ARSIP NASIONAL REPUBLIK INDONESIA

Jalan Ampera Raya No. 7, Jakarta Selatan 12560, Indonesia Telp. 62 21 7805851, Fax. 62 21 7810280
http://www.anri.go.id, e-mail: info@anri.go.id

PERATURAN KEPALA ARSIP NASIONAL REPUBLIK INDONESIA

NOMOR 17 TAHUN 2011

TENTANG

PEDOMAN PEMBUATAN SISTEM KLASIFIKASI

KEAMANAN DAN AKSES ARSIP DINAMIS

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA ARSIP NASIONAL REPUBLIK INDONESIA,

Menimbang :

a. bahwa dalam rangka mendukung pengelolaan arsip dinamis yang efektif dan efisien sebagaimana diamanatkan Pasal 40 ayat (4) Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan serta untuk mencegah terjadinya penyalahgunaan arsip oleh pihak-pihak yang tidak berhak, perlu diatur dalam suatu pedoman;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Kepala Arsip Nasional Republik Indonesia tentang Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis;

Mengingat :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843);
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
4. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071);
5. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 94, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
6. Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen sebagaimana telah enam kali diubah terakhir dengan Peraturan Presiden Nomor 64 Tahun 2005;
7. Keputusan Presiden Nomor 27/M Tahun 2010 tentang Pengangkatan Kepala Arsip Nasional Republik Indonesia;
8. Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 03 Tahun 2006 tentang Organisasi dan Tata Kerja Arsip Nasional Republik Indonesia sebagaimana telah dua kali diubah terakhir dengan Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 05 Tahun 2010;
7. Peraturan Komisi Informasi Nomor 1 Tahun 2010 tentang Standar Layanan Informasi Publik;

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA ARSIP NASIONAL REPUBLIK INDONESIA TENTANG PEDOMAN PEMBUATAN SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS.

Pasal 1

Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis adalah sebagaimana tercantum dalam Lampiran Peraturan ini dan merupakan bagian yang tidak terpisahkan dari Peraturan ini.

Pasal 2

Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis sebagaimana dimaksud dalam Pasal 1 diberlakukan bagi pencipta arsip sebagai panduan dalam melakukan pembuatan klasifikasi keamanan dan penentuan hak akses arsip dinamis, serta pembuatan daftar arsip dinamis berdasarkan klasifikasi keamanan dan akses arsip dinamis.

Pasal 3

Peraturan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 20 Desember 2011

KEPALA ARSIP NASIONAL REPUBLIK INDONESIA,

ttd

M. ASICHIN

LAMPIRAN
PERATURAN KEPALA ARSIP NASIONAL REPUBLIK INDONESIA
NOMOR 17 TAHUN 2011
TENTANG
PEDOMAN PEMBUATAN SISTEM KLASIFIKASI KEAMANAN
DAN AKSES ARSIP DINAMIS

BAB I
PENDAHULUAN

A. Latar Belakang

Sebagaimana amanat Pasal 40 Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, pengelolaan arsip dinamis dilaksanakan untuk menjamin ketersediaan arsip dalam penyelenggaraan kegiatan sebagai bahan akuntabilitas kinerja dan alat bukti yang sah berdasarkan suatu sistem yang memenuhi persyaratan andal, sistematis, utuh, menyeluruh dan sesuai norma, standar, prosedur dan kriteria (NSPK). Ketersediaan arsip digunakan untuk kegiatan operasional manajemen pencipta arsip dan layanan publik. Untuk itu diperlukan adanya sistem klasifikasi keamanan dan akses arsip dinamis.

Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis disusun sebagai dasar untuk melindungi hak dan kewajiban pencipta arsip dan publik terhadap akses arsip. Dalam era keterbukaan seperti saat ini, arsip dinamis pada prinsipnya terbuka dan dapat diakses oleh publik, kecuali yang dinyatakan tertutup, sebagaimana diatur pada Pasal 42 ayat (1) Undang-Undang Nomor 43 Tahun 2009 bahwa “pencipta arsip wajib menyediakan arsip dinamis bagi pengguna arsip yang berhak”. Arsip dinamis sebagai salah satu sumber informasi publik adalah bersifat terbuka dan dapat diakses oleh publik sesuai Pasal 2 ayat (1) Undang-Undang Nomor 14 Tahun 2008 bahwa “setiap informasi publik bersifat terbuka dan dapat diakses oleh setiap pengguna informasi publik”. Hal ini sejalan dengan konsideran menimbang Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, yang menguraikan bahwa informasi merupakan kebutuhan pokok dan hak asasi manusia, merupakan salah satu ciri penting negara demokratis, dan sekaligus merupakan sarana dalam

mengoptimalkan pengawasan publik terhadap penyelenggaraan negara dan badan publik.

Sebagai salah satu sumber informasi, arsip harus mudah diakses oleh publik, namun untuk pertimbangan keamanan dan melindungi fisik arsip maka perlu diatur ketentuan tentang pengamanan dan akses arsip dinamis. Pengaturan pengamanan dan akses tersebut untuk menjamin pengakuan serta kehormatan atas hak dan mengatur kebebasan orang lain dalam rangka untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan negara dan ketertiban umum dalam kehidupan masyarakat yang demokratis.

Mengingat pentingnya klasifikasi keamanan dan akses terhadap arsip dinamis, maka Arsip Nasional Republik Indonesia (ANRI) menyusun pedoman pembuatan sistem klasifikasi keamanan dan akses arsip dinamis yang dapat dipergunakan sebagai pedoman bagi pencipta arsip, dalam mengelola arsip dinamis sesuai kaidah kearsipan dan ketentuan Peraturan Perundang-undangan yang berlaku.

B. Maksud dan Tujuan

Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis dimaksudkan untuk memberikan panduan bagi pencipta arsip dalam membuat klasifikasi keamanan dan akses arsip dinamis, dengan tujuan:

1. Melindungi fisik dan informasi arsip dinamis dari kerusakan dan kehilangan sehingga kebutuhan akan ketersediaan, keterbacaan, keutuhan, integritas, otentisitas dan reliabilitas arsip tetap dapat terpenuhi;
2. Mengatur akses arsip dinamis yang sesuai ketentuan peraturan perundang-undangan sehingga dapat dicegah terjadinya penyalahgunaan arsip oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah.

C. Ruang Lingkup

Ruang lingkup Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis memuat ketentuan sebagai berikut:

1. Ketentuan Umum;
2. Tata Cara Pembuatan Klasifikasi Keamanan dan Penentuan Hak Akses Arsip Dinamis;
3. Tata Cara Pembuatan Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis.

D. Pengertian

1. Klasifikasi Keamanan Arsip Dinamis adalah pengkategorian/ penggolongan arsip dinamis berdasarkan pada tingkat keseriusan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik dan perorangan.
2. Klasifikasi Akses Arsip Dinamis adalah pengkategorian pengaturan ketersediaan arsip dinamis sebagai hasil dari kewenangan hukum dan otoritas legal pencipta arsip untuk mempermudah pemanfaatan arsip.
3. Pengamanan Arsip Dinamis adalah program perlindungan terhadap fisik dan informasi arsip dinamis berdasarkan klasifikasi keamanan yang ditetapkan sebelumnya.
4. 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.
5. Arsip Dinamis adalah arsip yang digunakan secara langsung dalam kegiatan pencipta arsip dan disimpan selama jangka waktu tertentu.
6. Publik adalah warganegara atau badan hukum yang mengajukan permohonan untuk mengakses arsip dinamis.

7. Pencipta Arsip adalah pihak yang mempunyai kemandirian dan otoritas dalam pelaksanaan fungsi, tugas, dan tanggung jawab di bidang pengelolaan arsip dinamis.
8. Sangat Rahasia adalah klasifikasi informasi dari arsip yang memiliki informasi yang apabila diketahui oleh pihak yang tidak berhak dapat membahayakan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan/atau keselamatan bangsa.
9. Rahasia adalah klasifikasi informasi dari arsip yang apabila diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya fungsi penyelenggaraan negara, sumber daya nasional dan/atau ketertiban umum.
10. Terbatas adalah klasifikasi informasi dari arsip yang memiliki informasi yang apabila diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya pelaksanaan tugas dan fungsi lembaga pemerintahan.
11. Biasa/Terbuka adalah klasifikasi informasi dari arsip yang memiliki informasi yang apabila diketahui oleh publik tidak merugikan siapapun.
12. Tingkat klasifikasi keamanan arsip dinamis adalah pengelompokkan arsip dalam tingkatan tertentu berdasarkan dampak yang ditimbulkan apabila informasi yang terdapat di dalamnya diketahui oleh pihak yang tidak berhak.

BAB II
KETENTUAN UMUM

A. Kebijakan Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis

Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis harus ditetapkan oleh pimpinan pencipta arsip. Pencipta Arsip yang dimaksud adalah lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan.

B. Prinsip Dasar Klasifikasi Keamanan Arsip Dinamis

Prinsip dasar dalam penetapan klasifikasi keamanan arsip dinamis adalah:

1. Memperhatikan tingkat keseriusan dampak yang timbul apabila informasi yang terdapat dalam arsip dinamis disalahgunakan oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah;
2. Pengklasifikasian keamanan arsip dinamis harus dituangkan dalam suatu ketetapan pimpinan berupa pernyataan tertulis yang disertai alasan sebagai dasar pertimbangan dalam menentukan tingkat klasifikasi.

C. Prinsip Dasar Akses Arsip Dinamis

Prinsip dasar dalam penetapan hak akses arsip dinamis adalah:

1. Pengaksesan arsip dinamis hanya dapat dilakukan oleh pejabat dan staf yang mempunyai kewenangan untuk akses;
2. Pejabat yang lebih tinggi kedudukannya dapat mengakses arsip yang dibuat oleh pejabat atau staf di bawahnya sesuai dengan hierarki kewenangannya dalam struktur organisasi; dan
3. Pejabat atau staf yang lebih rendah kedudukannya tidak dapat mengakses arsip yang dibuat oleh pejabat di atasnya kecuali sebelumnya telah diberikan izin oleh pejabat yang berwenang.

BAB III
TATA CARA PEMBUATAN KLASIFIKASI KEAMANAN DAN PENENTUAN HAK AKSES ARSIP

Kegiatan membuat klasifikasi keamanan dan menentukan hak akses arsip dinamis berada pada lingkup penciptaan dan penggunaan arsip yang dalam penyusunannya harus memperhatikan langkah-langkah sebagai berikut: identifikasi ketentuan hukum, analisis fungsi unit kerja dalam organisasi, analisis *job description* serta analisis risiko, sehingga dapat ditentukan kategori klasifikasi keamanan dan hak akses arsip dinamis.

A. Identifikasi Ketentuan Hukum

Dalam identifikasi ketentuan hukum yang menjadi pedoman utama adalah:

1. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan;
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
4. Peraturan perundang-undangan sektor pencipta arsip yang terkait dengan klasifikasi keamanan dan akses arsip dinamis.

Identifikasi ketentuan hukum yang dapat dipergunakan sebagai dasar penentuan klasifikasi keamanan dan akses arsip dinamis, seperti yang terdapat dalam pasal-pasal sebagai berikut:

1. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan

   Pasal 44 ayat (1):
   "Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila arsip dibuka untuk umum dapat:
   a. menghambat proses penegakan hukum;
   b. mengganggu kepentingan pelindungan hak atas kekayaan intelektual dan pelindungan dari persaingan usaha tidak sehat;
   c. membahayakan pertahanan dan keamanan negara;

d. mengungkapkan kekayaan alam Indonesia yang masuk dalam kategori dilindungi kerahasiaannya;
e. merugikan ketahanan ekonomi nasional;
f. merugikan kepentingan politik luar negeri dan hubungan luar negeri;
g. mengungkapkan isi akta autentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang kecuali kepada yang berhak secara hukum;
h. mengungkapkan rahasia atau data pribadi; dan
i. mengungkap memorandum atau surat-surat yang menurut sifatnya perlu dirahasiakan."

Pasal 44 ayat (2):
"Pencipta arsip wajib menjaga kerahasiaan arsip tertutup sebagaimana dimaksud pada ayat (1)".

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Pasal 17:
"Setiap badan publik wajib membuka akses bagi setiap Pemohon Informasi Publik untuk mendapatkan Informasi Publik", kecuali:
a. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat menghambat proses penegakan hukum, yaitu informasi yang dapat:
   1) Menghambat proses penyelidikan dan penyidikan suatu tindak pidana;
   2) Mengungkapkan identitas informan, pelapor, saksi, dan/atau korban yang mengetahui adanya tindak pidana;
   3) Mengungkapkan data intelijen kriminal dan rencana-rencana yang berhubungan dengan pencegahan dan penanganan segala bentuk kejahatan transnasional;
   4) Membahayakan keselamatan dan kehidupan penegak hukum dan/atau keluarganya; dan/atau
   5) Membahayakan keamanan peralatan, sarana, dan/atau prasarana penegak hukum.

b. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat;
c. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat membahayakan pertahanan dan keamanan negara, yaitu:
   1) Informasi tentang strategi, intelijen, operasi, taktik dan teknik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara, meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi dalam kaitan dengan ancaman dari dalam dan luar negeri;
   2) Dokumen yang memuat tentang strategi, intelijen, operasi, teknik dan taktik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara yang meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi;
   3) Jumlah, komposisi, disposisi, atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya;
   4) Gambar, peta, dan data tentang situasi dan keadaan pangkalan dan/atau instalasi militer;
   5) Data perkiraan kemampuan militer dan pertahanan negara lain terbatas pada segala tindakan dan/atau indikasi negara tersebut yang dapat membahayakan kedaulatan Negara Kesatuan Republik Indonesia dan/ atau data terkait kerjasama militer dengan negara lain yang disepakati dalam perjanjian tersebut sebagai rahasia atau sangat rahasia;
   6) Sistem persandian negara; dan/atau
   7) Sistem intelijen negara.
d. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkapkan kekayaan alam Indonesia;
e. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik, dapat merugikan ketahanan ekonomi nasional:

1) Rencana awal pembelian dan penjualan mata uang nasional atau asing, saham dan aset vital milik negara;
2) Rencana awal perubahan nilai tukar, suku bunga, dan model operasi institusi keuangan;
3) Rencana awal perubahan suku bunga bank, pinjaman pemerintah, perubahan pajak, tarif, atau pendapatan negara/daerah lainnya;
4) Rencana awal penjualan atau pembelian tanah atau properti;
5) Rencana awal investasi asing;
6) Proses dan hasil pengawasan perbankan, asuransi, atau lembaga keuangan lainnya; dan/atau
7) Hal-hal yang berkaitan dengan proses pencetakan uang.

f. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik, dapat merugikan kepentingan hubungan luar negeri:
   1) Posisi, daya tawar dan strategi yang akan dan telah diambil oleh negara dalam hubungannya dengan negosiasi internasional;
   2) Korespondensi diplomatik antarnegara;
   3) Sistem komunikasi dan persandian yang dipergunakan dalam menjalankan hubungan internasional; dan/atau
   4) Perlindungan dan pengamanan infrastruktur strategis Indonesia di luar negeri.
g. Informasi Publik yang apabila dibuka dapat mengungkapkan isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang.
h. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkap rahasia pribadi, yaitu:
   1) Riwayat dan kondisi anggota keluarga;
   2) Riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang;
   3) Kondisi keuangan, aset, pendapatan, dan rekening bank seseorang;

4) Hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan seseorang; dan/atau
5) Catatan yang menyangkut pribadi seseorang yang berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan nonformal.

i. Memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang menurut sifatnya dirahasiakan kecuali atas putusan Komisi Informasi atau pengadilan.
j. Informasi yang tidak boleh diungkapkan berdasarkan undang-undang.

3. Pasal 27, Pasal 29, Pasal 30, Pasal 31, Pasal 32, Pasal 35, Pasal 36, dan Pasal 37 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Pasal 27:

(1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.
(2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian.
(3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
(4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 29:

"Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi."

Pasal 30:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.
(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau

institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau dokumen elektronik milik orang lain atau milik publik.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 35

“Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.”

Pasal 36

‘Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain.”

Pasal 37

"Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi Indonesia."

4. Pasal 3 ayat (4) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

   Pasal 3 ayat (4)

   "Menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi"

5. Pasal 7, Pasal 8, Pasal 168, Pasal 169, Pasal 189 ayat (2) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan

   Pasal 7

   "Setiap orang berhak untuk mendapatkan informasi dan edukasi tentang kesehatan yang seimbang dan bertanggung jawab."

   Pasal 8

   "Setiap orang berhak memperoleh informasi tentang data kesehatan dirinya termasuk tindakan dan pengobatan yang telah maupun yang akan diterimanya dari tenaga kesehatan."

   Pasal 168

   (1) Untuk menyelenggarakan upaya kesehatan yang efektif dan efisien diperlukan informasi kesehatan.
   (2) Informasi kesehatan sebagaimana dimaksud pada ayat (1) dilakukan melalui sistem informasi dan melalui lintas sektor.
   (3) Ketentuan lebih lanjut mengenai sistem informasi sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

   Pasal 169

   "Pemerintah memberikan kemudahan kepada masyarakat untuk memperoleh akses terhadap informasi kesehatan dalam upaya meningkatkan derajat kesehatan masyarakat."

Pasal 189 ayat (2):

(2) Penyidik sebagaimana dimaksud pada ayat (1) berwenang:

a. melakukan pemeriksaan atas kebenaran laporan serta keterangan tentang tindak pidana di bidang kesehatan;
b. melakukan pemeriksaan terhadap orang yang diduga melakukan tindak pidana di bidang kesehatan;
c. meminta keterangan dan bahan bukti dari orang atau badan hukum sehubungan dengan tindak pidana di bidang kesehatan;
d. melakukan pemeriksaan atas surat dan/atau dokumen lain tentang tindak pidana di bidang kesehatan;
e. melakukan pemeriksaan atau penyitaan bahan atau barang bukti dalam perkara tindak pidana di bidang kesehatan;
f. meminta bantuan ahli dalam rangka pelaksanaan tugas penyidikan tindak pidana di bidang kesehatan;
g. menghentikan penyidikan apabila tidak terdapat cukup bukti yang membuktikan adanya tindak pidana di bidang kesehatan.

6. Pasal 18, Pasal 20, Pasal 40, Pasal 41, Pasal 42, dan Pasal 43 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Pasal 18:

(1) Penyelenggara jasa telekomunikasi wajib mencatat/ merekam secara rinci pemakaian jasa telekomunikasi yang digunakan oleh pengguna telekomunikasi.
(2) Apabila pengguna memerlukan catatan/rekaman pemakaian jasa telekomunikasi sebagaimana dimaksud pada ayat (1), penyelenggara telekomunikasi wajib memberikannya.
(3) Ketentuan mengenai pencatatan/perekaman pemakaian jasa telekomunikasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 20:

“Setiap penyelenggara telekomunikasi wajib memberikan prioritas pengiriman, penyaluran, dan penyampaian informasi penting menyangkut:

a. Keamanan negara;

b. Keselamatan jiwa manusia dan harta benda;
c. Bencana alam;
d. Marabahaya, dan atau
e. Wabah penyakit.

Pasal 40:

“Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.”

Pasal 41:

“Dalam rangka pembuktian kebenaran pemakaian fasilitas telekomunikasi atas permintaan pengguna jasa telekomunikasi, penyelenggara jasa telekomunikasi wajib melakukan kegiatan perekaman pemakaian fasilitas telekomunikasi yang digunakan oleh pengguna jasa telekomunikasi dan dapat melakukan perekaman informasi sesuai dengan peraturan perundang-undangan yang berlaku”.

Pasal 42:

(1) Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jasa telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.
(2) Untuk keperluan proses pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi yang diperlukan atas:
    a. Permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu;
    b. Permintaan penyidik untuk tindak pidana tertentu sesuai dengan Undang-Undang yang berlaku.
(3) Ketentuan mengenai tata cara permintaan dan pemberian rekaman informasi sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 43:

“Pemberian rekaman informasi oleh penyelenggara jasa

telekomunikasi kepada pengguna jasa telekomunikasi sebagaimana dimaksud dalam Pasal 41 dan untuk kepentingan proses peradilan pidana sebagaimana dimaksud dalam Pasal 42 ayat (2), tidak merupakan pelanggaran Pasal 40".

7. Pasal 2 dan Pasal 3 Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang

   Pasal 2:
   "Lingkup perlindungan Rahasia Dagang meliputi metode produksi, metode pengolahan, metode penjualan, atau informasi lain di bidang teknologi dan/atau bisnis yang memiliki nilai ekonomi dan tidak diketahui oleh masyarakat umum".

   Pasal 3:
   a. Rahasia Dagang mendapat perlindungan apabila informasi tersebut bersifat rahasia, mempunyai nilai ekonomi, dan dijaga kerahasiaannya melalui upaya sebagaimana mestinya.
   b. Informasi dianggap bersifat rahasia apabila informasi tersebut hanya diketahui oleh pihak tertentu atau tidak diketahui secara umum oleh masyarakat.
   c. Informasi dianggap memiliki nilai ekonomi apabila sifat kerahasiaan informasi tersebut dapat digunakan untuk menjalankan kegiatan atau usaha yang bersifat komersial atau dapat meningkatkan keuntungan secara ekonomi.
   d. Informasi dianggap dijaga kerahasiaannya apabila pemilik atau para pihak yang menguasainya telah melakukan langkah-langkah yang layak dan patut.

B. Analisis Fungsi Unit Kerja dalam Organisasi dan *Job Description*

Setelah melakukan identifikasi terhadap ketentuan hukum yang menjadi bahan pertimbangan dalam pembuatan klasifikasi keamanan dan penentuan hak akses arsip dinamis, langkah selanjutnya adalah melakukan analisis fungsi unit kerja dalam organisasi dan analisis *job description* pada masing-masing jabatan.

1. Analisis Fungsi Unit Kerja dalam Organisasi

   Analisis fungsi dalam organisasi dilakukan terhadap unit kerja yang menjalankan fungsi baik subtantif maupun fasilitatif dengan tujuan untuk menentukan fungsi strategis dalam organisasi. Fungsi substantif atau utama adalah kelompok kegiatan utama suatu organisasi sesuai dengan urusan penyelenggaraan pemerintahan. Fungsi fasilitatif adalah kelompok kegiatan pendukung yang terdapat pada setiap organisasi misalnya sekretariat, keuangan, kepegawaian, dan lain-lain.

   Contoh arsip yang dihasilkan berdasarkan analisis fungsi substantif yang mempunyai nilai strategis bagi individu, masyarakat, organisasi, dan negara antara lain:

   a. Dalam struktur organisasi Kementerian Pertahanan terdapat Badan Sarana Pertahanan. Salah satu fungsi Badan Sarana Pertahanan adalah di bidang pengelolaan sarana pertahanan. Kegiatan yang tercipta dari fungsi pengelolaan sarana pertahanan antara lain pengadaan jasa konstruksi dan sarana pertahanan, sertifikasi kelaikan, kodefikasi materiil, dan pengelolaan aset/barang milik negara di bidang pertahanan. Untuk kegiatan jasa konstruksi dan sarana pertahanan, contoh arsip yang dihasilkan adalah ketersediaan suku cadang peralatan pertahanan dari dalam maupun luar negeri. Berdasarkan analisis fungsi, arsip dari kegiatan tersebut dapat dipertimbangkan sebagai arsip rahasia, karena kegiatan tersebut mempunyai nilai strategis bagi negara.
   b. Dalam struktur organisasi Kementerian Energi dan Sumber Daya Mineral terdapat Badan Geologi. Salah satu fungsi Badan Geologi adalah mengungkap potensi *geo-resources* (sumber daya geologi) yang terdapat di suatu wilayah di Indonesia, seperti: migas, panas bumi, mineral dan air tanah, serta potensi geologi lainnya. Dalam melaksanakan fungsi tersebut, Badan Geologi mempunyai kegiatan pemetaan terhadap potensi sumber daya geologi. Kegiatan tersebut menghasilkan arsip berupa nama, luas wilayah, jumlah penduduk wilayah tersebut beserta peta. Berdasarkan analisis fungsi, arsip dari kegiatan tersebut dapat

dipertimbangkan sebagai arsip rahasia, karena kegiatan tersebut mempunyai nilai strategis bagi negara.

c. Salah satu unit organisasi di lingkungan Kementerian Komunikasi dan Informatika adalah Direktorat Jenderal Aplikasi Informatika. Salah satu fungsi Direktorat Jenderal Aplikasi Informatika adalah menjaga keamanan informasi. Arsip yang dihasilkan dari fungsi tersebut antara lain arsip yang berhubungan dengan daftar situs di internet terkait dengan jaringan teroris di Solo yang harus diblokir sehingga arsip yang tercipta dari fungsi tersebut dapat dipertimbangkan sebagai arsip rahasia, karena kegiatan tersebut terkait dengan keamanan nasional.

Analisis Fungsi dari unit kerja dalam organisasi dapat digambarkan dalam bagan sebagai berikut:

Tabel 1. Contoh Analisis Fungsi Unit Kerja Dalam Organisasi

No.	Unit Kerja	Fungsi	Kegiatan	Arsip Tercipta	Keterangan
1.	Badan Sarana Pertahanan, Kementerian Pertahanan	Melaksanakan pengelolaan sarana pertahanan	1. Pengadaan jasa konstruksi & sarana pertahanan 2. Sertifikasi kelaikan 3. Kodefikasi Materiil 4. Pengelolaan aset/barang milik negara di bidang pertahanan	Arsip tentang ketersediaan suku cadang peralatan pertahanan	Dipertimbangkan rahasia
2.	Badan Geologi, Kementerian Energi dan Sumber Daya Mineral	Mengungkap potensi *geo-resources* (sumber daya geologi) yang terdapat di suatu wilayah di Indonesia	1. Pemetaan migas 2. Pemetaan panas bumi 3. Pemetaan mineral 4. Pemetaan air tanah	Arsip tentang nama, luas, jumlah penduduk beserta peta wilayah tersebut	Dipertimbangkan rahasia
3.	Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika	Menjaga keamanan informasi	Memblokir situs yang mengandung SARA, Porno, dan yang dapat mengganggu keamanan negara	Arsip yang berhubungan dengan daftar situs di internet yang terkait dengan jaringan teroris di Solo yang harus diblokir	Dipertimbangkan rahasia

Contoh arsip berdasarkan fungsi fasilitatif yang mempunyai nilai strategis bagi individu, masyarakat, organisasi, dan negara antara lain:

a. Unit kepegawaian, dalam rangka melaksanakan fungsi pembinaan pegawai, unit kepegawaian melaksanakan kegiatan penyusunan *personal file* diantaranya meliputi disiplin pegawai, DP3, dan lain-lain. Arsip yang tercipta dari kegiatan ini dapat dipertimbangkan sebagai arsip rahasia karena mempunyai nilai bagi individu pegawai yang bersangkutan dan dapat menimbulkan kerugian yang serius terhadap masalah *privacy*.
b. Unit keuangan, dalam rangka melaksanakan salah satu fungsi yaitu pengelolaan perbendaharaan, diantaranya melakukan kegiatan administrasi pembayaran gaji. Arsip yang dihasilkan diantaranya adalah daftar gaji, daftar potongan gaji pegawai, dan lain-lain yang dapat dipertimbangkan arsip rahasia karena mempunyai nilai bagi individu pegawai dan dapat menimbulkan kerugian yang serius terhadap masalah *privacy*.

2. Uraian Jabatan *(Job Description)*

Selain analisis fungsi unit organisasi, perlu didukung adanya analisis sumber daya manusia sebagai penanggung jawab dan pengelola melalui analisis *job description*. *Job description* (uraian jabatan) adalah suatu catatan yang sistematis tentang tugas dan tanggung jawab suatu jabatan tertentu, yang diuraikan berdasarkan fungsi sebagaimana yang tercantum dalam struktur organisasi.

Uraian Jabatan berbentuk dokumen formal yang berisi ringkasan tentang suatu jabatan untuk membedakan jabatan yang satu dengan jabatan yang lain dalam suatu organisasi. Uraian jabatan disusun dalam suatu format yang terstruktur sehingga informasi mudah dipahami oleh setiap pihak yang berkaitan di dalam organisasi. Pada hakikatnya, uraian jabatan merupakan hal yang penting dalam pengelolaan sumber daya manusia dalam suatu organisasi, dimana suatu jabatan dijelaskan dan diberikan batasan.

Hal-hal yang harus diperhatikan dalam Uraian Jabatan meliputi:

a. Identifikasi Jabatan, berisi informasi tentang nama jabatan dan bagian dalam suatu organisasi;

b. Fungsi Jabatan berisi penjelasan tentang kegiatan yang dilaksanakan berdasarkan struktur organisasi;
c. Tugas-tugas yang harus dilaksanakan, bagian ini merupakan inti dari uraian jabatan; dan
d. Pengawasan yang harus dilakukan dan yang diterima.

Penyusunan uraian jabatan harus dilakukan dengan baik agar mudah dimengerti, untuk itu diperlukan suatu proses terstruktur, yang dikenal dengan nama analisis jabatan.

Analisis jabatan adalah proses untuk memahami suatu jabatan dan kemudian menuangkannya ke dalam format agar orang lain mengerti tentang suatu jabatan. Prinsip penting yang harus dianut dalam melakukan analisis jabatan, yaitu:

a. Analisis dilakukan untuk memahami tanggung jawab setiap jabatan dan kontribusi jabatan terhadap pencapaian hasil atau tujuan organisasi. Dengan analisis ini, maka uraian jabatan akan menjadi daftar tanggung jawab.
b. Yang dianalisis adalah jabatan, bukan pemegang jabatan.
c. Kondisi jabatan yang dianalisis dan dituangkan dalam uraian jabatan adalah kondisi jabatan pada saat dianalisis berdasarkan rancangan strategi dan struktur organisasi.

Dari analisis jabatan, dapat dilihat pejabat yang mempunyai wewenang dan tanggung jawab terhadap tingkat/derajat klasifikasi keamanan dan mempunyai hak akses arsip dinamis. Untuk itu, dapat digolongkan personil tertentu yang diberi wewenang dan tanggung jawab dalam pembuatan, penanganan, pengelolaan keamanan informasi dan diberi hak akses arsip dinamis. Penggolongan personil untuk menjamin perlindungan pengamanan informasi dan mempunyai hak akses arsip dinamis terdiri dari penentu kebijakan, pelaksana, dan pengawas. Tanggung jawab tersebut, dapat diuraikan sebagai berikut:

a. Penentu kebijakan
    1) Menentukan tingkat/derajat klasifikasi keamanan dan hak akses arsip dinamis;
    2) Memberikan pertimbangan atau alasan secara tertulis mengenai pengklasifikasian keamanan dan penentuan hak akses arsip dinamis;

3) Menentukan sumber daya manusia yang bertanggung jawab dan mempunyai kewenangan dalam mengamankan informasi dalam arsip dinamis yang telah diklasifikasikan keamanannya; dan
4) Menuangkan kebijakan, dasar pertimbangan, dan sumber daya manusia yang bertanggung jawab dalam suatu pedoman, petunjuk pelaksanaan, atau petunjuk teknis.

b. Pelaksana kebijakan
1) Memahami dan menerapkan klasifikasi keamanan dan hak akses arsip dinamis sesuai dengan kewenangan yang sudah ditetapkan;
2) Melaksanakan pengelolaan arsip sesuai dengan tingkat klasifikasi keamanan dan hak akses arsip dinamis sesuai dengan kewenangan yang telah ditentukan;
3) Merekam semua pelanggaran yang ditemukan;
4) Melaporkan semua tindakan penyimpangan dan pelanggaran;
5) Menjamin bahwa implementasi tingkat klasifikasi keamanan dan hak akses arsip dinamis telah dikoordinasikan dengan pejabat yang terkait secara tepat;
6) Menjamin informasi yang berada dalam kendali pejabat yang mempunyai wewenang dan tanggung jawab terhadap tingkat klasifikasi keamanan dan mempunyai hak akses arsip dinamis telah dilindungi dari kerusakan fisik dan dari akses, perubahan, serta pemindahan ilegal berdasarkan standar keamanan;
7) Mengidentifikasi semua kebutuhan dalam rangka menjamin keamanan informasi dan hak akses arsip dinamis yang terdapat dalam arsip yang telah diklasifikasikan keamanannya.

c. Pengawas
1) Menindaklanjuti pelanggaran dan penyimpangan yang ditemukan; dan
2) Melaporkan semua dugaan pelanggaran dan penyimpangan kepada penentu kebijakan.

Contoh penggolongan personil dalam suatu organisasi untuk menjamin perlindungan keamanan informasi dan hak akses arsip dinamis adalah:

a. Penentu kebijakan adalah pejabat yang mempunyai fungsi, tugas, tanggung jawab, dan kewenangan kedinasan ke luar dan ke dalam instansi seperti: Pimpinan tertinggi sampai dengan eselon 2 pada instansi pemerintah pusat dan pemerintah daerah atau eselon 3 pada instansi setingkat Balai/UPT/Kantor;
b. Pelaksana kebijakan adalah pejabat pada unit kerja yang melaksanakan fungsi dan tugas organisasi setingkat eselon 3 dan 4, seperti: Kepala Bidang/Kepala Bagian/Kepala Sub Direktorat, Kepala Sub Bidang/Kepala Sub Bagian/Kepala Seksi pada pusat/direktorat/biro;
c. Pengawas adalah pejabat yang mempunyai fungsi dan tugas pengawasan, seperti: inspektur/auditor pada inspektorat, pengawas intern pada Satuan Pengawas Intern (SPI).

3. Analisis Risiko

Setelah dilakukan analisis fungsi unit kerja dalam organisasi dan *job description,* kemudian dilakukan analisis risiko. Analisis risiko dipergunakan untuk memberikan pertimbangan terhadap pengklasifikasian keamanan dan hak akses arsip dinamis karena apabila diketahui oleh orang yang tidak berhak, kerugian yang dihadapi jauh lebih besar daripada manfaatnya. Risiko tersebut dapat berdampak terhadap keamanan individu, masyarakat, organisasi, dan negara.

Contoh: analisis risiko

a. Arsip yang berhubungan dengan ketersediaan peralatan pertahanan, seperti misalnya pembelian pesawat tempur dari luar negeri dan pembelian senjata. Setelah dilakukan analisis risiko, hasil analisis menyimpulkan:
   1) Jika arsip tentang pembelian pesawat perang dan senjata tersebut dibuka, maka risiko yang dapat timbul antara lain membahayakan potensi pertahanan negara.
   2) Jika arsip ditutup, maka kemungkinan risiko yang dapat timbul tidak ada sehingga lebih baik dikategorikan rahasia atau sangat rahasia.

   Berdasarkan analisis risiko tersebut, kewenangan hak akses arsip dinamis hanya terdapat pada penentu kebijakan sesuai dengan kewenangannya.

b. Arsip yang berhubungan dengan potensi wilayah. Setelah dilakukan analisis risiko, hasil analisis menyimpulkan:
   1) Bila arsip diketahui publik, maka akan menimbulkan dampak pengeksploitasian potensi kekayaan negara oleh pihak yang tidak bertanggung jawab.
   2) Bila arsip ditutup kemungkinan risiko yang dapat timbul tidak ada sehingga lebih baik dikategorikan rahasia atau sangat rahasia.

   Berdasarkan analisis risiko tersebut, kewenangan hak akses arsip dinamis hanya terdapat pada penentu kebijakan.

c. Arsip rencana tata kota.
   1) Bila arsip dirahasiakan, maka kemungkinan risiko yang akan timbul adalah disalahgunakan oleh pejabat yang berwenang karena tidak ada kontrol dari masyarakat.
   2) Bila arsip diketahui oleh publik maka akan ada kontrol dan koreksi, sehingga lebih baik dikategorikan sebagai arsip biasa dan dapat diakses oleh masyarakat.

4. Penentuan Kategori Klasifikasi Keamanan

Berdasarkan identifikasi ketentuan hukum, analisis fungsi unit kerja dalam organisasi dan *job description* serta analisis risiko, dapat ditentukan kategori klasifikasi keamanan, yaitu:

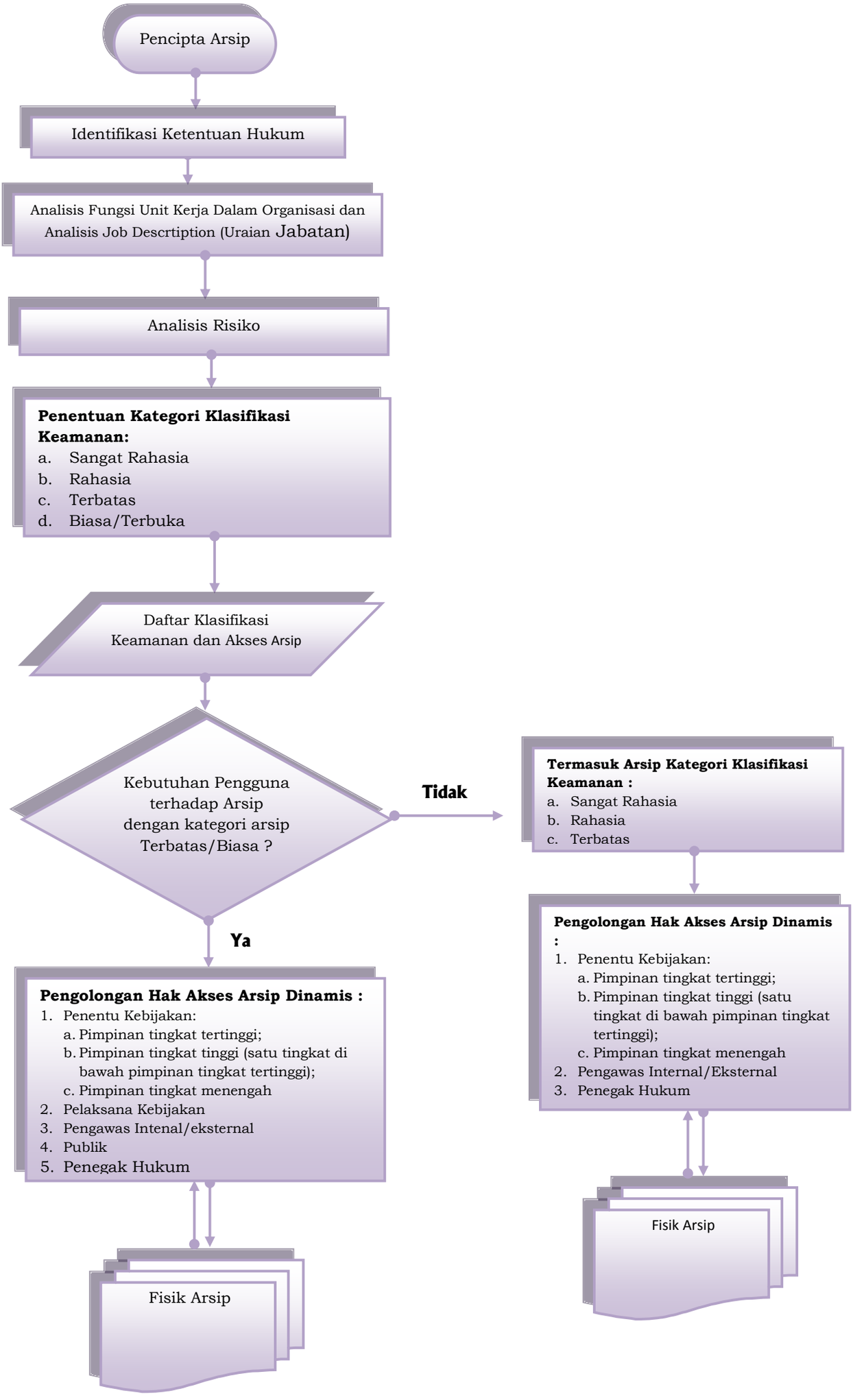
a. Sangat Rahasia apabila diketahui oleh pihak yang tidak berhak dapat membahayakan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan bangsa;
b. Rahasia apabila diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya fungsi penyelenggaraan negara, sumber daya nasional, ketertiban umum, termasuk dampak ekonomi makro. Apabila informasi yang terdapat dalam arsip bersifat sensitif bagi lembaga/organisasi akan menimbulkan kerugian yang serius terhadap *privacy*, keuntungan kompetitif, hilangnya kepercayaan, serta merusak kemitraan dan reputasi;
c. Terbatas apabila diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya pelaksanaan fungsi dan tugas lembaga pemerintahan, seperti kerugian finansial yang signifikan;

d. Biasa/Terbuka apabila dibuka untuk umum tidak membawa dampak apapun terhadap keamanan negara.

Penentuan keempat tingkat klasifikasi keamanan tersebut disesuaikan dengan kepentingan dan kondisi setiap lembaga. Di suatu lembaga, dimungkinkan untuk membuat sekurang-kurangnya 2 (dua) tingkat/derajat klasifikasi keamanan arsip dinamis. Setelah dibuat tingkat kategori klasifikasi keamanan arsip, selanjutnya dapat dituangkan dalam Daftar Arsip Dinamis berdasarkan klasifikasi keamanan dengan memperhatikan item-item sebagaimana diatur dalam BAB IV.

Prosedur penyusunan Klasifikasi Keamanan dan Hak Akses Arsip Dinamis, dapat digambarkan dengan bagan alur sebagai berikut:

ARSIP NASIONAL REPUBLIK INDONESIA



5. Penggolongan Hak Akses Arsip Dinamis

Berdasarkan identifikasi ketentuan hukum, analisis fungsi unit kerja dalam organisasi, analisis *job description*, analisis risiko, dan penentuan kategori klasifikasi keamanan, dapat ditentukan penggolongan pengguna yang berhak mengakses terhadap arsip dinamis, yaitu:

a. Pengguna yang berhak di lingkungan internal instansi

1) Penentu Kebijakan mempunyai kewenangan untuk mengakses seluruh arsip yang berada di bawah kewenangannya, dengan ketentuan sebagai berikut:
   a) Pimpinan tingkat tertinggi mempunyai kewenangan untuk mengakses seluruh arsip yang berada di bawah kewenangannya.
   b) Pimpinan tingkat tinggi (satu tingkat di bawah pimpinan tingkat tertinggi) mempunyai kewenangan untuk mengakses seluruh arsip yang berada di bawah kewenangannya, namun tidak diberikan hak akses untuk informasi yang terdapat pada pimpinan tingkat tertinggi dan yang satu tingkat dengan unit di luar unit kerjanya, kecuali telah mendapatkan izin.
   c) Pimpinan tingkat menengah (satu tingkat di bawah pimpinan tingkat tinggi) mempunyai kewenangan untuk mengakses seluruh arsip yang berada di bawah kewenangannya, namun tidak diberikan hak akses untuk informasi yang terdapat pada pimpinan tingkat tertinggi, pimpinan tingkat tinggi, dan yang satu tingkat dengan unit di luar unit kerjanya kecuali telah mendapatkan izin.
2) Pelaksana kebijakan mempunyai kewenangan untuk mengakses seluruh arsip yang berada di bawah kewenangannya dengan tingkat klasifikasi biasa, tetapi tidak diberikan hak akses untuk arsip dengan tingkat klasifikasi terbatas, rahasia, dan sangat rahasia yang terdapat pada pimpinan tingkat tertinggi, pimpinan tingkat tinggi, pimpinan tingkat menengah, dan yang satu tingkat di atas unit kerjanya kecuali telah mendapatkan izin.

3) Pengawas internal mempunyai kewenangan untuk mengakses seluruh arsip pada pencipta arsip dalam rangka melaksanakan fungsi pengawasan internal sesuai dengan ketentuan peraturan perundang-undangan, seperti pengawasan yang dilakukan oleh Inspektorat Jenderal/ Inspektur Utama Kementerian/Lembaga dan Satuan Pengawas Internal (SPI)

b. Pengguna yang berhak di lingkungan eksternal instansi

1) Publik mempunyai hak untuk mengakses seluruh arsip dengan kategori biasa/terbuka.
2) Pengawas eksternal mempunyai hak untuk mengakses seluruh arsip pada pencipta arsip dalam rangka melaksanakan fungsi pengawasan eksternal sesuai dengan ketentuan peraturan perundang-undangan, seperti pengawasan yang dilakukan oleh Badan Pemeriksa Keuangan (BPK) dan Badan Pengawasan Keuangan Pembangunan (BPKP)
3) Aparat penegak hukum mempunyai hak untuk mengakses arsip pada pencipta arsip yang terkait dengan perkara atau proses hukum yang sedang ditangani dalam rangka melaksanakan fungsi penegakan hukum.

Dalam rangka pelaksanaan klasifikasi keamanan dan akses arsip dinamis, pengguna yang berhak untuk mengakses arsip dinamis sebagaimana tabel berikut:

Tabel 2. Pengguna yang berhak akses arsip dinamis

No.	Tingkat Klasifikasi Keamanan dan Akses	Penentu Kebijakan	Pelaksana Kebijakan	Pengawas Internal/ Eksternal	Publik	Penegak Hukum
1.	Biasa/ Terbuka	√	√	√	√	√
2.	Terbatas	√	-	√	-	√
3.	Rahasia	√	-	√	-	√
4.	Sangat Rahasia	√	-	√	-	√

Keterangan Tabel 2:

a. Arsip Berklasifikasi Sangat Rahasia, hak akses diberikan kepada pimpinan tertinggi lembaga dan yang setingkat di bawahnya apabila sudah diberikan izin, pengawas internal/eksternal dan penegak hukum
b. Arsip Berklasifikasi Rahasia, hak akses diberikan kepada pimpinan tingkat tinggi dan setingkat di bawahnya apabila sudah diberikan izin, pengawas internal/eksternal dan penegak hukum
c. Arsip Berklasifikasi Terbatas, hak akses diberikan kepada pimpinan tingkat menengah dan setingkat di bawahnya apabila sudah diberikan izin, pengawas internal/eksternal dan penegak hukum
d. Arsip Berklasifikasi Biasa/Terbuka, hak akses diberikan kepada semua tingkat pejabat dan staf yang berkepentingan.

6. Pengamanan Tingkat Klasifikasi

Berdasarkan tingkat Klasifikasi Keamanan dan Akses Arsip Dinamis, maka pencipta arsip mengacu ketentuan peraturan perundang-undangan melaksanakan pengamanan fisik arsip dinamis maupun informasinya sesuai dengan tingkat klasifikasi, antara lain dalam penyimpanan dan penyampaian sebagai berikut:

1. Penyimpanan

   Penyimpanan dalam rangka penanganan fisik maupun informasi arsip dinamis sesuai dengan tingkat klasifikasi dapat dilakukan dengan memparhatikan media arsip. Pengaturan pengguna arsip serta prasarana dan sarana sebagaimana bagan di bawah ini:

ARSIP NASIONAL REPUBLIK INDONESIA

Tabel 3. Tabel Pengamanan Arsip Dinamis Sesuai Dengan Tingkat Klasifikasi Keamanan

NO.	TINGKAT KLASIFIKASI KEAMANAN	MEDIA ARSIP					
		ARSIP KONVENSIONAL			ARSIP ELEKTRONIK		
		Arsip	Pengguna	Prasarana & Sarana	Arsip	Pengguna	Prasarana & Sarana
1.	Biasa/ Terbuka	Tidak ada persyaratan dan prosedur khusus.	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus	*Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2.	Terbatas	Ada persyaratan dan prosedur dengan memberikan cap "TERBATAS" pada fisik arsip	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Diperlukan tempat penyimpanan yang aman	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Autentikasi pengguna (nama pengguna/ *password* atau ID digital) 2. Penggunaan untuk *log in* pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3. *Firewall* dan sistem-sistem serta prosedur-prosedur deteksi terhadap intrusi

ARSIP NASIONAL REPUBLIK INDONESIA

NO.	TINGKAT KLASIFIKASI KEAMANAN	MEDIA ARSIP					
		ARSIP KONVENSIONAL			ARSIP ELEKTRONIK		
		Arsip	Pengguna	Prasarana & Sarana	Arsip	Pengguna	Prasarana & Sarana
3.	Rahasia	1. Ada persyaratan dan prosedur rahasia dengan memberikan cap "RAHASIA" pada fisik arsip 2. Tidak sembarangan meletakkan arsip/ dokumen yang bersifat rahasia	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Lokasi aman dengan akses yang terbatas	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	3. Hanya staf yang ditunjuk oleh kementerian atau organisasi dan tingkat di atasnya yang dapat mengakses arsip tersebut 4. Autentikasi pengguna (nama pengguna/ *password* atau ID digital) 5. Penggunaan untuk *log in* pada tingkat individual	4. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 5. *Firewall* serta sistem-sistem dan prosedur-prosedur deteksi terhadap intrusi. *Firewall* adalah sistem untuk melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk mengakses komputer atau jaringan kita
4.	Sangat Rahasia	Ada persyaratan dan prosedur rahasia dengan memberikan cap "SANGAT RAHASIA" pada fisik arsip	Dibatasi hanya untuk Penentu Kebijakan, Pengawasan, dan Penegak Hukum	1. Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses 2. Penerapan kebijakan "Meja harus bersih"	*1. Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip *2.* File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-	1. Autentikasi pengguna (nama pengguna/*password* atau ID digital) 2. Penggunaan untuk *log in* pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3. Firewall dan sistem-sistem dan prosedur-prosedur deteksi terhadap intrusi.

ARSIP NASIONAL REPUBLIK INDONESIA

NO.	TINGKAT KLASIFIKASI KEAMANAN	MEDIA ARSIP					
		ARSIP KONVENSIONAL			ARSIP ELEKTRONIK		
		Arsip	Pengguna	Prasarana & Sarana	Arsip	Pengguna	Prasarana & Sarana
					pihak eksternal		

Catatan:

Ketentuan tentang *back up* pada arsip elektronik yang berlaku pada arsip dengan klasifikasi sangat rahasia meliputi juga ketentuan yang berlaku pada arsip dengan ketentuan rahasia dan terbatas. Ketentuan tentang *back up* pada arsip elektronik yang berlaku pada arsip dengan klasifikasi terbatas dengan metode *back up* yang sesuai dengan tingkatan klasifikasi keamanan.

2. Penyampaian

Penyampaian dalam rangka penanganan fisik maupun informasi arsip dinamis sesuai dengan tingkat klasifikasi dapat dilakukan melalui pengiriman yang dilindungi sebagaimana tabel di bawah ini:

Tabel 4. Prosedur Pengiriman Informasi

NO.	TINGKAT/ DERAJAT KLASIFIKASI	ARSIP KONVENSIONAL	ARSIP ELEKTRONIK
1.	Biasa/Terbuka	Tidak ada persyaratan prosedur khusus.	Tidak ada prosedur khusus.
2.	Terbatas	Amplop segel.	Apabila pesan elektronik atau email berisi data tentang informasi personal, harus menggunakan enkripsi, email yang dikirim dengan alamat khusus, *password,* dan lain-lain.
3.	Rahasia	1. Menggunakan warna kertas yang berbeda 2. Diberi kode rahasia 3. Menggunakan amplop dobel 4. Amplop segel, stempel rahasia. 5. Konfirmasi tanda terima. 6. Harus dikirim melalui orang yang sudah diberi wewenang dan tanggung jawab terhadap pengendalian arsip/ dokumen rahasia.	1. Harus ada konfirmasi dari penerima pesan elektronik atau email. 2. Menggunakan perangkat yang dikhususkan bagi pesan elektronik atau email rahasia. 3. Menggunakan persandian atau kriptografi.
4.	Sangat Rahasia	1. Menggunakan warna kertas yang berbeda. 2. Menggunakan amplop dobel bersegel. 3. Audit jejak untuk setiap titik akses (misal: tandatangan). 4. Harus dikirim melalui orang yang sudah diberi wewenang dan tanggung jawab terhadap pengendalian arsip/dokumen rahasia.	1. Harus ada konfirmasi dari penerima pesan elektronik atau email. 2. Menggunakan perangkat yang dikhususkan bagi pesan elektronik atau email rahasia. 3. Menggunakan persandian atau kriptografi 4. Harus ada pelacakan akses informasi untuk suatu pesan elektronik atau email.

Catatan: ketentuan yang berlaku pada arsip dengan klasifikasi sangat rahasia meliputi juga ketentuan yang berlaku pada arsip dengan klasifikasi rahasia dan terbatas. Ketentuan yang berlaku pada arsip dengan klasifikasi rahasia meliputi juga ketentuan yang berlaku pada arsip dengan klasifikasi terbatas.

ARSIP NASIONAL REPUBLIK INDONESIA

BAB IV

TATA CARA PEMBUATAN DAFTAR ARSIP DINAMIS BERDASARKAN KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS

A. Format Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis

Format Daftar Arsip Dinamis berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis terdiri atas: nomor, kode klasifikasi, jenis arsip, klasifikasi keamanan, hak akses, dasar pertimbangan, dan unit pengolah. Rincian lebih lanjut sebagai berikut:

Daftar Arsip Dinamis
Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis

Nomor	Kode Klasifikasi	Jenis Arsip	Klasifikasi Keamanan	Hak Akses	Dasar Pertimbangan	Unit Pengolah
1	2	3	4	5	6	7

Pengesahan:
Tempat, tanggal. bulan, tahun
Jabatan
Tanda tangan pejabat yang mengesahkan
Nama

Keterangan:

1. Kolom “Nomor”, diisi dengan nomor urut;
2. Kolom “Kode Klasifikasi”, diisi dengan kode angka, huruf atau gabungan angka dan huruf yang akan berguna untuk mengintegrasikan antara penciptaan, penyimpanan, dan penyusutan arsip dalam satu kode yang sama sehingga memudahkan pengelolaan;
3. Kolom “Jenis Arsip” diisi dengan judul dan uraian singkat yang menggambarkan isi dari jenis/seri arsip;
4. Kolom “Klasifikasi Keamanan”, diisi dengan tingkat keamanan dari masing-masing jenis/seri arsip yaitu sangat rahasia, rahasia, terbatas atau biasa/terbuka;

5. Kolom “Hak Akses”, diisi dengan nama jabatan yang dapat melakukan pengaksesan terhadap arsip berdasarkan tingkat/ derajat klasifikasi;
6. Kolom dasar pertimbangan, diisi dengan uraian yang menerangkan alasan pengkategorian arsip sebagai sangat rahasia, rahasia dan terbatas;
7. Kolom unit pengolah, diisi dengan unit kerja yang bertanggung jawab terhadap keselamatan dan keamanan fisik dan informasi arsip yang dikategorikan sangat rahasia, rahasia dan terbatas.

B. Prosedur Pembuatan Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis.

Langkah-langkah Pembuatan Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis adalah sebagai berikut:

1. Penentuan Klasifikasi Keamanan dan Hak Akses.

   Penentuan Klasifikasi Keamanan dan Hak Akses dilakukan dengan mempertimbangkan:

   a. Aspek ketentuan peraturan perundang-undangan dan Norma Standar Pedoman Kriteria masing-masing instansi;
   b. Hasil analisis fungsi unit kerja dan *Job Description;*
   c. Aspek analisis risiko;
2. Pencantuman Klasifikasi Keamanan dan Hak Akses pada kolom daftar.

   Hasil penentuan Klasifikasi Keamanan dan Hak Akses Arsip Dinamis pada pencipta arsip dituangkan dalam kolom-kolom yang terdiri dari: nomor, kode klasifikasi, jenis arsip, klasifikasi keamanan, hak akses dan dasar pertimbangan dan unit pengolah.

   Kode klasifikasi dicantumkan apabila sudah dimiliki. Apabila belum, perlu dilakukan analisis fungsi untuk menentukan jenis arsip tanpa mengisi kolom kode klasifikasi.
3. Pencantuman dasar pertimbangan.

   Dasar pertimbangan dituangkan untuk mengetahui alasan mengapa arsip dikategorikan pada tingkat/derajat klasifikasi keamanan sangat rahasia, rahasia dan terbatas.

4. Menentukan unit pengolah

   Unit pengolah perlu dicantumkan dalam daftar guna mengetahui unit yang bertanggung jawab terhadap keselamatan dan keamanan fisik dan informasi arsip yang dikategorikan sangat rahasia, rahasia dan terbatas.

5. Pengesahan oleh Pimpinan Organisasi.

   Pimpinan organisasi yang berwenang mengesahkan Daftar Arsip Dinamis berdasarkan klasifikasi keamanan dan akses arsip adalah pimpinan pencipta arsip.

ARSIP NASIONAL REPUBLIK INDONESIA

BAB V

PENUTUP

Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis dilaksanakan oleh setiap pencipta arsip berdasarkan ketentuan sebagaimana dimaksud dalam peraturan ini, sehingga informasi dalam arsip dinamis dapat terlindungi secara fisik dan dari akses oleh pihak yang tidak berhak.

KEPALA ARSIP NASIONAL REPUBLIK INDONESIA,

ttd

M. ASICHIN