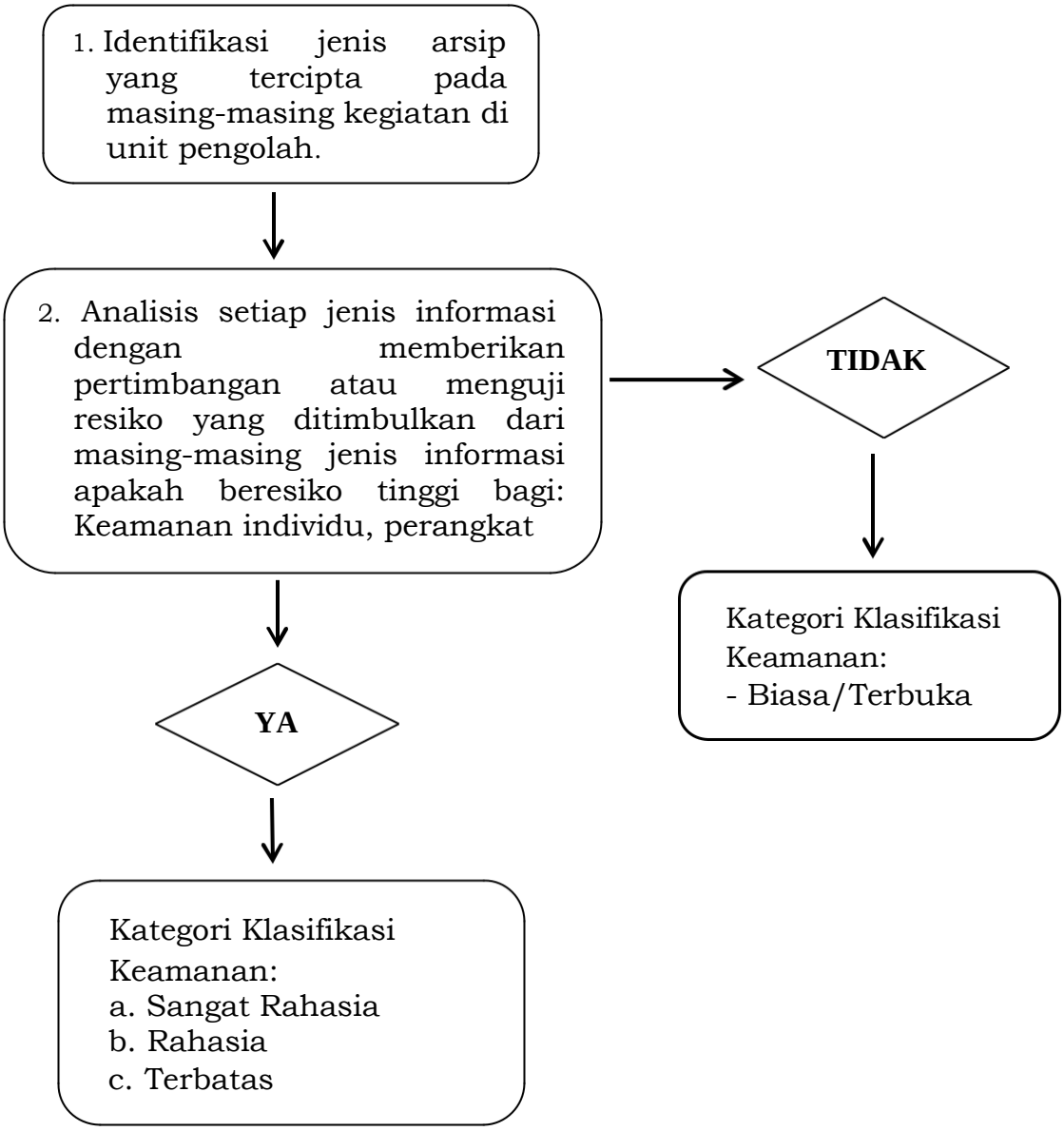
Lampiran Peraturan Walikota Batu
Nomor : 7 Tahun 2020
Tanggal : 17 Januari 2020

PEDOMAN PEMBUATAN SISTEM KLASIFIKASI KEAMANAN DAN HAK AKSES ARSIP DINAMIS DI LINGKUNGAN PEMERINTAH KOTA BATU

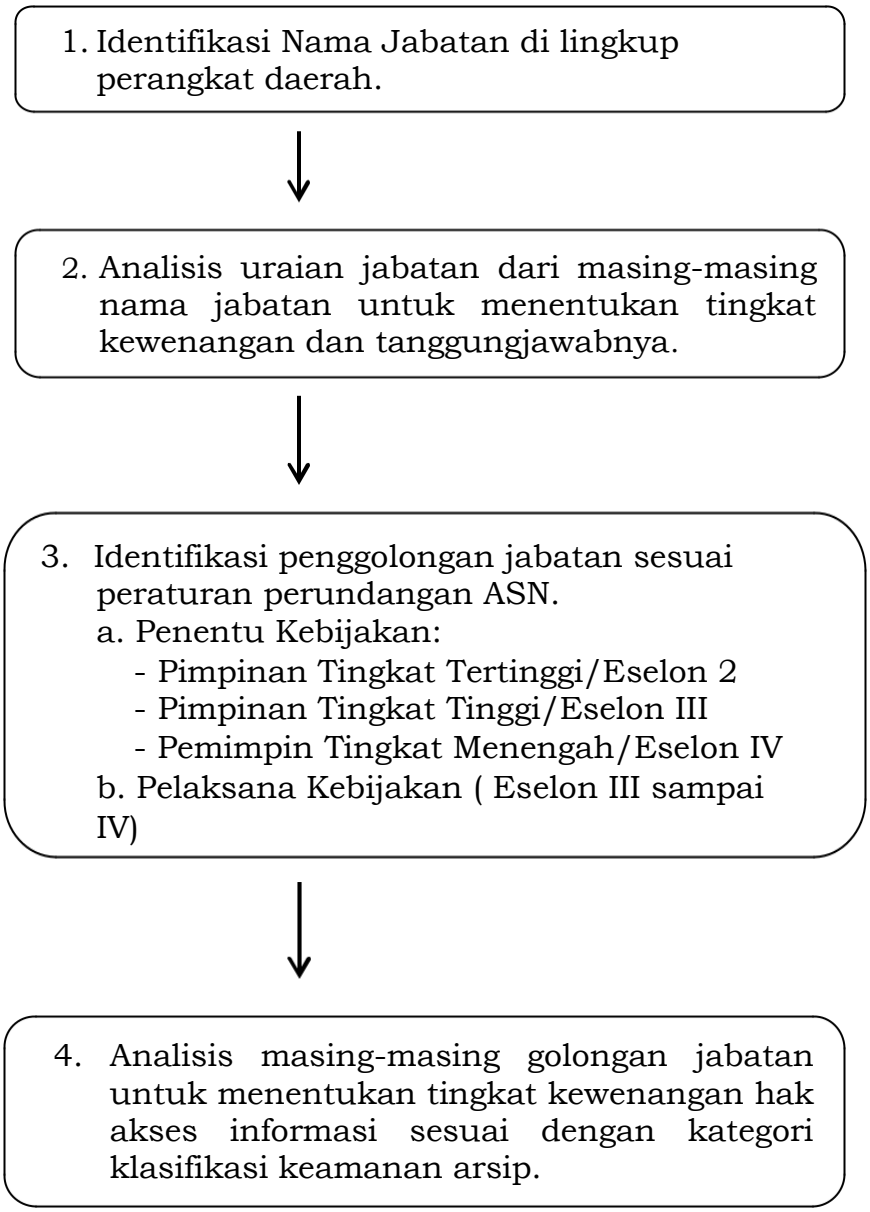
A. Prosedur melakukan Analisis Resiko Terhadap Jenis Informasi yang Tercipta/Dihasilkan



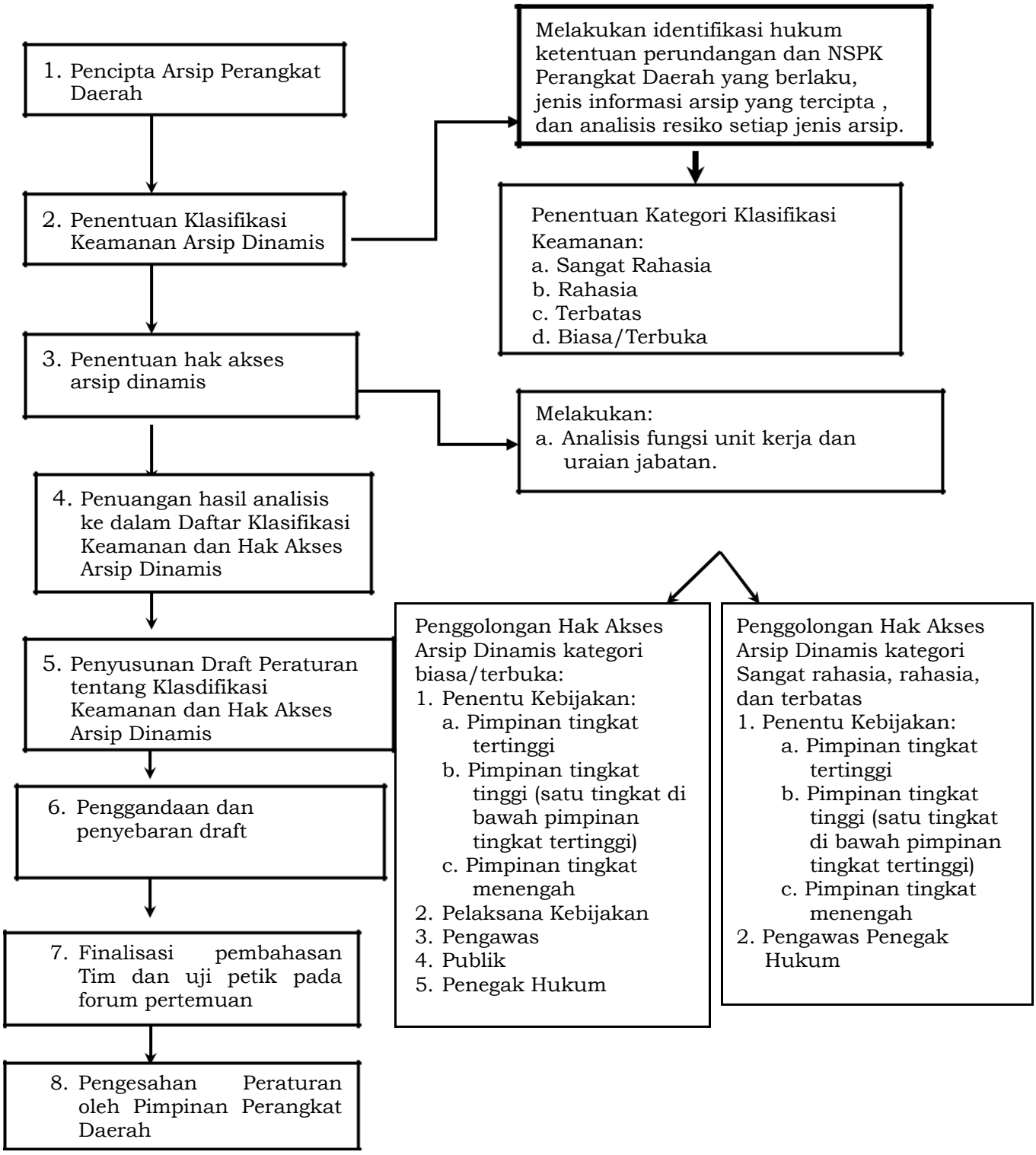
B. Hasil Analisis Resiko Terhadap Jenis Informasi Arsip Dinamis Perangkat Daerah

No.	Unit Kerja	Fungsi	Kegiatan	Arsip Tercipta	Keterangan
1.	Dinas Perpustakaan dan Kearsipan Provinsi Jawa Timur	Melaksanakan fungsi perpustakaan dan kearsipan	1. Pelayanan informasi perpustakaan	- Data koleksi arsip layanan - Data pengguna pustaka - Pengembangan minat baca - Perpustakaan digital - Otomasi perpustakaan	Dipertimbangkan terbatas Dipertimbangkan biasa/terbuka Dipertimbangan terbatas Dipertimbangkan terbatas Dipertimbangkan terbatas
			1. Akuisisi/pengadaan bahan pustaka 2. Pemeliharaan bahan pustaka 3. Lokal konten	- Data pengadaan buku - Statistik restorasi bahan pustaka - Distribusi bahan pustaka	Dipertimbangkan terbatas Dst Dst
			1. Pembinaan kearsipan	- Data lokus pembinaan - Pembinaan SDM kearsipan - Sertifikasi LKD/Unit Kearsipan/Arsiparis	Dipertimbangkan terbatas Dipertimbangkan terbatas Dipertimbangkan rahasia
			2. Pengawasan kearsipan	- Pengaawasan internal - Pengawasan eksternal - Publikasi pengawasan	Dipertimbangkan rahasia
			3. Pemasyarakatan kearsipan	dst	dst
			4. Penilaian Arsiparis	dst	dst

C. Prosedur Penentuan Hak Akses Arsip Dinamis oleh Pengguna Internal



D. Prosedur Penyusunan Klasifikasi Keamanan dan Hak Akses Arsip Dinamis



E. Format Daftar Klasifikasi Keamanan dan Hak Akses Arsip Dinamis

DAFTAR KLASIFIKASI KEAMANAN DAN HAK AKSES ARSIP DINAMIS

No.	Kode Klasifikasi	Jenis Arsip	Klasifikasi Keamanan	Hak Akses	Dasar Pertimbangan	Unit Pengolah
1	2	3	4	5	6	7

Disahkan di : .....
Pada tanggal : .....

KEPALA
PERANGKAT DAERAH

TTD

Nama Pejabat
Pangkat
NIP

Keterangan:

1 Kolom “Nomor” : Diisi dengan nomor urut;
2 Kolom “Kode Klasifikasi” : Diisi dengan kode klasifikasi yang berlaku di perangkat daerah;
3 Kolom “Jenis Arsip” : Diisi dengan uraian singkat yang menggambarkan isi dari jenis/seri arsip;
4 Kolom “Klasifikasi Keamanan” : Diisi dengan tingkat keamanan dari masing-masing jenis/seri arsip (sangat rahasia, rahasia, terbatas, atau biasa/terbuka);
5 Kolom “Hak Akses” : Diisi dengan nama jabatan yang dapat melakukan pengaksesan terhadap arsip, baik di lingkungan internal perangkat daerah maupun eksternal
6 Kolom “Dasar Pertimbangan” : Diisi dengan uraian yang menerangkan alasan kekategorian arsip sebagai sangat rahasia, rahasia, terbatas, dan terbuka.
7 Kolom “Unit Pengolah” : Diisi dengan nama unit kerja yang bertanggung jawab terhadap keselamatan, keamanan fisik, dan informasi arsip yang dikategorikan sangat rahasia, rahasia, dan terbatas.

F. Teknik dan Prosedur Penyampaian Informasi Arsip Dinamis Berdasarkan Klasifikasi Keamanan Arsip

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