Walikota Tasikmalaya

Provinsi Jawa Barat

PERATURAN WALI KOTA TASIKMALAYA

NOMOR 45 TAHUN 2017

TENTANG

TATA CARA PENYUSUNAN
SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA TASIKMALAYA,

Menimbang :

a. bahwa sistem klasifikasi keamanan dan akses arsip dinamis disusun sebagai upaya untuk melindungi hak dan kewajiban pencipta arsip dan publik terhadap akses arsip;

b. bahwa sesuai dengan ketentuan Pasal 5 dan Pasal 8 Peraturan Daerah Kota Tasikmalaya Nomor 5 Tahun 2015 tentang Penyelenggaraan Kearsipan, Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang kearsipan selaku Lembaga Kearsipan memiliki tanggung jawab untuk menyusun pedoman kearsipan, termasuk sistem klasifikasi keamanan dan akses arsip dinamis;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Wali Kota tentang Tata Cara Penyusunan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis;

Mengingat :

1. Undang-Undang Nomor 10 Tahun 2001 tentang Pembentukan Kota Tasikmalaya (Lembaran Negara Republik Indonesia Tahun 2001 Nomor 89, Tambahan Lembaran Negara Republik Indonesia Nomor 4117);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 3151);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Nomor 61, Tambahan Lembar Negara Republik Indonesia Nomor 86);

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. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik

Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);

6. Peraturan Pemerintah Nomor 28 Tahun 2012 tentang Pelaksanaan Undang Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 53, Tambahan Lembaran Negara Republik Indonesia Nomor 5286);
7. Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 17 Tahun 2011 tentang Penyusunan Pedoman Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis;
8. Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 26 Tahun 2011 tentang Tata Cara Penyediaan Arsip Dinamis sebagai Informasi Publik;
9. Peraturan Daerah Kota Tasikmalaya Nomor 5 Tahun 2015 tentang Penyelenggaraan Kearsipan (Lembaran Daerah Kota Tasikmalaya Tahun 2015 Nomor 163, Tambahan Lembaran Daerah Kota Tasikmalaya Nomor 7);

MEMUTUSKAN :

Menetapkan : PERATURAN WALI KOTA TENTANG TATA CARA PENYUSUNAN SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini, yang dimaksud dengan :

1. Daerah adalah Kota Tasikmalaya.
2. Wali Kota adalah Wali Kota Tasikmalaya.
3. Perangkat Daerah adalah Perangkat Daerah di lingkungan Pemerintah Kota Tasikmalaya.
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 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. Klasifikasi Keamanan Arsip Dinamis adalah pengkategorian/penggolongan arsip dinamis berdasarkan pada tingkat keseriusan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik dan perorangan.
7. Akses Arsip adalah ketersediaan arsip sebagai hasil dari kewenangan hukum dan otorisasi legal serta keberadaan sarana bantu untuk mempermudah penemuan dan pemanfaatan arsip.
8. Pengamanan Arsip Dinamis adalah program perlindungan terhadap fisik dan informasi arsip dinamis berdasarkan klasifikasi keamanan yang ditetapkan sebelumnya.
9. Badan Publik adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat, dan/atau luar negeri.
10. Pencipta Arsip adalah pihak yang mempunyai kemandirian dan otoritas dalam pelaksanaan fungsi, tugas, dan tanggung jawab di bidang pengelolaan arsip dinamis.
11. Pemohon Informasi Publik adalah warga Negara dan/atau badan hukum Indonesia yang mengajukan permintaan informasi publik.
12. 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.
13. 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.
14. 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.
15. Biasa/Terbuka adalah klasifikasi informasi dari arsip yang memiliki informasi yang apabila diketahui oleh publik tidak merugikan siapapun.
16. 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
MAKSUD DAN TUJUAN

Pasal 2

(1) Peraturan Wali Kota ini dibentuk dengan maksud untuk menjadi pedoman bagi pencipta arsip di lingkungan Pemerintah Daerah dalam membuat sistem klasifikasi keamanan dan akses arsip dinamis.

(2) Peraturan Wali Kota ini dibentuk dengan tujuan untuk :
   a. melindungi fisik dan informasi arsip dinamis dari kerusakan dan kehilangan sehingga kebutuhan terhadap ketersediaan, keterbacaan, keutuhan, integritas, otentisitas dan reliabilitas arsip tetap dapat terpenuhi; dan
   b. mengatur akses arsip dinamis yang sesuai dengan ketentuan peraturan perundang-undangan sehingga dapat dicegah terjadinya penyalahgunaan arsip oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah.

BAB III
RUANG LINGKUP

Pasal 3

Ruang lingkup Peraturan Wali Kota ini mengatur hal-hal yang berkenaan dengan Tata Cara Penyusunan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis, yang meliputi :

a. tata cara penyusunan Klasifikasi Keamanan dan Penentuan Hak Akses Arsip Dinamis; dan
b. tata cara penyusunan Daftar Arsip Dinamis berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis.

BAB IV
TATA CARA PENYUSUNAN SISTEM KLASIFIKASI
KEAMANAN DAN AKSES ARSIP DINAMIS

Pasal 4

(1) Tata Cara Penyusunan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis berlaku bagi pencipta arsip sebagai panduan dalam melaksanakan:
   a. penyusunan klasifikasi keamanan dan penentuan hak akses arsip dinamis; dan
   b. penyusunan daftar arsip dinamis berdasarkan klasifikasi keamanan dan akses arsip dinamis.

(2) Tata Cara Penyusunan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis sebagaimana dimaksud pada ayat (1), tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB V
KETENTUAN PENUTUP

Pasal 5

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Tasikmalaya.

Ditetapkan di Tasikmalaya
pada tanggal 16 November 2017

WALI KOTA TASIKMALAYA,

ttd

H. BUDI BUDIMAN

Diundangkan di Tasikmalaya
pada tanggal 16 November 2017

Plt. SEKRETARIS DAERAH KOTA TASIKMALAYA,

ttd

IVAN DICKSAN HASANNUDIN

BERITA DAERAH KOTA TASIKMALAYA TAHUN 2017 NOMOR 410

LAMPIRAN
PERATURAN WALI KOTA TASIKMALAYA
NOMOR 45 TAHUN 2017
TENTANG
PEDOMAN PENYUSUNAN SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS

TATA CARA PENYUSUNAN SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS

BAB I
UMUM

A. Prinsip Dasar Penyusunan Sistem Klasifikasi Keamanan Arsip Dinamis.

Prinsip dasar dalam penetapan Sistem Klasifikasi Keamanan Arsip Dinamis adalah sebagai berikut:

1. memperhatikan tingkat keseriusan dampak yang timbul apabila informasi yang terdapat dalam arsip disalahgunakan oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah; dan
2. pengklasifikasian keamanan arsip yang dituangkan dalam keputusan pimpinan pencipta arsip yang berisi boleh atau tidaknya suatu arsip diakses dengan disertai alasan sebagai dasar pertimbangan dalam menentukan tingkat klasifikasi.

B. Prinsip Dasar Akses Arsip Dinamis.

Prinsip dasar dalam penetapan hak akses Arsip Dinamis adalah:

1. pengaksesan arsip hanya dapat dilakukan oleh pejabat dan staf yang mempunyai kewenangan untuk mengakses;
2. pejabat yang lebih tinggi kedudukannya dapat mengakses arsip yang dibuat oleh pejabat atau staf di bawahnya sesuai dengan hierarki kewenangan dalam struktur organisasi; dan
3. pejabat atau staf yang lebih rendah kedudukannya tidak dapat mengakses arsip yang dibuat oleh pejabat yang lebih tinggi kedudukannya kecuali atas izin pimpinan pencipta arsip.

BAB II
TATA CARA PENYUSUNAN SISTEM KLASIFIKASI
KEAMANAN DAN AKSES ARSIP

Kegiatan penyusunan sistem klasifikasi keamanan dan penentuan hak akses arsip dinamis terletak pada proses penciptaan dan penggunaan arsip yang dalam penyusunannya harus memperhatikan langkah-langkah sebagai berikut:

a. identifikasi ketentuan hukum;
b. analisis fungsi unit kerja dalam organisasi; dan
c. analisis uraian Jabatan (*job description*) serta analisis risiko.

Melalui ketiga langkah tersebut di atas, Pencipta Arsip dapat menentukan 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 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
3. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan;
4. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
5. Peraturan Pemerintah Nomor 28 Tahun 2012 tentang Pelaksanaan Undang-undang Nomor 43 tahun 2009 tentang Kearsipan;
6. Peraturan Daerah Kota Tasikmalaya Nomor 5 Tahun 2015 tentang Penyelenggaraan Kearsipan; dan
7. 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 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."

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 rencanarencana 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 antar negara;

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. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan.

Pasal 42

ayat (1)

“Pencipta arsip wajib menyediakan arsip dinamis bagi kepentingan pengguna arsip yang berhak”.

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)".

4. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Pasal 2

1) Dalam hal ada permintaan Informasi Publik oleh Pemohon Informasi Publik, Badan Publik wajib membuat pertimbangan tertulis atas setiap kebijakan yang diambil untuk memenuhi hak setiap Pemohon Informasi Publik.

2) Pertimbangan tertulis sebagaimana dimaksud pada ayat (1) ditetapkan oleh PPID atas persetujuan pimpinan Badan Publik yang bersangkutan.

3) Pertimbangan tertulis sebagaimana dimaksud pada ayat (1) dapat diakses oleh setiap Pemohon Informasi Publik.

Pasal 3

1) Pengklasifikasian Informasi ditetapkan oleh PPID di setiap Badan Publik berdasarkan Pengujian Konsekuensi secara saksama dan penuh ketelitian sebelum menyatakan Informasi Publik tertentu dikecualikan untuk diakses oleh setiap orang.

2) Penetapan Pengklasifikasian Informasi sebagaimana dimaksud pada ayat (1) dilakukan atas persetujuan pimpinan Badan Publik yang bersangkutan.

5. Peraturan Pemerintah Nomor 28 Tahun 2012 tentang Pelaksanaan Undang-undang Nomor 43 tahun 2009 tentang Kearsipan;

Pasal 37

Ayat (1)

"Penggunaan arsip dinamis sebagaimana dimaksud dalam Pasal 31 huruf b diperuntukkan bagi kepentingan pemerintahan dan masyarakat".

Ayat (4)

"Pimpinan unit kearsipan bertanggung jawab terhadap ketersediaan, pengolahan, dan penyajian arsip inaktif untuk kepentingan penggunaan internal dan kepentingan publik".

Pasal 38

"Penggunaan arsip dinamis sebagaimana dimaksud dalam Pasal 37 ayat (1) dilaksanakan berdasarkan sistem klasifikasi keamanan dan akses arsip".

Pasal 39

"Penggunaan arsip dinamis oleh pengguna yang berhak dilaksanakan berdasarkan ketentuan peraturan perundang-undangan".

Pasal 125

1) Untuk meningkatkan manfaat arsip bagi kesejahteraan rakyat, JIKN digunakan sebagai wadah layanan informasi kearsipan untuk kepentingan pemerintahan dan masyarakat.
2) Informasi kearsipan sebagaimana dimaksud pada ayat (1) bersifat terbuka sesuai dengan ketentuan peraturan perundang-undangan.

6. Peraturan Daerah Kota Tasikmalaya Nomor 5 tahun 2015 tentang penyelenggaraan Kearsipan.

Pasal 11

ayat (1)

"Pengelolaan Arsip dilakukan untuk menjamin ketersediaan dan keselamatan arsip yang autentik, utuh dan terpercaya dengan didasarkan pada sifat keterbukaan dan ketertutupan informasi sesuai dengan ketentuan peraturan perundang undangan".

Pasal 18

"Klasifikasi keamanan dan akses arsip disusun sebagai dasar untuk menentukan keterbukaan dan kerahasiaan arsip dalam rangka penggunaan arsip dan informasinya sesuai dengan ketentuan peraturan perundang-undangan".

Pasal 22

ayat (4)

"Pimpinan Unit Kearsipan II bertanggung jawab terhadap ketersediaan, pengolahan dan penyajian Arsip Inaktif untuk kepentingan penggunaan internal Pencipta Arsip dan kepentingan publik".

Ayat (6)

Penggunaan Arsip Dinamis sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan sistem klasifikasi keamanan dan akses arsip.

B. Analisis Fungsi Unit Kerja dalam Organisasi dan Uraian Jabatan (*Job Description).*

Setelah melakukan identifikasi terhadap ketentuan hukum yang menjadi bahan pertimbangan dalam Penyusunan klasifikasi keamanan dan penentuan hak akses arsip dinamis, langkah selanjutnya adalah melakukan analisis fungsi unit kerja dalam organisasi dan analisis uraian jabatan (*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:

- ✓ Dalam struktur organisasi Dinas Perpustakaan dan Kearsipan Daerah Kota Tasikmalaya, salah satu fungsinya adalah penyusutan arsip. Kegiatan yang tercipta dari fungsi tersebut antara lain SK Tim Penilai Arsip, Daftar Arsip yang disusutkan, Daftar Arsip yang dinilai, Rekomendasi Tim Penilai Arsip, Berita Acara Penyusutan dan Surat Persetujuan Pemusnahan Arsip (apabila arsip dimusnakan).

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

No	Unit Kerja	Fungsi	Kegiatan	Arsip Tercipta	Keterangan
1	Dinas Perpustakaan dan Kearsipan Daerah	Pengelolaan Arsip	Penyusutan Arsip	✓ SK Tim Penilai Arsip ✓ Daftar Arsip yang disusutkan ✓ Daftar Arsip yang dinilai ✓ Rekomendasi Tim Penilai Arsip ✓ Berita Acara Penyusutan ✓ Surat Persetujuan Pemusnahan Arsip (apabila arsip dimusnakan).	✓ Dipertimbang kan terbuka ✓ Dipertimbang kan terbuka ✓ Dipertimbang kan terbuka ✓ Dipertimbang kan Terbuka ✓ Dipertimbang kan terbuka ✓ Dipertimbangkan terbuka

No	Unit Kerja	Fungsi	Kegiatan	Arsip Tercipta	Keterangan
			Penyusunan Peraturan Wali Kota	Peraturan Wali Kota (Arsip Statis)	Terbuka

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/SKP, 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 Uraian Jabatan (*Job Description*). Uraian Jabatan (*Job Description*) 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. Untuk itu, dapat digolongkan personil tertentu yang diberi wewenang dan tanggung jawab dalam Penyusunan, penanganan, pengelolaan keamanan informasi dan diberi hak akses arsip.

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
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. Pelaksanaan 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 OPD Satpol PP misalnya arsip razia penertiban penyakit masyarakat dan penegakan PPNS (dijelaskan diatas ketententuan umum) mulai dari perencanaan dan pelaksanaannya dirahasiakan. Setelah dilakukan analisis risiko, hasil analisis menyimpulkan:
   1) Jika arsip tersebut dibuka, maka dapat menimbulkan terganggunya ketertiban umum dan individu serta fungsi penyelenggaraan pemerintah Satpol PP tidak berjalan.
   2) Jika arsip ditutup, maka kemungkinan risiko yang dapat timbul tidak ada sehingga lebih baik dikategorikan rahasia. Berdasarkan analisis risiko tersebut, kewenangan hak akses arsip dinamis hanya terdapat pada penentu kebijakan sesuai dengan kewenangannya.
b. 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 terbatas 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 privasi, 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 sekurangkurangnya 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:

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	V	V	V	V	V
2	Terbatas	V	-	V	-	V
3	Rahasia	V	-	V	-	V
4	Sangat Rahasia	V	-	V	-	V

Keterangan Tabel 2:

1. 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.
2. Arsip Berklasifikasi Rahasia, hak akses diberikan kepada pimpinan tingkat tinggi dan setingkat di bawahnya apabila sudah diberikan izin, pengawas internal/eksternal dan penegak hukum.
3. Arsip Berklasifikasi Terbatas, hak akses diberikan kepada pimpinan tingkat menengah dan setingkat di bawahnya apabila sudah diberikan izin, pengawas internal/eksternal dan penegak hukum.
4. 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:

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	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Biasa / Terbuka	Tidak ada persyaratan dan prosedur khusus	Pengguna yang berasal dari eksternal dan internal yang mepunyai hak akses	Tidak memerlukan prasarana dan sarana khusus	Back up secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autensitas 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 autensitas arsip 2. File-file elektro-nik (termasuk database) harus dilindungi terhadap penggunaan internal atau pihakpihak eksternal	1. Autentifikasi peng-guna (nama pengguna/pass word atau ID digital) 2. Penggunaan untuk log in pada tingkat individual	1. Autentifikasi server 2. Langkah-langkah keamanan dengan operating system khusus atau aplikasi khusus

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 pemu-lihan sistem dalam rangka menjamin autentisita s arsip. 2. File-file elek-tronik (te-ma-suk data-base) harus di lindungi terhadap penggunaan internal atau oleh pihakpihak eksternal	1. Hanya staf yang di tunjuk oleh kemantrian atau organisasi dan tingkat di atasnya dapat mengakses arsip tersebut. 2. Autentikasi pengguna (nama pengguna/ pasword atau id digital). 3. Pengguna untuk log in pada tingkat individual	1. Firewall dan system-sistem serta prosedur-prosedur deteksi terhadap intrusi 2. Langkah-langkah keamanan dengan operating system khusus atau aplikasi khusus. 3. Firewall serta sistem-sistem dan prosedur-prosedur deteksi terhadap intruksi. Firewall adalah system untuk melindungi computer 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, Pengawas internal dan eksternal serta penegak hukum	1. Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses	1. Back up secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip	1. Autensifikasi pengguna (nama pengguna/ password atau ID digital)	1. Autensifikasi server 2. Langkah-langkah keamanan dengan operating system khusus atau aplikasi khusus

				2. Penerapan kebijakan “Meja harus bersih”	2. File-file elektronik (termasuk database) harus di lindungi terhadap penggunaa n internal atau oleh pihakpihak eksternal .	2.Penggunaan untuk log in pada tingkat individual	3. Firewall dan sistem-sistem dan prosedurprosedur deteksi terhadap intrusi

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.

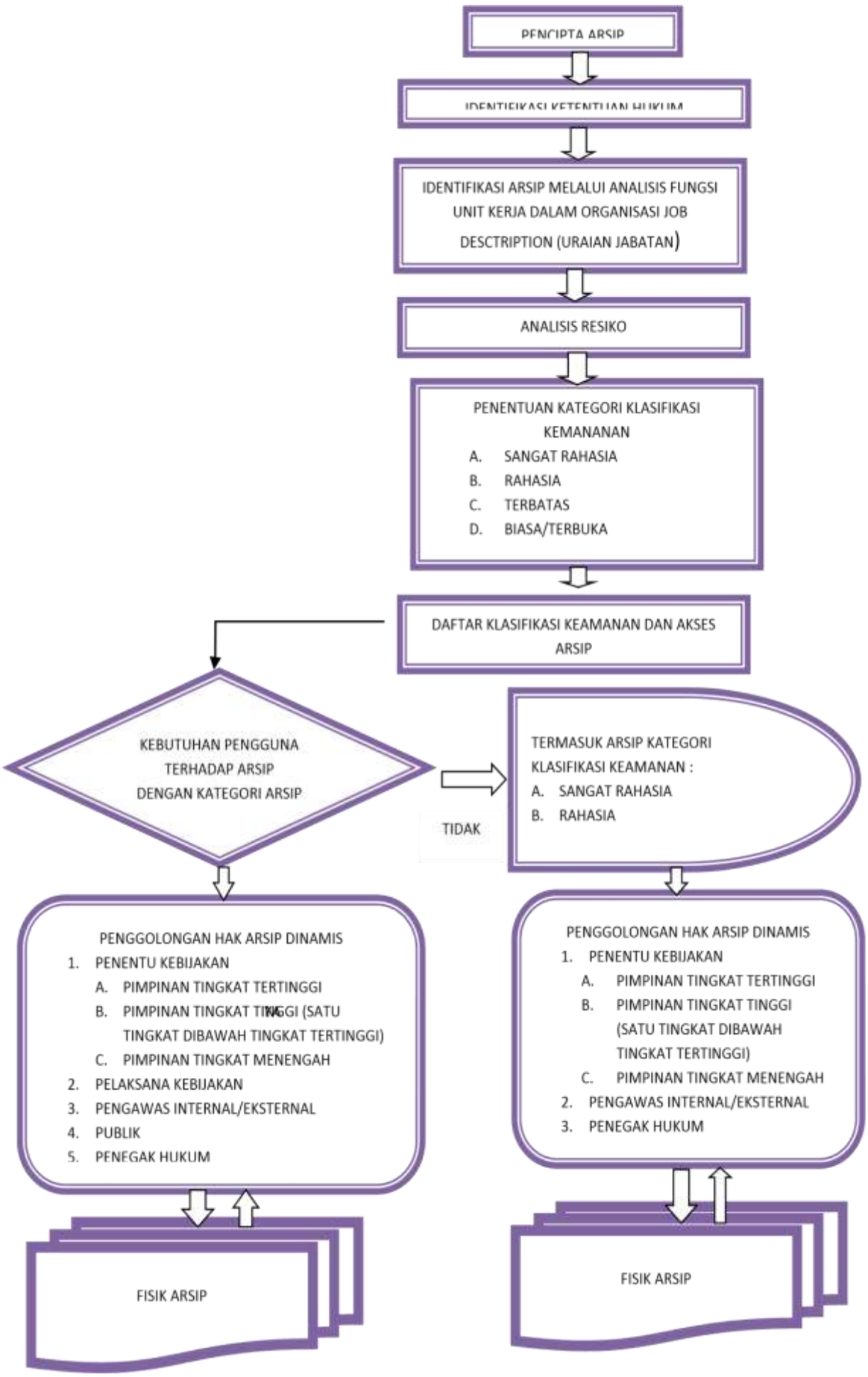
2) Penyampaian.

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	*2*	*3*	*4*
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 persan-dian 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

Tata Cara Penyusunan Sistem Klasifikasi Keamanan dan Hak Akses Arsip Dinamis, dapat digambarkan dengan bagan alur sebagai berikut:



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.

BAB III
TATA CARA PENYUSUNAN 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. Tata Cara Penyusunan Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis.

Langkah-langkah Penyusunan 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.

BAB IV
PENUTUP

Dalam rangka melindungi setiap informasi yang tertuang dalam arsip dinamis, baik secara fisik maupun akses pihak yang tidak berhak, maka setiap Penyusunan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis pada pencipta arsip di lingkungan Pemerintah Daerah dan BUMD wajib mempedomani ketentuan dalam Peraturan Wali Kota ini dan dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

WALI KOTA TASIKMALAYA

ttd

H. BUDI BUDIMAN