



PROVINSI SULAWESI SELATAN

PERATURAN WALIKOTA MAKASSAR

Nomor - 34 TAHUN 2018

TENTANG

PEDOMAN PEMBUATAN SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS

DENGAN RAHMAT TUHAN YANG Maha ESA.

WALIKOTA MAKASSAR,

- Membimbang : 4. bahwa dalam ranahnya mendukung pengelolaan arsip dinamis yang efektif dan efisien sebagaimana diamanatkan dalam Pasal 4D ayat (4) Undang-Undang Nomor 43 Tahun 2009 tentang Keardipan, serta untuk mencegah terjadinya penyalahgunaan arsip oleh pihak-pihak yang tidak berhak, maka perlu diatur dalam suatu pedoman pembuatan sistem klasifikasi keamanan dan akses arsip dinamis;
5. bahwa berdasarkan pertimbangan pada huruf a tersebut di atas, perlu ditetapkan Peraturan Walikota Kota Makassar tentang Pedoman Pembuatan Sistem Klasifikasi Keamanan Dan Akses Arsip Dinamis.

- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 29 Tahun 1959 tentang pembentukan Daerah tingkat II di Sulawesi (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 74, Tambahan Lembaran Negara Republik Indonesia Nomor 1822);
3. Undang-Undang Nomor 11 Tahun 2008 tentang Infrastruktur dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
4. 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);
5. Undang-Undang Nomor 26 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

6. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071);
7. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234);
8. 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 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 38, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
9. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
10. Peraturan Pemerintah Nomor 51 Tahun 1971 tentang Perubahan Batas-batas Daerah Kota/Muadzim Makassar dan Kabupaten/kabupaten Gowa, Maros, dan Pangkajene dan Kepulauan Dalam Lingkungan Daerah Propinsi Sulawesi Selatan (Lembaran Negara Republik Indonesia Tahun 1971 Nomor 65, Tambahan Lembaran Negara Republik Indonesia Nomor 2970);
11. Peraturan Pemerintah Nomor 86 Tahun 1999 tentang Perubahan Nama Kota Ujung Pandang menjadi Kota Makassar Dalam Wilayah Propinsi Sulawesi Selatan (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 193);
12. 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);
13. 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);
14. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Nomor 2036 Tahun 2015).

MEMUTUSKAN :

Menetapkan

PERATURAN WALIKOTA MAKASSAR TENTANG PEDOMAN PEMBUATAN SISTEM KLASIFIKASI KEMAMUAN DAN AKSES ARSIP DINAMIS.

BAB I KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini, yang di maknai dengan :

1. Daerah adalah Kota Makassar;
2. Pemerintah Daerah adalah Pemerintah Kota Makassar;
3. Walikota adalah Walikota Makassar;
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Makassar;
5. Perangkat Daerah adalah unsur bantuan Walikota dalam penyelenggaraan pemerintahan daerah yang terdiri dari Sekretariat Daerah, Sekretariat DPRD, Dinas, Inspektorat, Badan, Satuan Polisi Pamong Praja, Kantor, Kecamatan dan Kelurahan;
6. Arsip adalah rekaman kejadian 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 peradilan dalam pelaksanaan kehidupan berasyarakat, berbangsa, dan bernegara.
7. Arsip dinamis adalah arsip yang digunakan secara langsung dalam kegiatan pencipta arsip dan diimpan selama jangka waktu tertentu.
8. Pencipta arsip adalah pihak yang mempunyai kemandirian dan otoritas dalam pelaksanaan fungsi, tugas, dan tanggung jawab di bidang pengelolaan arsip dinamis.
9. Akses arsip adalah ketersediaan arsip sebagai hasil dari kewenangan hukum dan otorisasi legal serta keberadaan satuan bantu untuk mempermudah penemuan dan pemanfaatan arsip.

BAB II

Pasal 2

Pedoman Pembuatan Sistem Klasifikasi Kemamuhan dan Akses Arsip Dinamis tercantum dalam lampiran Peraturan ini dan merupakan bagian yang tidak terpisahkan dari Peraturan ini.

Pasal 3

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

**BAB III
KETENTUAN PENUTUP**

Pasal 4

Persetujuan Walikota ini mulai berlaku sejak teranggip diundangkan.

Agar semakin orang mengetahui hal ini, maka diundangkan persetujuan Walikota ini dengan penempatannya dalam Berita Daerah Kota Makassar.

Ditetapkan di Makassar
pada tanggal 25 September 2015

WALIKOTA MAKASSAR,


MUHAMAD RAMDHAN POMANTO

Diketahui di Makassar
pada tanggal 25 September 2015

Pj. Gubernur Daerah Kota Makassar,


A. NASYWAN T. AZIZIN

BERITA DAERAH KOTA MAKASSAR TAHUN 2015 NOMOR 36

LAMPIRAN
PERATURAN WALIKOTA MAKASSAR
NOMOR 3 TAHUN 2015
TENTANG PEDOMAN PEMBUATAN SISTEM
KLASIFIKASI KEAMANAN DAN AKSES
ARSIP DINAMIS

BAB I
PENDAHULUAN

A. Latar Belakang

Selanjutnya dalam Pasal 40 Undang-Undang Nomor 43 Tahun 2009 tentang Kebersihan, pengelolaan arsip ditentukan untuk menjamin ketepatan arsip dalam penyelenggaran kegiatan sebagai bahan akuntabilitas kinerja dan alat bukti yang sah berdasarkan sistem yang memenuhi persyaratan andal, sistematis, utuh, menyeluruh dan sesuai norma, standar, prosedur dan kriteria (NSPK). Ketersedian arsip digunakan untuk kegiatan operasional manajemen penciptaan arsip dan layanan publik. Untuk itu diperlukan adanya sistem klasifikasi keamanan dan akses arsip dinamis.

Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis diciptakan sebagai dasar untuk melindungi hak dan keutuhan penikahan arsip dan publik terhadap arsip arsip. Dalam era keserbaan seperti saat ini, arsip dinamis pada prinsipnya terbuka dan dapat diakses oleh publik, kecuali yang diwajibkan tertutup, sebagaimana diatur pada Pasal 42 ayat (1) Undang-Undang Nomor 43 Tahun 2009 bahwa "pembentukan arsip wajib menyediakan arsip dinamis bagi pengguna arsip yang berlaku". Arsip dinamis adalah salah satu warisan informasi publik adalah bersifat terbatas dan dapat diakses oleh publik sejauh Pasal 2 ayat (1) Undang-Undang Nomor 14 Tahun 2008 bahwa "setiap informasi publik bersifat terbatas dan dapat diakses oleh setiap pengguna informasi publik". Hal ini sejalan dengan konsepsi meningkat Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, yang menggantikan bahwa informasi merupakan kewajiban pelaksanaan pokok dan hak azasi 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 hak arsip maka perlu datur ketentuan tentang pengarahan dan akses arsip dinamis. Pengaturan pengarahan dan akses tersebut untuk menjamin pengarahan serta keamanan atas hak dan mengatur kebutuhan orang lain dalam rangka untuk mencapai tujuan yang adil sesuai dengan pertumbuhan 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 (AKRI) menyatakan pedoman pembuatan sistem klasifikasi keamanan dan akses arsip dinamis yang dapat dipergunakan sebagai pedoman bagi penciptaan arsip, dalam mengelola arsip dinamis sesuai kaidah kesesuaian 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 penciptaan arsip dalam menjamin klasifikasi keamanan dan akses arsip dinamis, dengan tujuan:

1. Melindungi fisik dan informasi arsip dinamis dari kerusakan dan kerugian sehingga keberadaan akan ketepatan, keabsahan, keutuhan, integritas, identitas dan reliabilitas arsip tetap dapat terjermuk;
2. Menghalangi akses arsip dinamis yang secara ketentuan peraturan perundang-undangan sehingga dapat dicegah terjadinya penyabotage arsip oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah.

C. Ruang Lingkup

Ruang lingkup P-odoker o Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis antara ketentuan sebagai berikut:

1. Ketentuan Umum;
2. Tata Cara Pembuatan Klasifikasi Keamanan dan Penentuan Jatah Akses Arsip Dinamis;

3. Tuju Cara Pembuatan Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis.

D. Pengertian

1. Klasifikasi Keamanan Arsip Dinamis adalah pengkategorian/penggrupan arsip dinamis berdasarkan pada tingkat keamanan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik dan perorangan.
2. Klasifikasi Akses Arsip Dinamis adalah pengkategorian pengaturan keteraksesian arsip dinamis sebagai hasil dari kewenangan hukum dan otoritas legal pencipta arsip untuk mempermudah pelaksanaan arsip.
3. Pengamanan Arsip Dinamis adalah program perlindungan terhadap fisik dan informasi arsip dinamis berdasarkan klasifikasi keamanan yang ditetapkan sebelumnya.
4. Arsip adalah rekaman atau peristiwa dalam bentuk benda dan media manual maupun perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh berbagai negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan dan perorangan dalam pelaksanaan kehidupan bersosial-sosial, berbangsa dan bernegara.
5. Arsip Dinamis adalah arsip yang digunakan secara langsung dalam kegiatan penelitian arsip dan disimpan selama jangka waktu tertentu.
6. Publik adalah warganegara atau beras dasar hukum yang mengajukan pertanyaan untuk mempelajari arsip dinamis.
7. Pencipta Arsip adalah pihak yang mempunyai kepentingan di atasnya 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 bertujuh dapat membahayakan kestabilitan 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 bertujuh dapat mengakibatkan terganggunya

fungsinya penyelenggaraan Negara, sumber daya nasional dan/atau ketertiban umum.

10. Terbatas adalah klasifikasi informasi dinas/strip yang memilki informasi yang apabila diketahui oleh pihak yang tidak berhak dapat menghalangi terpenuhinya pelaksanaan tugas dan fungsi lembaga pemerintahan.
11. Buka/Terbatas adalah klasifikasi informasi dari strip yang memilki informasi yang apabila diketahui oleh publik tidak mengikuti kepentingan negara.
12. Tingkat klasifikasi kerentanan strip dinas/strip adalah pengelompokan strip dalam angketan tertentu berdasarkan dampak yang ditimbulkan apabila informasi yang terdapat di dalamnya diketahui oleh pihak yang tidak berhak.

BAB II

KETENTUAN UMUM

A. Kebijakan Pembentukan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis

Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis harus diketepikan oleh pimpinan pencipta arsip. Pencipta Arsip yang dimaksud adalah lembaga negara, pemintahahan 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 ketekunan dampak yang timbul apabila informasi yang terdapat dalam arsip dinamis dialihgunakan oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah;
2. Pengklasifikasian keamanan arsip dinamis harus diungkapkan dalam suatu ketepatan 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 kompetensi untuk akses;
2. Pejabat yang lebih tinggi kedudukannya dapat mengakses arsip yang diturut oleh pejabat atau staf di bawahnya selain dengan hierarki kompetensinya 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 KEMAMUAN DAN PENERIMAAN HAK AKSES ARSIP

Kegiatan membuat klasifikasi kemamuan dan menentukan hak akses arsip dinamis berada pada bagian prinsipal dan penggunaan arsip yang dalam: penyusunannya harus memperhatikan langkah-langkah sebagai berikut: identifikasi ketentuan hukum, analisa fungsi unitkerja dalam organisasi, analisa job description serta analisa risiko, sehingga dapat ditentukan kategoridiklasifikasi kemamuan dan hak akses arsip dinamis.

A. Identifikasi Ketentuan Hukum

Dalam identifikasi ketentuan hukum yang menjadi pedoman dalam arsip 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 perwujudan arsip yang berkaitan dengan klasifikasi kemamuan dan akses arsip dinamis.

Identifikasi ketentuan hukum yang dapat diungkapkan sebagai dasar penentuan klasifikasi kemamuan 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):

"Pemimpin arsip dapat menurunkan akses atas arsip dengan alas an spesialis arsip dibutuh untuk tujuan dapat:

- a. menghindari proses penegakan hukum;
- b. menggaung kepentingan perlindungan hak atau kekayahan intelektual dan perlindungan dari perselingkuhan usaha tidak sehat;
- c. membantayakan pertimbangan dari kesadaran negara;

- d. mengungkapkan kekayaan alam Indonesia yang masuk dalam kategori dilindungi kerahasiaannya;
- e. merugikan ketahanan ekonomi nasional;
- f. merugikan keperingatan politik luar negeri dan hubungan luar negeri;
- g. mengungkapkan isi sifat-sifat yang bersifat pribadi dan kemauan terakhir seseorang walaupun sebagian kecuali keadaan yang berlaku secara hukum;
- h. mengungkapkan rahasia atau data pribadi; dan
- i. mengungkap memorandum atau surat-surat yang menurut sifatnya perlu dirahasiakan.”

Pasal 44 ayat (2) :

“Pemohon arsip wajib menjaga kerahasiaan arsip tertutup sebagaimana diaksud pada ayat (1)”.

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

Pasal 17 :

“Setiap badan publik wajib memberikan akses bagi setiap Pemohon Informasi Publik untuk mendapatkan informasi Publik”, kecuali:

- a. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat menghambar proses persegulitan hukum, yaitu informasi yang dapat:
 - 1) Menghambar proses penyelidikan dan penyidikan suatu tindak pidana;
 - 2) Mengungkapkan identitas informan, pelaporkan, saksi dan/atau korban yang mengetahui adanya tindak pidana;
 - 3) Mengungkapkan data intai dan kronik dan rekaman yang berhubungan dengan peneguhan dan pertanggungan negara bentuk kejahatan transnasional;
 - 4) Mengungkapkan keseksualan dan kehidupan pribadi hukum dan/atau keluarganya; dan/atau
 - 5) Mengungkapkan keseksualan penulis, arahan, dan/atau prasaranan perugikan hukum.

- b. Informasi Publik yang spesial dibuka dan diberikan kepada Pemohon: Informasi Publik dapat menggunakan kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari perselingkuhan tanpa tidak sehat;
- c. Informasi Publik yang spesial dibuka dan diberikan kepada Pemohon: Informasi Publik dapat membahayakan pertahanan dan keamanan negara, yaitu:
- 1) Informasi tentang strategi, intelligen, operasi, teknik dan teknik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara, termasuk tahap perencanaan, pelaksanaan dan pengawasannya atau evaluasi dalam kaitan dengan keamanan dari dalam dan luar negri;
 - 2) Dokumen yang merumus tentang strategi, intelligen, operasi, teknik dan teknik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara yang meliputi tahap perencanaan, pelaksanaan dan pengawasan atau evaluasi;
 - 3) Komponen, alat-alat, atau dislokasi ketua tim dan jumlah puas dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pembangunannya;
 - 4) Gambar, peta dan data tentang situasi dan keadaan pergerakan dan/atau instalasi militer;
 - 5) Data perkiraan jumlah puas 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 perintah militer negara; dan/atau
 - 7) Sistem intelligen negara.
- d. Informasi Publik yang spesial dibuka dan diberikan kepada Pemohon: Informasi Publik dapat mengungkapkan kekayaan alam Indonesia;

- c. Informasi Publik yang wajib dibuka dan diberikan kepada Pemohon Informasi Publik, dapat mengakibatkan ketidakamanan ekonomi negara (a):
- 1) Rencana awal pembelian dan penjualan mata uang nasional atau asing, sebanding atau nilai tukar, suku bunga, dan model operasi institusi keuangan;
 - 2) Rencana awal perubahan suku bunga bank, program pemeringkatan, perubahan pajak, tarif, atau pendapatan negara/daerah lainnya;
 - 3) Rencana awal penjualan atau pembelian tanah atau properti;
 - 4) Rencana awal investasi asing;
 - 5) Proses dan hasil penggunaan perbankan, sektorini, atau sektor keuangan lainnya; dan/atau
 - 6) Hal-hal yang berkaitan dengan proses pencetakan uang.
- f. Informasi Publik yang wajib dibuka dan diberikan kepada Pemohon Informasi Publik, dapat mengakibatkan kepentingan hubungan luar negeri:
- 1) Politik, daya tawar dan strategi yang akan dan telah diambil oleh negara dalam hubungannya dengan negara-negara internasional;
 - 2) Korespondensi diplomatik antarnegara;
 - 3) Situasi korutuksion dan persaudaraan yang diperlukan akhir dalam menjalankan hubungan internasional; dan/atau
 - 4) Perilaku dan pengamanan Infrastruktur strategis Indonesia di luar negeri.
- g. Informasi Publik yang wajib dibuka dapat mengungkapkan isi aktivitas yang bersifat pribadi dan komunikasi berulang seputar waktu tersebut;
- h. Informasi Publik yang wajib dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkap rahasia pribadi, yaitu:
- 1) Alamat dan kontak anggota keluarga;

- 2) Riwayat, kondisi dan perawatan, pengabutan keseksualan fisik, dan pasca sesoring;
 - 3) Kondisi keuangan, aset, pendapatan, dan rekening bank sesoring;
 - 4) Hasil-hasil evaluasi solubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan sesoring;
 - 5) Catatan yang menyangkut pribadi sesoring yang bercahaya dengan kegiatan selain pendidikan formal dan sebuah pendidikan nonformal;
- c. Memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang memuat sifatnya diaksesinya kecuali atas putusan Komisi Informasi atau pengambilan.
- 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 37 :
- (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 ciri-ciri yang melanggar ketentuan;
 - (2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentranmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memihkam atau menghinaan dan/atau penyebarluasan nama baik;
 - (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 ciri-ciri penghinaan dan/atau penyebarluasan nama baik;
 - (4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat

disksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki tujuan penerapan dan/atau pengamanan.

Pasal 129 :

"Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi Elektronik dan/atau dokumen elektronik yang berisi ucapan kejemuhan atau ancaman-nakut-nakut yang ditujukan secara prima."

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 intenciyas, tujuan bahwa melampauinya atau menjebol sistem perigardian.

Pasal 31 :

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atau 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 atau 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 pengheretan

informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

- (3) Kecuali ketepatan sebagaimana dimaksud pada ayat (1) dan ayat (2), intempsi yang dilakukan dalam rangka penegakan hukum atau permintaan kejatuhan, kejaksaan, dan/atau institusi penegak hukum lainnya yang dilimpahkan berdasarkan undang-undang.
- (4) Ketentuan lebih lanjut mengenai tata cara intempsi 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, memisahkan, meramaikan, merusak, menghilangkan, memindahkannya, menyembunyikannya 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 memindahkannya atau mentransfer informasi elektronik dan/atau dokumen elektronik ke dalam sistem elektronik orang lain yang tidak berhak.
- (3) Terhadap perturunan sebagaimana dimaksud pada ayat (1) yang menggunakan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia mengakibatinya dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 35 :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukannya 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 mengalihkan korupsi bagi orang lain."

Pasal 37 :

"Setiap orang dengan sengaja menciptakan 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 memungkinkan unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi"

5. Pasal 7, Pasal 8, Pasal 168, Pasal 169, Pasal 169 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 risikonya dan pengobatan yang telah dipimpin yang akan diberikan oleh tenaga kesehatan."

Pasal 168 :

- (1) Untuk menyelenggarakan upaya kesehatan yang efektif dan efisien dipertuliskan infomasi kesehatan.
- (2) Informasi kesehatan sebagaimana dimaksud pada ayat (1) dibuktikan melalui sistem informasi dari melalui instansi sektor.
- (3) Keterbitan lebih lanjut mengenai sistem informasi edukasi kesehatan 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 170 ayat (2):

- (2) Penyidik sebagaimana dimaksud pada ayat (1) berwajib:
- a. melakukan pemeriksaan atau kebenaran laporan serta keterangan tentang tindak pidana di bidang kesehatan;
 - b. melakukan penemuan tetap orang yang diduga melakukannya 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 atau surat dan/atau dokumen lain tentang tindak pidana di bidang kesehatan;
 - e. melakukan pemeriksaan atau penyidikan bahan atau bukti dalam perkara tindak pidana di bidang kesehatan;
 - f. membuat perintah ahli dalam rangka pelaksanaan tugas penyidikan tindak pidana di bidang kesehatan;
 - g. menghentikan penyidikan apabila tidak terselipnya 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) ditentukan Peraturan Pemerintah

Pasal 20 :

"Setiap penyelenggara telekomunikasi wajib mematuhi prinsip pengriman, penyiaran, dan penyampaian informasi penting menyangkut:

- a. Keamanan negara;
- b. Keselamatan jiwa manusia dan harta benda;
- c. Berita a alam ;
- d. Murbabahayu, dan atau
- e. Wabah penyakit.

Pasal 40 :

"Setiap orang dilarang melakukan kegiatan penyidikan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."

Pasal 41 :

"Dalam rangka pembuktian kebenaran pemakaian fasilitas telekomunikasi atau pertimbangan pengguna jasa telekomunikasi, penyelenggara jasa telekomunikasi wajib melakukan kegiatan perikmanan pemakaian fasilitas telekomunikasi milik yang dilakukan oleh pengguna jasa telekomunikasi dan dapat melakukan penilaian tentang informasi sesuai dengan peraturan perundang- undangan yang berlaku".

Pasal 42 :

- (1) Penyelenggara jasa telekomunikasi wajib memahasiikan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jasa telekomunikasi dan atau jasa telekomunikasi yang diakruggarakaranya.
- (2) Untuk keperluan proses pidana, penyelenggara jasa telekomunikasi dapat memberikan informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi yang diperlukan atau:
 - a. Permintaan tertulis Jaksas Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu;

- b. Perintah penyidik untuk tidak pidana torrent sejuni dengan Undang-Undang yang berlaku.
- (3) Ketentuan mengenai tata cara perintah dan pemberian rekomendasi informasi sebagaimana diwakili pada ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 43:

"Pemberian rekomendasi informasi oleh penyelenggara jasa telekomunikasi kepada pengguna jasa telekomunikasi sebagaimana dimaksud dalam Pasal 4) dan untuk kepentingan proses penyelesaian perdamaian 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 12 :

"Lingkup perlindungan Rahasia Dagang meliputi negosiasi produksi, metode pengolahan, metode penjualan, atau informasi lain di bidang teknologi dan/atau bantuan 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 diperlukan kerahasiaannya melalui ketuntasan dan ketetapan menggunakannya.
- 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 nilai 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 mengungkapnya telah melakukan langkah-langkah yang bijak dan patut.

B. Analisis Fungsi Unit Kerja dalam Organisasi dan Job Description

Selain melakukam identifikasi terhadap ketentuan hukum yang menjadi bahan pertimbangan dalam pembuatan klasifikasi keramuan dan penentuan hak akim arsip dinamis, langkah selanjutnya adalah melakukam 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 berdasarap unit kerja yang menjalankan fungsi substantif maupun fungsional dengan tujuan untuk memenuhi fungsi strategis dalam organisasi. Fungsi substantif atau utama adalah kelompok kegiatan utama suatu organisasi sejauh dengan urusan penyelenggaraan perwakilan. Fungsi fungsional adalah kelompok kegiatan pendukung yang terlibat 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 Pemerintah Kota Makassar terdapat Badan Kepegawaian; Dsnak. Salah satu fungsi Badan Kepegawaian Daerah adalah di bidang pengelolaan karana pertahanan. Kegiatan yang tercipta dari fungsi pengelolaan karana pertahanan antara lain pengedaran jasa konstruksi dan sarana pertahanan, sertifikasi kelalkatan, kodefikasi materil, dan pengelolaan aset/barang milik negara di bidang pertahanan. Untuk kegiatan jasa konstruksi dan sarana pertahanan, contoh arsip yang dihasilkan adalah keterangan saku cadang peralatan pertahanan dari dalam maupun luar negeri. Berdasarkan analisis fungsi, arsip dari kegiatan tersebut dapat dipergunakan 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 geologis) yang terdapat di suatu wilayah di Indonesia, seperti migas, pasca bumi, mineral dan air tanah, serta potensi geologi lainnya. Dalam melaksanakan tugas tersebut, Badan Geologi mempunyai kegiatan pemetaan terhadap potensi sumber daya geologis. 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 kogilatannya belum mempunyai nilai strategis bagi negara.
- c. Salah satu unit organik di lingkungan Kementerian Kostruktasi dan Informatika adalah Direktorat Jenderal Aplikasi Informatika. Salah satu fungsi Direktorat Jenderal Aplikasi Informatika adalah menjaga kerumunan informasi. Arsip yang dimiliki dari fungsi tersebut antara lain arsip yang berhubungan dengan daftar situs di internet tetapi dengan jaringan berbasis Solo yang harus diblok sehingga arsip yang tersimpan dari fungsi tersebut dapat dipertimbangkan sebagai arsip rahasia, karena kegiatan tersebut terkait dengan kerumunan data dan analisis. Fungsi dari unit kerja dalam organisasi dapat digunakan dalam bagian sebagai berikut:

Tabel 1. Contoh Analisis Fungsi Unit Kerja Dalam Organisasi

No.	Unit Kerja	Fungsi	Kegiatan	Arsip Tersipat	Keterangan
1.	Badan Sensus Pertanahan Kependidikan Penelitian dan Inovasi	Melaksanakan pengelolaan, monitoring dan evaluasi	1. Pengelolaan jasa konservasi & infrastruktur pertanian 2. Berifikasi keabsahan & kelayakan Maret 3. Pengelolaan esa/batas nella negara di tidak pertambahan	Arsip tentang konservasi sela dan pertambahan pertanian	Diperlukan revisi
2.	Badan Geologi, Konservasi Energi dan Rambu Daerah Mineral	Mengelola potensi geosumber umber daya alam yang terdapat di suatu wilayah di Indonesia	1. Penetapan ruang 2. Penetapan pemanfaatan 3. Penyelenggaran 4. Pengelolaan ruang	Arsip terdiri ang ruang, batas, Jumlah penduduk berwira peta wilayah Lahan	Diperlukan revisi
3.	Guru besar Jenderal Aplikasi Informasi, Netizen Komunikasi dan Inovasi	Mengelola keamanan informasi	Membuktikan situs yang bersifat dengan SARA, Porno, dan yang berpot ensi mengganggu keamanan negara	Arsip yang berhubungan dengan dolar sebut internet yang berbahaya jaringan teknologi yang harus dihindari	Diperlukan revisi

Ciri-ciri 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 penyuluhan personal fiduciataranya & meliputi disiplin pegawai, DPD, dan lain-lain. Aksi yang tercipta dari kegiatan ini dapat dipertimbangkan sebagai upaya reaksi karena mempunyai nilai bagi individu pegawai yang beranggutan dan dapat menimbulkan kerugian yang serius terhadap masalah privacy.
- b. Unit keuangan dalam rangka melaksanakan salah satu fungsi yaitu pengelolaan pertendaharaan, diantaranya melakukan kegiatan administrasi pembayaran gaji. Aksi yang dilakukan diantaranya adalah daftar gaji, daftar potongan gaji pegawai, dan lain-lain yang dapat dipertimbangkan aksi reaksi 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 sifat-sifat daya manusia sebagai penanggung jawab dan pengelola dalam analisis job description. Job description (uraian jabatan) adalah suatu catatan yang sistematis tentang tugas dan tanggung jawab suatu jabatan tertentu, yang dimulai berdasarkan fungsi sebagaimana yang terdapat dalam struktur organisasi.

Uraian Jabatan berbentuk dilihat informal yang berisi ringkasan tentang suatu jabatan untuk membedakannya 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 penyelesaian sumber daya manusia dalam suatu organisasi, dimana suatu jabatan dijelaskan dan diberikan detailan.

Hal-hal yang harus diperhatikan dalam Uraian Jabatan meliputi:

- a. Identifikasi Jabatan, berisi informasi tentang nature jabatan dan bagaimana dala suatu organisasi;

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

Penyusunan uraian jabatan harus dilakukan dengan baik agar tidak diabaikan, untuk itu diperlukan suatu proses terstruktur, yang diketahui dimulai dengan analisis jabatan.

Analisis jabatan adalah proses untuk memahami struktur jabatan dan kinerjanya menganggotainya ke dalam format agar orang lain mengerti tentang suatu jabatan. Prinsip pending 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 dinilai adalah jabatan, bukan pemegang jabatan.
- c. Kondisi jabatan yang dinilai dan dituangkan dalam uraian jabatan adalah kondisi jabatan pada saat dinilai berdasarkan rancangan strategi dan struktur organisasi.

Dari analisis jabatan, dapat dilihat pejabat yang mempunyai wewenang dan tanggung jawab terhadap tingkat/derajat klasifikasi keleluasaan dan mempunyai hak akses arsip dinamis. Untuk itu, dapat digolongkan personil tertentu yang diberi wewenang dan tanggung jawab dalam pertimbangan, pengelolaan, pengiklanan keamanan informasi dan diberi hak akses arsip dinamis. Pengelolongan personil untuk menjamin perlindungan pengamanan informasi dan mempunyai hak akses arsip dinamis terdiri dari penentuan kebijakan, polisikana, dan peraturan. Tanggung jawab tersebut, dapat diuraikan sebagai berikut:

- a. Penentuan kebijakan, meliputi tanggungjawab :
 - i) Memerlukan tingkat/derajat klasifikasi keleluasaan dan hak akses arsip dinamis;
 - ii) 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) Menunjukkan kebijakan, dasar pertimbangan, dan sumber daya manusia yang bertanggung jawab dalam suatu pedoman/petunjuk pelaksanaan, atau petunjuk teknis.

b. Pelaksana kebijakan meliputi tanggungjawab :

- 1) Memahami dan menerapkan klasifikasi keamanan dan hak akses arsip dinamis sesuai dengan kewenangan yang sudah dimungkinkan;
- 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 undukan penyimpangan dan pelanggaran;
- 5) Menjamin bahwa implementasi tingkat klasifikasi keamanan dan hak akses arsip dinamis telah dilaksanakan 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 mempertahani hak akses arsip dinamis telah dilindungi dari kerusakan fisik dan dari akses, perubahan, serta pemindahan legal berdasarkan standar resmi di RI ;
- 7) Mengidentifikasi semua kebutuhan dalam rangka menjaga keamanan informasi dan hak akses arsip dinamis yang tersimpan dalam arsip yang telah diklasifikasikan keamanannya.

c. Pedoman

- 1) Menindaklanjuti pelanggaran dan penyimpangan yang ditemukan; dan
- 2) Melakukan semua dugaan pelanggaran dan penyimpangan kepada penentu kebijakan

Catatan pengujian pekerja 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 kelembagaan ke luar dari lembaga dalam instansi seperti pada Instansi pemerintah pusat dan pemerintah daerah atau sejauh 3 pada instansi setingkat Balai/UPT/Kantor,

- b. Petahanaan kebijakan adalah pejabat pada unit kerja yang mendeklarasikan fungsi dan tugas organisasi seiringan 3 dan 4, seperti: Kepala Bidang/Kepala Bagian, Kepala Sub Bidang/Kepala Sub Bagian/Kepala Seksi;
- 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 pengklasifikasiannya dan hal-hal akibat arsip diwajibkan secara 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 ketertiban dan peralihan pertahanan, seperti misalnya pembelian pesawat tempur dari luar negeri dan pembelian senjata. Setelah dilakukan analisis risiko, hasil analisis menjadi sifat-sifat:

- 1) Jika arsip tentang pembelian pesawat tempur 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, keruangan 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 pengeksploitasi potensi kerugian negara oleh pihak yang tidak bertanggung jawab.
- 2) Bila arsip ditutup kemungkinan hal-hal 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 pematu kebijakan.

c. Arsip rencana tata kota.

- 1) Bila arsip dirahasiakan, maka kemungkinan risiko yang akan timbul adalah disalahgunakan oleh pihak yang berwawancara maupun tidak ada kontrol dari masyarakat.
- 2) Bila arsip diketahui oleh publik maka ada kontrol dan komisi, sehingga lebih baik dikategorikan sebagai arsip biasa dan dapat dikenai oleh masyarakat.

4. Penentuan Kategori Klasifikasi Keamanan

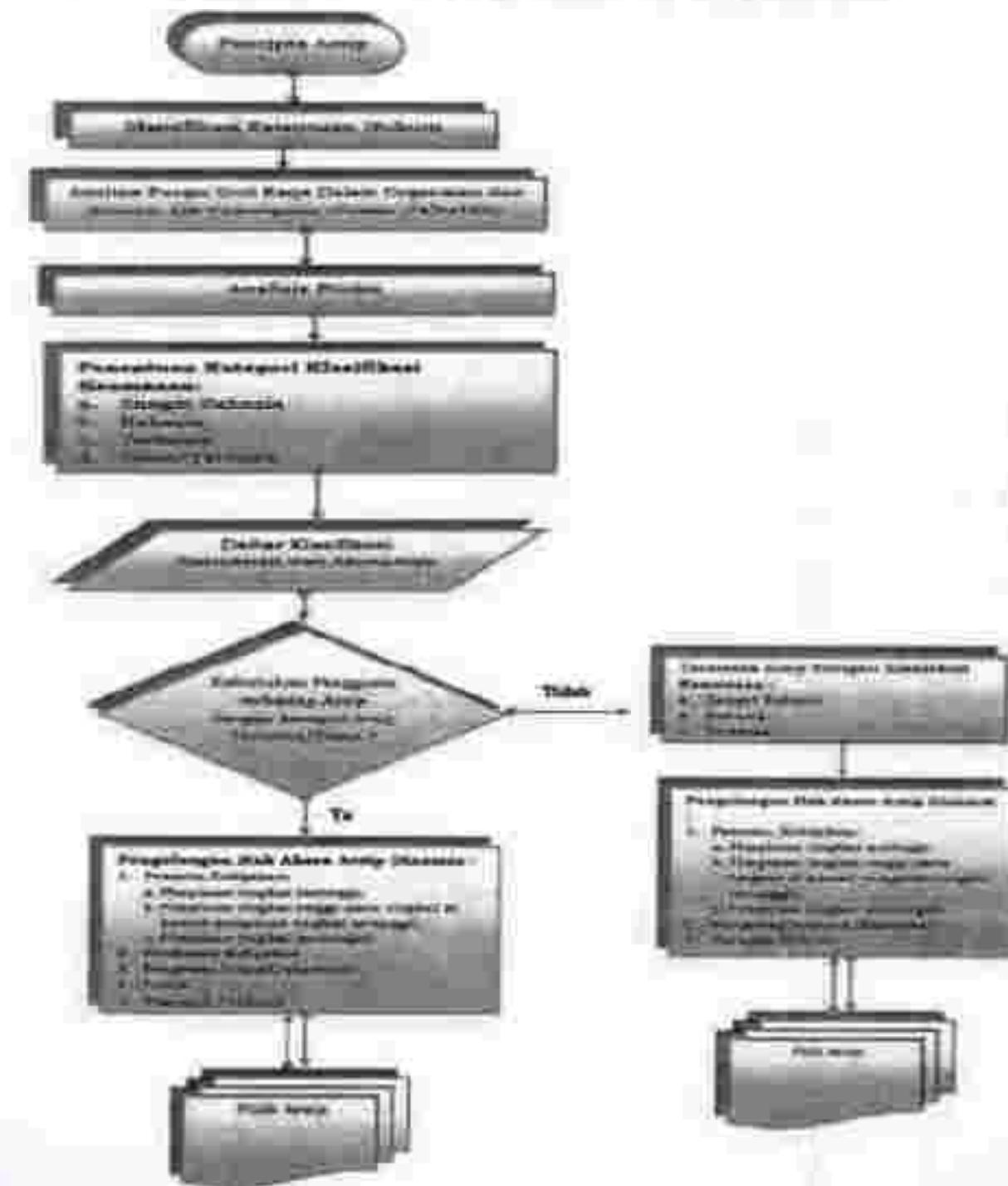
Berdasarkan identifikasi ketentuan hukum, analisis fungsi unit kerja dalam organisasi dan job description serta analisis risiko, dapat ditentukan kategori klasifikasi keamanan, yaitu:

- a. Sangat Rahasia apabila diketahui oleh pihak yang tidak berhak dapat membahayakan kestabilitan negara, ketertiban wilayah Negara Kesatuan Republik Indonesia, dan kesadaran bangsa;
- b. Rahasia apabila diketahui oleh pihak yang tidak berhak dapat menggalakan terganggunya fungsi penyelenggaraan negara, sumber daya nasional, ketertiban umum, termasuk dampak ekonomi makro. Apabila informasi yang terdapat dalam arsip bersifat berulang bagi lembaga/organisasi akan meningkatkan kerugian yang sejauh terhadap privasi, keuntungan komersial, hilangnya kiprah/dukungan serta merusak kredibilitas dan reputasi;
- c. Terbatas apabila diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya pelaksanaan tugas dan tugas lembaga pemerintahan seperti kerugian finansial yang signifikan;

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

Penerapan kecuali tingkat klasifikasi keamanan tersebut ditentukan dengan kepentingan dan kondisi setiap lembaga. Di suatu lembaga, dimungkinkan untuk membuat sekitar 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 kesiapan sebagai berikut dalam BAB IV.

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



5. Pengalokasian Hak Akses Arsip Dinas

Bantuan kerja identifikasi ketentuan hak akses, analisa fungsi unit kerja dalam organisasi, analisis job description, analisis risiko, dan penentuan kategori klasifikasi keamanan, dapat ditentukan pengalokasian pengguna yang berhak mengakses terhadap arsip dinas, yaitu:

a. Pengguna yang berhak di lingkungan internal instansi

- 1) Pemimpin 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, dengan ketentuan sebagai berikut:
 - a) 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 pimpinan tingkat tinggi, dan yang satu tingkat dengan unit di luar unit kerjanya kecuali telah mendapatkan izin.
 - b) Pimpinan tingkat menengah (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 pimpinan tingkat tinggi, dan yang satu tingkat dengan unit di luar unit kerjanya kecuali telah mendapatkan izin.
 - b) Pelaksana ketujuhan 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 memperoleh izin.
 - c) Petugas internal mempunyai kewenangan untuk mengakses seluruh arsip pada posisi ta arsip dalam rangka melaksanakan fungsi pengawasan internal tetapi dengan ketentuan peraturan

perundang-undangan, seperti pengawasan yang dilakukan oleh Lembaga Audit Pemerintah dan Satuan Pengawas Internal (SPI).

b. Pengguna yang berhak di lakukan eksternal internal

- 1) Publik mempunyai hak untuk mengakses sebarang arsip dalam kategori biasa/terbatas.
- 2) Pengawas eksternal mempunyai hak untuk mengakses seluruh arsip pada pencipta arsip dalam rangka melaksanakan fungsi pengawasan eksternal termasuk dengan ketentuan peraturan perundang-undangan, seperti pengawasan yang dilakukan oleh Badan Pemeriksa Keuangan (BPK), Badan Pengawas Keuangan Pembangunan (BPKP), Inspektorat Daerah Provinsi dan Kota.
- 3) Aparat penegak hukum mempunyai hak untuk mengakses arsip pada pencipta arsip yang terkait dengan pedoman atau proses hukum yang sedang ditangani dalam rangka melaksanakan fungsi pengakses hukum.

Dalam rangka pelaksanaan klasifikasi keamanan dan akses arsip dinas, pengguna yang berhak untuk mengakses arsip dinas sebagai berikut:

Tabel 2. Pengguna yang berhak akses arsip dinamis

No.	Kategori Klasifikasi Keamanan dan Akses	Pemohon Kebijakan	Pelaksana Kebijakan	Pengawas Internal/Eksternal	Pihak	Pengakses Hukum
1.	Biasa/Terbatas	V	V	V	V	V
2.	Terbatas	V	-	V	-	V
3.	Rahasia	V	-	V	-	V
4.	Sangat Rahasia	V	-	V	-	V

Keterangan Tabel 2:

- a. Arsip Berklasifikasi Sangat Rahasia, hak akses diberikan kepada pimpinan tertinggi kebagia dan yang seingkat di bawahnya apabila sudah diberikan ijin, pengawas internal/eksternal dan pengakses hukum

- b. Arsip Berklasifikasi Rahasia, hak akses diberikan kepada pimpinan tingkat tinggi dan setingkat di bawahnya apabila sudah dilakukan tindak pengawas internal/eksternal dan penegak hukum
- c. Arsip Berklasifikasi Terbatas, hak akses diberikan kepada pimpinan tingkat menengah dan setingkat di bawahnya apabila sudah dilakukan tindak pengawas internal/eksternal dan penegak hukum
- d. Arsip Berklasifikasi Biasa/Terbuka, hak akses diberikan kepada semua tingkat pejabat dan staf yang berperan tinggi.

6. Pengamanan Tingkat Klasifikasi

Berdasarkan tingkat Klasifikasi Keamanan dan Akses Arsip Dinamis, makas konsepsi arsip mengacu ketentuan peraturan perundang-undangan melakukannya pengamanan fisik arsip dinamis maupun informasinya sesuai dengan tingkat klasifikasi, antara lain dalam penyimpanan dan peryampahtan sebagai berikut:

1. Penyimpanan

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

Tabel 3. Tabel Pengembanan Analip Dinamis Sensus Dengan Tingkat Klasifikasi Kelemanan

No KLAUSIFIKASI KELEMANAN	TINGKAT ANALIP	ANALIP TEORIAL		MEDIA ANALIP	ANALIP EKSPRESI	PRIMARIA & BURNIN
		Analip Pengaman	Analip Kesadaran			
1 Dalam/ Terbatas	1 Tidak ada perangaman dan procedur kritis	Pengaman yang berasal dari dokumentasi lalu internal yang memungkinkan dilakukan	Tidak diketahui ataupun praktisnya data yang dikenal mengenai sifat-sifat data	1. Back-up secara regular untuk tujuan pemuliharaan, aman dalam rangka memenuhi standarisasi analip	Analip yang berasal dari internal dan externa dari sistem dapat menyebabkan kesalahan	Analip pertama yang berasal dari internal dan eksternal serta memungkinkan dilakukan
2 Terbatas	2 Analip dan perangaman dilakukan dalam/ TERBATAS pada data yang	Diketahui data yang perangaman yang aman	1. Back-up secara regular untuk tujuan pemuliharaan, aman dalam rangka memenuhi standarisasi analip 2. File file elektronik (termasuk database) harus dilakukan kebutuhan perangaman internal atau tidak memungkinkan dilakukan	1. Automatisasi perangaman berdasar perintah/ proses untuk ID digital 2. Pengecekan tanda bagi hasil analip komunikasi 3. Perangaman data sistem dilakukan perangaman dokumentasi dilakukan	Analip pertama yang berasal dari internal dan eksternal dapat menyebabkan kesalahan	Analip pertama yang berasal dari internal dan eksternal dapat menyebabkan kesalahan

No	JENIS KELAMAHAN	AKIBAT	AKIBAT KELAMAHAN		ALIRI ELEKTRONIK	PRINSIP & KONSEP
			Prinsip	Konsep		
1	Rahasia	1. Ada penyalahgunaan dan pencurian rahasia dengan memindahkan "data rahasia" pada sistem komputer.	1. Objek harus untuk memiliki kebutuhan yang tertentu	1. Lokasi dengan alamat yang terbatas	1. Kartu atau jangkauan yang tidak dijangkau oleh komputer atau sistem operasi dan sistem yang dapat mengaksesnya	1. Langkah-langkah krusial dengan Operating System bahwa sistem aplikasi dilakukan secara bertahap.
2	Rahasia	2. File dibuang (terminasi delapan karakter dilanjutkan dengan penghapusan file internal atau oleh pihak ketiga)	2. File-file dibuang (terminasi delapan karakter dilanjutkan dengan penghapusan file internal atau oleh pihak ketiga)	2. Automatis penghapusan/jantur	2. Perintah erat ketika sistem dijalankan dan prosedur dan verifikasi intinya. Perintah ini akan dijalankan secara otomatis.	2. Langkah-langkah krusial dengan Operating System bahwa sistem aplikasi dilakukan secara bertahap.
3	Rahasia	3. Pengalihan untuk ke peretasan tradisional	3. Pengalihan untuk ke peretasan digital	3. Komputer atau perangkat lain yang dilakukan dengan berjaringan dan akhirnya berhasil melakukan komunikasi dengan sistem	3. Perintah erat ketika sistem dijalankan dan prosedur dan verifikasi intinya. Perintah ini akan dijalankan secara otomatis.	3. Langkah-langkah krusial dengan Operating System bahwa sistem aplikasi dilakukan secara bertahap.

Surat Salinan	Alk dant mhsan dengar memperbaiki “BANTU RAKYAT” Perpustakaan pada halaman	Diketahui bahwa untuk pertama kali, dengan pengamanan, dan Perpustakaan, dikenakan penalti sanksi dalam rangka menjaga 1. Penanggung kerugian “Bantuan Rakyat”
		1. Bantuan dibuat berdasarkan surat penalti sanksi dalam rangka menjaga 2. Penanggung kerugian “Bantuan Rakyat”
		1. Autentikasi penerima (namun pembuat/pemohon tidak diidentifikasi) 2. Penanggung kerugian dibuat dalam rangka menjaga 3. Autentikasi server 2. Lembaran, lampiran kesepakatan dengan Operasional Operasional klarifikasi atau klarifikasi Hormat kelembagaan lulus, ditandatangani berikut: perintah menulis titik pada garis

Catatan

Kemudian terdapat back up media arsip elektronik yang berlaku pada setiap lembaran salinan dan terdapat ketentuan tentang back up media arsip elektronik yang berlaku pada arsip dokumentasi tributus dengan metode back up yang valid dengan tingkat klasifikasi kerahasiaan.

2. Pengiriman

Persiapan dalam rangka penanganan file merupakan 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 KONVENTIONAL	ARsip ELEkTRONIK
1. Birokratik/Tertutup	Tidak ada persyaratan pengetahuan teknis.	Tidak ada pengetahuan teknis.
2. Terbatas	Amplop sempit.	Ayolah pesan elektronik atau email berisi data tertulis yg informasi penerima belum mampu memahami maknanya, misalnya yang dikirim dengan akronimik, glosariorum dan lain-lain.
3. Publik	<ol style="list-style-type: none"> 1. Menggunakan wacana kerjas yang berbeda 2. Diberi kode rahasia 3. Menggunakan ampirup dobel 4. Menggunakan singkatan teknis 5. Koefisien tanda terima 6. Harus diinformasikan orang yang sudah diberi wewenang dan tanggungjawab untuk terima pesan lalu nantinya pengirim akan resipit/dokumentasi bahwa 	<ol style="list-style-type: none"> 1. Harus ada konfirmasi dari penerima pesan elektronik atau email. 2. Menggunakan perangkat yang dilengkapi sistem bagi pesan elektronik atau email rahasia. 3. Menggunakan pesan yang dituliskan dengan kriptografi.
4. Simpat Pihak-pihak	<ol style="list-style-type: none"> 1. Menggunakan wacana kerjas yang berbeda 2. Menggunakan ampirup dobel berwrgi 3. Aturan jasak untuk setiap teknologi dan teknologi berikutnya 4. Harus diketahui makna orang yang sudah diberi wewenang dan tanggungjawab pengirim lalu nantinya pengirim akan resipit/dokumentasi bahwa 	<ol style="list-style-type: none"> 1. Harus ada konfirmasi dari penerima pesan elektronik atau email. 2. Menggunakan perangkat yang dilengkapi sistem bagi pesan elektronik atau email rahasia. 3. Menggunakan pesan yang dituliskan dengan kriptografi 4. Harus ada prilaku dan siklus informasi untuk mewujudkan arsip elektronik atau email.

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

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 daar pertimbangan, dan unit pengolah. Rincian lebih lanjut sebagai berikut:

Daftar Arsip Dinamis Berdasarkan Klasifikasi Keamanan dan Akses Arsip Dinamis

No	Kode Klasifikasi	Jenis Arsip	Klasifikasi Keamanan	Hak Akses	Dasar Pertimbangan	Unit Pengolah
1						

Pengesahan:

Tempat, tanggal, bulan, tahun:

Jabatan:

Tanda tangan pejabat yang mengesahkan:

Nama:

Keterangan:

1. Kolom "Nomor", dituliskan dengan huruf urut;
2. Kolom "Kode Klasifikasi", dituliskan dengan kode angka, huruf atau gabungan angka dan huruf yang akan berguna untuk mengintegrasikan antara pendokumen, penyimpanan, dan penyusunan arsip dalam satu kode yang sertai sehingga memudahkan pengolahan;
3. Kolom "Jenis Arsip" dituliskan dengan judul dan urutan singkat yang menggambarkan isi dari jenis/seri arsip;
4. Kolom "Klasifikasi Keamanan", dituliskan tingkat keamanan dari masing-masing jenis/seri arsip yaitu sangat rahasia, rahasia, terbatas atau buka/terbuka;
5. Kolom "Hak Akses", dituliskan nama jabatan yang dapat melakukan pengaksesan terhadap arsip berdasarkan tingkat/derajat klasifikasi;

6. Kolom dasar pertimbangan, diisi dengan uraian yang menunjukkan daftar pengkategorian arsip sebagai sangat rahasia, rahasia dan terbatas;
7. Kolom unit pengolah, diisi dengan uraian yang bertanggung jawab terhadap kesesuaian dan kemanan fisik dan informasi arsip yang dikategorikan sebagai rahasia, rahasia dan terbatas.

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

Lengkapnya 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 dari Norma Standar Pedoman Kriteria masing-masing instansi;
- b. Kualitas dan fungsi unit kerja dan Job Description;
- c. Aspek amanah instansi;

2. Penentuan Klasifikasi Keamanan dan Hak Akses pada kolom daftar.

Hasil penentuan Klasifikasi Keamanan dan Hak Akses Arsip Dinamis pada penciptaan 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. Penentuan dasar pertimbangan.

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

4. Menentukan unit pengolah

Unit pengolah perlu dicantumkan dalam daftar gilia mengenai unit yang bertanggung jawab terhadap kesesuaian dan kemanan fisik dan informasi arsip yang dikategorikan sebagai 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 penciptaan arsip.