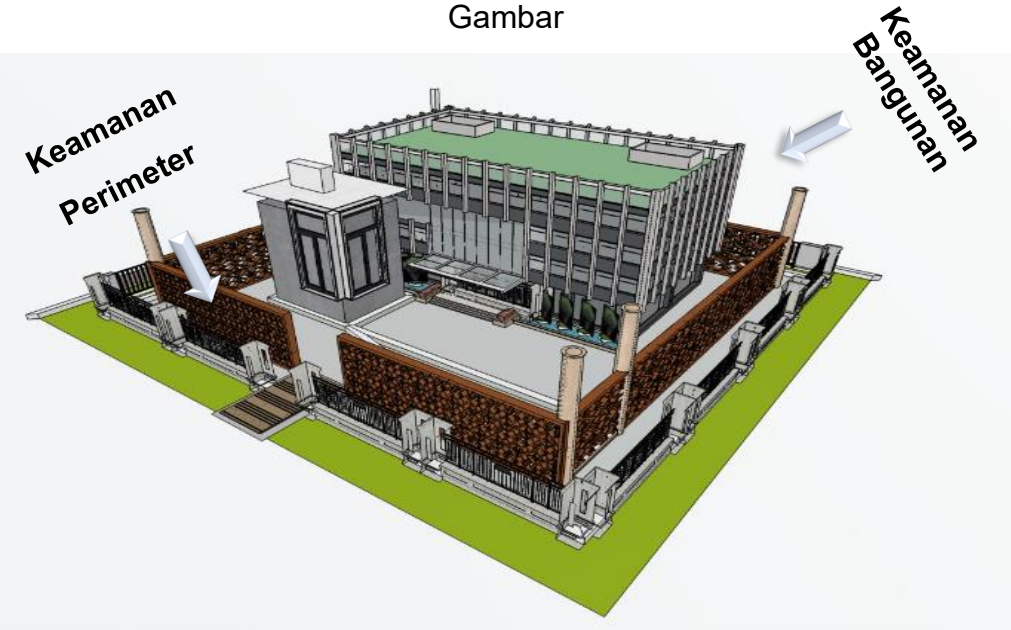
Pun sama halnya dengan uji publik yang dilaksanakan dengan mengundang narasumber (salah satunya) dari Satu Data Indonesia. Satu Data Indonesia saat ini masih berfokus pada aspek pemenuhan data geospasial. Arsip Nasional Republik Indonesia, sebagai satu satunya lembaga yang menyelenggarakan data kearsipan nasional, dapat berperan sebagai wali data untuk arsip. Pengajuan Arsip Nasional

sebagai walidata tersebut, harus melalui forum satu data dan disepakati oleh tim Satu Data.

Merujuk kedua pernyataan narasumber tersebut, Arsip Nasional Republik Indonesia dalam penyelenggaraan arsip elektronik, memiliki peluang besar dalam proses transformasi elektronik. Peluang ini harus dimanfaatkan dengan mempersiapkan strategi dan kebijakan, salah satunya keamanan arsip elektronik sebagai bagian dari proses penyelenggaraan arsip elektronik.

Dalam hal keamanan fisik arsip yang menjadi cakupan pembahasan dalam penyusunan kebijakan ini meliputi keamanan perimeter, keamanan bangunan, dan keamanan perangkat keras. Keamanan fisik arsip elektronik erat kaitannya dengan pembangunan depot arsip elektronik. Pada depot arsip konvensional, yang disimpan adalah arsip konvensional yang tersimpan dalam *filling cabinet.* Namun dalam konsep depot arsip elektronik yang disimpan dan dipelihara adalah server dan storage.Terkait dengan keamanan fisik dapat dijelaskan berikut ini:

Gambar



a. Keamanan perimeter

   Keamanan perimeter adalah sistem dan teknologi yang dibangun untuk melindungi tempat penyimpanan arsip elektronik dengan menghalangi intrusi fisik yang tidak sah di sekeliling area. Terkait dengan hal tersebut, berdasarkan hasil pengumpulan data, di Arsip Nasional Republik Indonesia sendiri setidaknya ada 3 (tiga) substansi penyelenggaraan kegiatan yang menggunakan server dan storage sebagai media penyimpanan yaitu:

1) Server dan storage SRIKANDI yang dikelola oleh Pusat Data dan Informasi. Saat ini kapasitas storage Pusat Data dan Informasi sebesar 49,162 Gigabyte dengan 17 TB telah terpakai sehingga sisa kapasitas storage yang tersedia sebesar 31 TB. Penyimpanan data arsip elektronik dilaksanakan oleh ANRI maupun Pusat Data Nasional Kementerian Komunikasi dan Informatika
2) Server dan storage SIKN JIKN yang dikelola oleh Pusat SIKN dan JIKN. Saat ini storage SIKN dan JIKN di ANRI sebesar 1017.3 GB, sementara di Pusat Data Nasional sebesar 3000 GB dan di Perpustakaan Nasional sebesar 556,301 GB. Artinya server arsip untuk SIKN JIKN sebesar 4.573,301 GB
3) Server dan storage arsip statis elektronik untuk menyimpan hasil reproduksi digital yang dikelola oleh Direktorat Preservasi yang disimpan di Arsip Nasional Republik Indonesia. Storage di Preservasi sebesar 1880 Terabyte.

Berdasarkan dari data tersebut, dapat disimpulkan bahwa database kearsipan masih terpisah di berbagai lokasi. Tentu saja dalam hal ini rentan sekali dalam hal keamanan. Apalagi terkait dengan standar minimal yang dibutuhkan dalam pembangunan storage untuk kearsipan.

b. Keamanan bangunan

Keamanan bangunan meliputi sistem dan teknologi yang dibangun untuk melindungi bangunan dan menjaga keamanan arsip elektronik dan peralatan yang ada di dalamnya. Bangunan memberikan lingkungan yang sesuai dalam pengelolaan arsip elektronik terutama untuk arsip yang bernilai guna permanen. Kondisi bangunan yang baik dari segi lokasi maupun peralatan dapat mencegah bahaya dan ancaman terhadap keamanan arsip elektronik termasuk berbagai macam bencana.

c. Keamanan perangkat keras

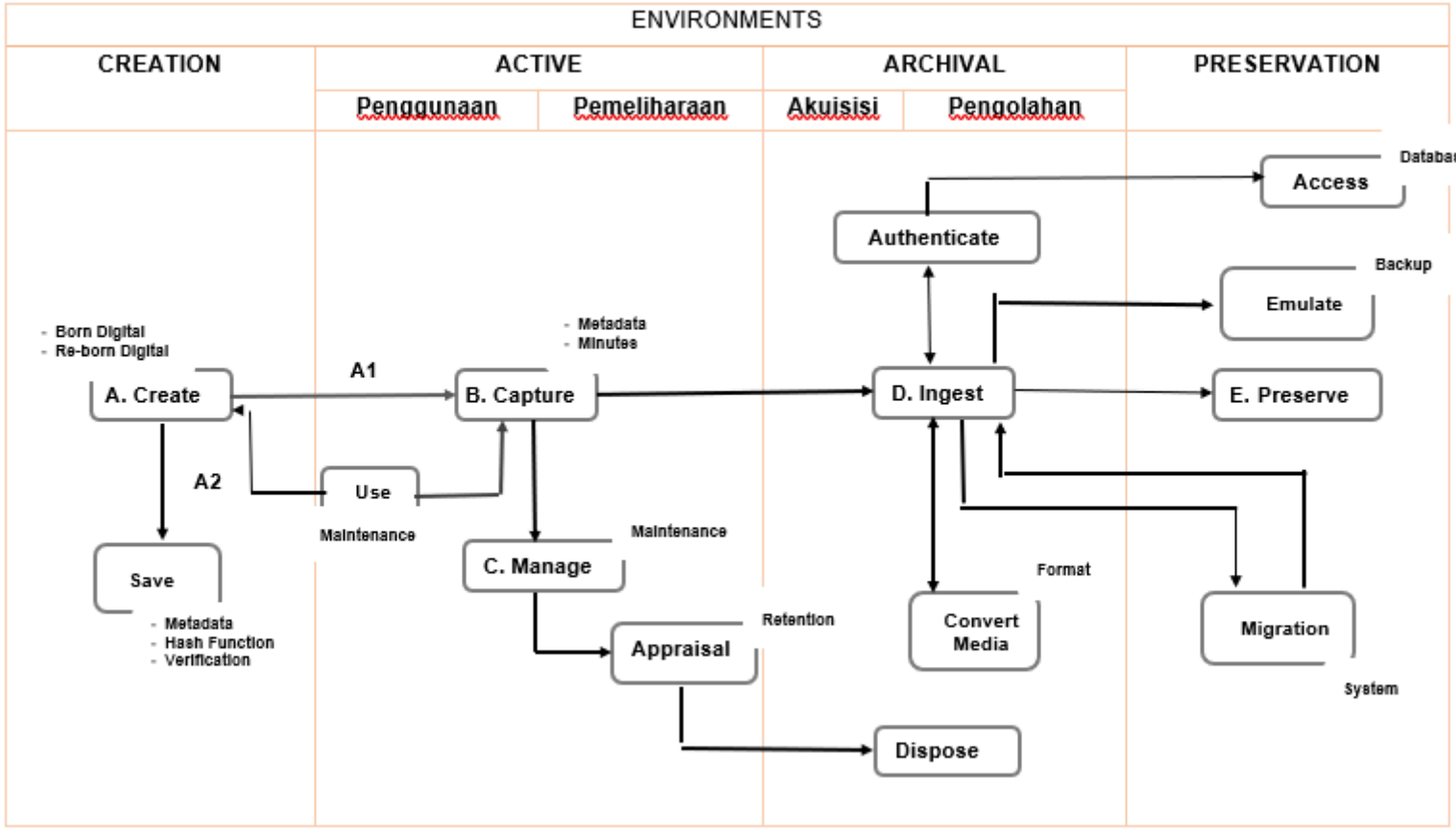
Keamanan perangkat keras adalah perlindungan perangkat fisik dari ancaman yang memfasilitasi akses tidak sah ke sistem. Ruang lingkup perangkat fisik yang dimaksud adalah keamanan perangkat laptop untuk mendukung kinerja kearsipan (utamanya SRIKANDI) dan keamanan bagi media penyimpanan

seperti hardisk eksternal atau flasdisk. Setidaknya ada beberapa hal yang menjadi ancaman bagi keamanan perangkat keras diantaranya :

1) Perangkat keras teregistrasi. Pada aplikasi SRIKANDI contohnya, laptop yang menjadi peralatan untuk kerja menjadi tanggung jawab masing masing personal. Sehingga perlu untuk meregistrasi setiap perangkat keras yang ada agar ketika terjadi penyalahgunaan dapat diketahui asalnya.
2) Tidak update antivirus secara berkala. Update antivirus pada perangkat kerja seperti laptop dan server sangat dibutuhkan dan harus dilaksanakan secara berkala. Hal tersebut karena virus pada konteks elektronik dengan cepat bermutasi dan adakalanya sulit untuk terdeteksi. Oleh karena itu pemasangan dan update antivirus diperlukan untuk melindungi data yang tersimpan baik dalam laptop maupun server.
3) Alamat protokol (IP-protokol) yang berbahaya. Seringkali alamat IP yang ada dalam penggunaan internet (jaringan) tidak memenuhi standar enskripsi protokol yang sesuai. Enskripsi sangat dibutuhkan untuk keamanan media yang tersambung ke jaringan. Informasi yang tidak dienskripsi dengan baik dapat diserang apabila dikoneksikan ke jaringan dan data dapat diakses bahkan dicuri oleh pihak yang tidak berhak
4) Akses lokal yang tidak aman. Perlu adanya pengamanan terhadap jaringan lokal agar tidak mudah terserang oleh pihak yang tidak berhak.
5) Kerentanan password. Pasword pada perangkat yang digunakan oleh personal seringkali tidak ditunjang dengan sistem keamanan yang kuat. Penggunaan default password memungkinkan akses oleh pihak yang tidak berhak.

Sementara, keamanan informasi berdasar pada prinsip kerahasiaan, keutuhan, keautentikan, dan ketersediaan informasi. Keamanan informasi sangat terkait dengan proses yang dilaksanakan dalam pengelolaan kearsipan sebagai berikut:

IDENTIFIKASI RISIKO ARSIP ELEKTRONIK



Sumber: data yang diolah (*Bearman, David. Moment of Risk: Identifying Threats to Electronic Records*)