GUBERNUR JAWA TENGAH

PERATURAN GUBERNUR JAWA TENGAH

NOMOR 12 TAHUN 2018

TENTANG

PENGELOLAAN DAN PERLINDUNGAN INFORMASI BERKLASIFIKASI
DI LINGKUNGAN PEMERINTAH PROVINSI JAWA TENGAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR JAWA TENGAH

Menimbang :

a. bahwa dalam rangka mencegah dimilikinya informasi berklasifikasi milik pemerintah oleh pihak tidak berwenang yang menyangkut keberlangsungan hidup bernegara, keutuhan dan ketentraman hidup masyarakat, perlu pedoman untuk mengelola informasi berklasifikasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan sesuai dengan ketentuan Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 Tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah perlu menetapkan Peraturan Gubernur Jawa Tengah tentang Pengelolaan Dan Perlindungan Informasi Berklasifikasi Milik Pemerintah;

Mengingat :

1. Undang-Undang Nomor 10 Tahun 1950 tentang Pembentukan Provinsi Jawa Tengah (Himpunan Peraturan-Peraturan Negara Tahun 1950 Nomor 86-92);
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 4843);
3. 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);
4. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
5. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071);

6. 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 beberapa kali 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);

7. 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 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);

8. Peraturan Pesiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100) sebagaimana telah diubah dengan Peraturan Pesiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Pesiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Nomor 277);

9. Peraturan Kepala Arsip Nasional Nomor 6 Tahun 2005 tentang Pedoman Perlindungan Arsip Vital;

10. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah;

11. Peraturan Kepala Arsip Nasional Nomor 13 Tahun 2015 tentang Pedoman Retensi Arsip Sektor Politik, Hukum, dan Keamanan Urusan Persandian;

12. Peraturan Gubernur Jawa Tengah Nomor 70 Tahun 2016 tentang Organisasi Dan Tata Kerja Dinas Komunikasi dan Informatika Provinsi Jawa Tengah;

13. Peraturan Gubernur Jawa Tengah Nomor 10 Tahun 2018 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintahan Provinsi;

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG PENGELOLAAN DAN PERLINDUNGAN INFORMASI BERKLASIFIKASI DI PROVINSI JAWA TENGAH.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan :

1. Daerah adalah Provinsi Jawa Tengah.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah otonom.
3. Gubernur adalah Gubernur Jawa Tengah.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Jawa Tengah.
5. Dinas adalah Dinas Komunikasi Dan Informatika Provinsi Jawa Tengah.
6. Kepala Dinas adalah Kepala Dinas Komunikasi Dan Informatika Provinsi Jawa Tengah.
7. Pengelolaan adalah suatu upaya, pekerjaan, kegiatan, dan tindakan yang meliputi pembuatan, pemberian label, pengiriman, dan penyimpanan.
8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
9. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic* data *interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
10. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
11. Informasi Non Elektronik adalah Informasi yang termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, dan simbol yang berupa suatu dokumen, kertas, dan bukti fisik lainnya.
12. Informasi berklasifikasi adalah informasi publik yang dikecualikan menurut peraturan perundang-undangan yang berlaku.
13. Instansi Pemerintah adalah kementerian negara, lembaga pemerintah non kementerian, sekretariat lembaga negara, dan pemerintah daerah.

14. Pengelola Informasi adalah Pejabat di dalam Instansi Pemerintah yang diberi kewenangan menangani dan/atau bertanggung jawab atas pengelolaan Informasi Berklasifikasi di lingkungan lembaganya berdasarkan standar, prosedur, dan ruang lingkup pengelolaan dan perlindungan Informasi Berklasifikasi.

15. Pemilik Informasi adalah pegawai maupun pejabat Instansi Pemerintah yang karena fungsi dan jabatannya bertanggung jawab atas semua data dan Informasi Berklasifikasi yang dihasilkan serta dikelola dan/atau dikumpulkannya selama bekerja dan atas nama instansinya.

16. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.

17. Konsep Informasi Berklasifikasi adalah rancangan atau buram surat dari Informasi Berklasifikasi.

18. Metadata adalah Informasi terstruktur yang mendeskripsikan, menjelaskan, menemukan, atau setidaknya membuat suatu informasi mudah untuk ditemukan kembali, digunakan, atau dikelola.

BAB II
MAKSUD, TUJUAN, SASARAN, ASAS DAN RUANG LINGKUP

Bagian Kesatu
Maksud

Pasal 2

Maksud ditetapkannya Peraturan Gubernur ini yaitu sebagai pedoman bagi Perangkat Daerah dalam mengelola dan melindungi informasi berklasifikasi di Provinsi Jawa Tengah.

Bagian Kedua
Tujuan

Pasal 3

Tujuan ditetapkannya Peraturan Gubernur ini yaitu agar mekanisme pengelolaan dan perlindungan informasi berklasifikasi di Provinsi Jawa Tengah berjalan secara aman, efektif, dan efisien serta terdapat keseragaman dalam pengelolaan dan perlindungannya.

Bagian Ketiga
Sasaran

Pasal 4

Sasaran ditetapkannya Peraturan Gubernur ini yaitu untuk mencegah terjadinya kebocoran infomasi berklasifikasi milik pemerintah melalui pengelolaan dan perlindungan informasi berklasifikasi secara utuh, efisien, efektif, dan akuntabel oleh setiap Perangkat Daerah guna mendukung terwujudnya keamanan nasional.

Bagian Keempat
Asas Dan Ruang Lingkup

Pasal 5

Asas Pengelolaan dan Perlindungan Informasi Berklasifikasi yaitu :

a. Asas Keamanan

   Pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah dilaksanakan dengan memperhatikan bahwa informasi tersebut hanya dapat diakses oleh orang yang berwenang, sekaligus menjamin kerahasiaan informasi yang dibuat, dikirim, dan disimpan.

b. Asas Keutuhan

   Pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah dilaksanakan dengan memastikan bahwa informasi tersebut tidak dapat diubah tanpa ijin dari pihak yang berwenang, menjamin keutuhan informasi dan tata kelolanya.

c. Asas Ketersediaan

   Pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah dilaksanakan untuk menjamin ketersediaan informasi tersebut saat dibutuhkan, dengan memperhatikan kewenangan pengguna informasi.

d. Asas Kecepatan dan Ketepatan

   Untuk mendukung kelancaran tugas dan fungsi unit kerja atau satuan organisasi, pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah harus dilakukan tepat waktu dan tepat sasaran.

e. Asas Efektif dan Efisien

   Pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah perlu dilakukan secara efektif dan efisien sesuai dengan klasifikasinya.

Pasal 6

Ruang lingkup ditetapkannya Peraturan Gubernur ini meliputi :

a. Pengelolaan Informasi Berklasifikasi Milik Pemerintah;
b. Perlindungan Informasi Berklasifikasi Milik Pemerintah;

Pasal 7

Pengelolaan dan perlindungan informasi berklasifikasi milik Pemerintah sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Pasal 8

Peraturan Gubernur Jawa Tengah ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur Jawa Tengah ini dengan penempatannya dalam Berita Daerah Provinsi Jawa Tengah.

Ditetapkan di Semarang
pada tanggal 6 Februari 2018

GUBERNUR JAWA TENGAH,

ttd

GANJAR PRANOWO

Diundangkan di Semarang
pada tanggal 6 Februari 2018

SEKRETARIS DAERAH PROVINSI
JAWA TENGAH,

ttd

SRI PURYONO KARTO SOEDARMO

BERITA DAERAH PROVINSI JAWA TENGAH TAHUN 2018 NOMOR 12

LAMPIRAN
PERATURAN GUBERNUR JAWA TENGAH
NOMOR 12 TAHUN 2018
TENTANG
PENGELOLAAN DAN PERLINDUNGAN
INFORMASI BERKLASIFIKASI DI
LINGKUNGAN PEMERINTAH PROVINSI
JAWA TENGAH

PENGELOLAAN DAN PERLINDUNGAN INFORMASI BERKLASIFIKASI DI LINGKUNGAN PEMERINTAH PROVINSI JAWA TENGAH

I. LATAR BELAKANG

Informasi merupakan aset penting bagi suatu organisasi. Setiap organisasi memiliki informasi kritis atau sensitif atau rahasia yang menjadikanya salah satu sumber daya strategis bagi kelangsungan hidup organisasi. Oleh karena itu, perlindungan terhadap informasi tersebut dari berbagai jenis ancaman yang dapat menyebabkan terjadinya kerugian organisasi merupakan hal yang mutlak yang harus diperhatikan baik oleh segenap jajaran pemilik, manajemen, maupun pegawai organisasi yang bersangkutan. Demikian pula informasi berklasifikasi di lingkungan instansi pemerintah, merupakan aset negara, perlu dikelola secara khusus untuk mencegah terjadinya kebocoran, baik sebagai akibat kelalaian sendiri maupun karena adanya ancaman pihak lain yang tidak memiliki otorisasi untuk memanfaatkan informasi yang dapat berdampak pada keberlangsungan hidup bernegara, keutuhan dan ketentraman hidup masyarakat.

Informasi yang dikelola dalam peraturan ini merupakan bagian dari informasi publik yang dikecualikan sebagaimana diatur dalam Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, informasi dimaksud telah ditetapkan sebagai informasi berklasifikasi oleh pimpinan instansi pemerintah. Tata kelola informasi berklasifikasi dilakukan guna menjamin kerahasiaan, keutuhan, keaslian, dan ketersediaan informasi, sehingga informasi dapat menjadi bahan pengambilan keputusan yang tepat bagi pimpinan organisasi atau institusi. Pengelolaan informasi berklasifikasi dapat berhasil dengan baik bila didukung dengan komitmen yang tinggi oleh semua aparatur pemerintah untuk sadar dan peduli terhadap keamanan infomasi berklasifikasi sehingga informasi tersebut dapat terjaga kerahasiaannya, keutuhannya, keasliannya, dan nir penyangkalannya demi kepentingan, keutuhan, dan keamanan negara.

II. PENGELOLAAN INFORMASI BERKLASIFIKASI DI LINGKUNGAN PEMERINTAH PROVINSI JAWA TENGAH

A. PEMBUATAN INFORMASI BERKLASIFIKASI

1. Pembuatan Informasi Berklasifikasi dilakukan oleh Pemilik Informasi atau Pengelola Informasi, dengan menggunakan sarana dan prasarana yang aman. Kriteria aman meliputi aman secara fisik, aman secara administrasi, dan aman secara lojik (*logical security*).

2. Perangkat atau peralatan yang digunakan untuk membuat dan/atau mengomunikasikan Informasi Berklasifikasi harus milik dinas dan hanya dimanfaatkan untuk kepentingan dinas.

   Contoh: Komputer/laptop/alat komunikasi milik dinas tidak digunakan untuk kepentingan pribadi.

3. Konsep Informasi Berklasifikasi tidak boleh disimpan dan harus dihancurkan secara fisik maupun lojik (*logical security*).

   Contoh: Apabila dokumen/surat resmi sudah selesai dibuat maka konsep surat/dokumen tersebut dihancurkan. Untuk *hardcopy* bisa dihancurkan dengan *paper shredder,* untuk *softcopy* menggunakan *software file shredder* yang direkomendasikan oleh BSSN.

4. Dokumen elektronik berklasifikasi yang sudah disahkan disimpan dalam bentuk yang tidak dapat diubah/dimodifikasi (*read only*).

   Contoh: Dokumen elekronik diubah menjadi berbentuk *file* pdf dan diberikan *watermark.*

5. Penggandaan dan/atau perubahan Informasi Berklasifikasi dilakukan harus dengan ijin dari Pemilik Informasi atau Pengelola Informasi.

B. TATA CARA KLASIFIKASI TINGKAT KERAHASIAAN

Kerahasiaan informasi diklasifikasikan menjadi 3 (tiga) tingkatan, yaitu:

1. Informasi Terbatas, merupakan informasi yang jika diakses oleh pihak yang tidak berkewenangan menimbulkan risiko rendah. Jika informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan kerusakan terhadap keamanan nasional.
2. Informasi Rahasia, merupakan informasi yang jika diakses oleh pihak yang tidak berkewenangan menimbulkan risiko sedang. Jika informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan kerusakan yang serius terhadap keamanan nasional.
3. Informasi Sangat Rahasia, merupakan informasi yang jika diakses oleh pihak yang tidak berkewenangan menimbulkan risiko tinggi. Jika informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan kerusakan yang sangat serius terhadap keamanan nasional.

Tata cara klasifikasi tingkat kerahasiaan merupakan proses yang berkelanjutan, yang meliputi:

1. Penilaian Risiko

   Penilaian risiko dilakukan oleh setiap OPD dengan berkoordinasi kepada masing-masing Unit Kerja dengan cara menghitung risiko yang akan ditimbulkan jika informasi tersebut diakses oleh pihak yang tidak berkewenangan. Informasi yang dinilai risikonya yaitu Informasi Publik yang dikecualikan sebagaimana dimaksud dalam Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, yaitu Informasi Publik yang apabila dibuka dan diberikan dapat menyebabkan:

   a. terhambatnya proses penegakkan hukum;

b. terungkapnya kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan tidak sehat;
c. terancamnya pertahanan dan keamanan negara;
d. terungkapnya kekayaan alam indonesia;
e. terungkapnya ketahanan ekonomi nasional;
f. terganggunya hubungan luar negeri;
g. terungkapnya isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang;
h. terungkapnya rahasia pribadi;
i. terungkapnya memorandum atau surat antar badan publik atau intra badan publik yang bersifat rahasia; atau
j. terungkapnya informasi yang tidak boleh diungkapkan berdasarkan undang-Undang.

Penghitungan tingkat risiko dicocokkan dengan kemungkinan terjadinya ancaman dan tingkat kemudahan eksploitasi seperti dapat dilihat pada matriks sebagai berikut:

	KEMUNGKINAN ANCAMAN TERJADI (A)	RENDAH (R)			SEDANG (S)			TINGGI (T)		
	KEMUDAHAN EKSPLOITASI (E)	R	S	T	R	S	T	R	S	T
NILAI ASET (NA)	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Penghitungan nilai risiko sebagaimana matriks di atas terdiri dari 3 (tiga) unsur:

a. Nilai Aset
   Nilai Aset ditentukan langsung oleh Pemilik Informasi yang dijabarkan dalam skala. Skala ini ditentukan berdasarkan kepentingan aset yang terdiri dari:
   1) Skala 1 : penting untuk tingkat Staf;
   2) Skala 2 : penting untuk tingkat Eselon III;
   3) Skala 3 : penting untuk tingkat Unit Kerja;
   4) Skala 4 : penting untuk tingkat OPD di Lingkungan Pemerintah Provinsi Jawa Tengah.

b. Kemungkinan Ancaman Terjadi

Kemungkinan ancaman terjadi dibagi menjadi 3 (tiga) tingkatan yaitu rendah (R), sedang (S), dan tinggi (T). Tingkat kemungkinan ancaman dapat terjadi dapat dilihat berdasarkan:

1) Pengalaman internal Organisasi Perangkat Daerah atas insiden yang pernah terjadi di lingkungannya;
2) Motivasi dan kemampuan pegawai;
3) Lingkungan fisik;
4) Faktor geografis;
5) Standar dan prosedur;
6) Ketergantungan pada pihak luar; dan/atau
7) Perangkat keras, perangkat lunak atau peralatan komunikasi yang digunakan.

c. Kemudahan Eksploitasi:
Kemudahan eksploitasi terjadi juga dibagi menjadi 3 (tiga) tingkatan yaitu rendah (R), sedang (S), dan tinggi (T). Tingkat kemudahan eksploitasi dapat dilihat berdasarkan:

1) Tingkat kesulitan pihak yang tidak berhak untuk mendapatkan informasi;
2) Jumlah jenis informasi di Pemerintah Provinsi Jawa Tengah yang wajib diamankan dengan persandian sesuai dengan peraturan perundangan-undangan;
3) Jumlah konten informasi dari setiap jenis informasi yang wajib diamankan dengan persandian;
4) Jumlah aset/fasilitas/instalasi kritis/vital/penting yang harus diamankan;
5) Jumlah rata-rata kegiatan penting yang membutuhkan dukungan pengamanan informasi per bulan;
6) Jumlah OPD yang menggunakan persandian untuk mengamankan setiap jenis informasi yang wajib diamankan.

2. Penetapan Tingkat Kerahasiaan :
   a. Penetapan Tingkat Kerahasiaan dilakukan oleh Kepala OPD masing-masing dan ditetapkan dalam bentuk surat penetapan klasifikasi. Penetapan Tingkat Kerahasiaan informasi ditentukan berdasarkan skor penilaian risiko sebagai berikut:
      1) Skor 1 – 3 masuk pada kategori risiko rendah, informasi pada tingkat ini diklasifikasikan ke dalam klasifikasi terbatas;
      2) Skor 4 – 6 masuk pada kategori risiko sedang, informasi pada tingkat ini diklasifikasikan ke dalam klasifikasi rahasia; dan

3) Skor 7 – 8 masuk pada kategori risiko tinggi, informasi pada tingkat ini diklasifikasikan ke dalam klasifikasi sangat rahasia.

b. Klasifikasi Tingkat Kerahasiaan Informasi memiliki jangka waktu pengecualian informasi sebagai berikut:

1) Terbatas memiliki jangka waktu pengecualian 5 tahun;
2) Rahasia memiliki jangka waktu pengecualian 15 tahun;
3) Sangat Rahasia memiliki jangka waktu pengecualian 30 tahun.

3. Perubahan Tingkat Kerahasiaan:

a. Perubahan Tingkat Kerahasiaan dilakukan melalui peninjauan secara berkala berdasarkan isi dan jangka waktu pengecualian informasinya. Peninjauan secara berkala bertujuan untuk:

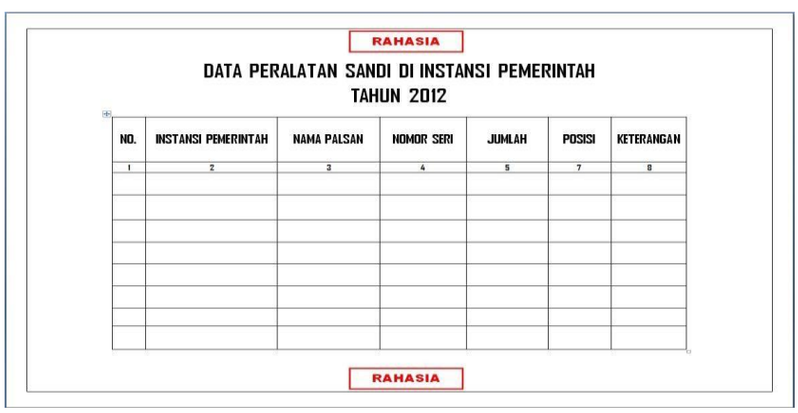
1) Deklasifikasi informasi sebelum jangka waktu pengecualian berakhir;
2) Deklasifikasi informasi sesuai dengan jangka waktu pengecualiannya; dan/atau
3) Penundaan deklasifikasi informasi.

b. Peninjauan secara berkala dilakukan oleh OPD dengan dibantu Perangkat Daerah pelaksana urusan pemerintahan bidang Persandian.

C. PEMBERIAN LABEL INFORMASI BERKLASIFIKASI

Informasi Berklasifikasi harus diberi label sesuai dengan tingkat klasifikasi informasinya yang telah ditentukan sebelumnya, dan bergantung pada bentuk dan media penyimpanannya.

1. Dokumen cetak: Label ditulis dengan cap (tidak diketik) berwarna merah pada bagian atas dan bawah setiap halaman dokumen. Jika dokumen tersebut disalin, cap label pada salinan harus menggunakan warna yang sama dengan warna cap pada dokumen asli.
   Contoh:


RAHASIA

DATA PERALATAN SANDI DI INSTANSI PEMERINTAH
TAHUN 2012

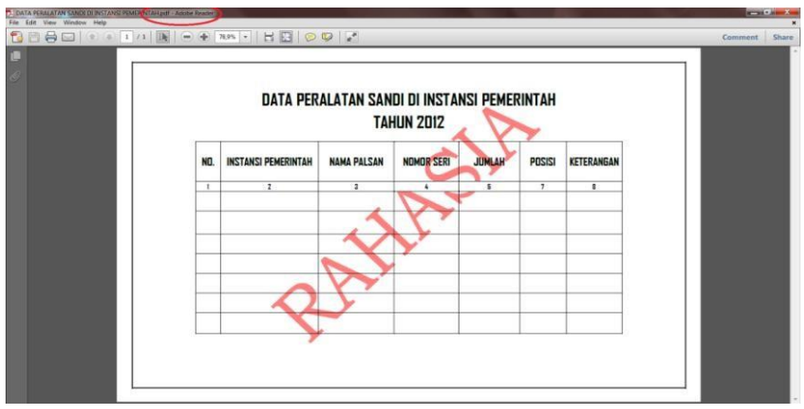
NO.	INSTANSI PEMERINTAH	NAMA PALSAN	NOMOR SERI	JUMLAH	POSISI	KETERANGAN
1	2	3	4	5	7	8

RAHASIA

2. Surat elektronik: Label ditulis pada baris *subject* pada *header* surat elektronik.
3. Dokumen Elektronik: Label diberikan dalam metadata dokumen. Dokumen Elektronik yang akan dicetak atau disimpan dalam format .pdf dapat diberikan

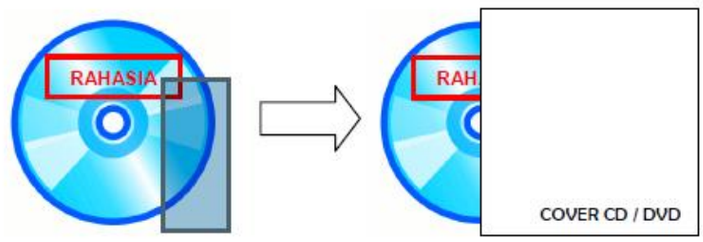
label pada *header* atau *footer* atau menggunakan *watermark* di setiap halaman termasuk *cover*.

Contoh:



4. Data base dan aplikasi bisnis: Label diberikan dalam metadata sistem/aplikasi.
5. Media lain, seperti: *cd, dvd, magnetic tape, harddrive*, dsb. Label ditempelkan pada fisik media penyimpanan dan terlihat dengan jelas, kemudian media penyimpanan tersebut dibungkus lagi tanpa diberi label. Label tersebut juga harus muncul saat informasi yang tersimpan di dalamnya diakses.

   Contoh:



D. PENGIRIMAN INFORMASI BERKLASIFIKASI

1. Pengiriman dokumen elektronik berklasifikasi :

   a. Dokumen Elektronik berklasifikasi dikirimkan dengan menggunakan teknik kriptografi dan melalui saluran komunikasi yang aman.

      Contoh: Dokumen elektronik dienkripsi dengan aplikasi enkripsi yang direkomendasikan oleh BSSN.

   b. Sebelum dikirim, harus dipastikan bahwa alamat tujuan benar dan hanya dikirimkan kepada alamat tujuan. Setelah menerima informasi tersebut, pihak penerima harus memberikan konfirmasi penerimaan kepada pengirim.

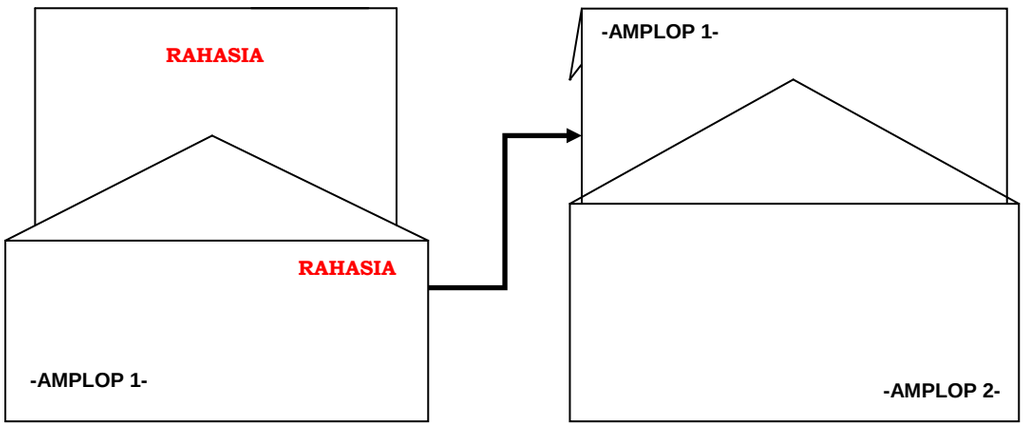
2. Pengiriman dokumen cetak berklasifikasi :

   a. Dokumen cetak berklasifikasi dikirim melalui kurir atau jasa pengiriman tercatat.

   b. Dokumen cetak berklasifikasi dimasukkan ke dalam dua amplop. Amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (kilat, sangat segera, segera, dan

biasa). Selanjutnya amplop pertama dimasukkan ke dalam amplop kedua dengan tanda-tanda yang sama kecuali cap klasifikasi.

Contoh :



c. Semua dokumen cetak berklasifikasi yang dikirim dicatat dalam buku ekspedisi sebagai bukti pengiriman atau dibuatkan tanda bukti pengiriman tersendiri.

E. PENYIMPANAN INFORMASI BERKLASIFIKASI

1. Penyimpanan Dokumen Elektronik berklasifikasi

   a. Lokasi penyimpanan Dokumen Elektronik berklasifikasi harus dilengkapi kendali akses untuk mencegah risiko kehilangan, kerusakan, dan manipulasi data.

      Contoh : Dokumen Elektronik disimpan pada *secure virtual disk.*

   b. *Data base* harus teruji baik secara lojik (*logical*) maupun fisik sebelum operasional, dilengkapi pula dengan kendali akses dan prosedur operasional yang aman dan komprehensif.

   c. Prosedur pengamanan Dokumen Elektronik berklasifikasi harus sesuai dengan klasifikasinya.

   d. Dokumen Elektronik berklasifikasi harus diamankan menggunakan teknik kriptografi serta tidak boleh disimpan di dalam komputer, *mobile devices*, atau media penyimpanan pribadi.

   e. Penyimpanan Dokumen Elektronik berklasifikasi harus diduplikasi (*backup*) secara berkala.

   f. Media penyimpanan Dokumen Elektronik berklasifikasi dilarang digunakan, dipinjam, atau dibawa ke luar ruangan atau kantor tanpa ijin Pengelola Informasi.

Contoh:

ALUR PROSES PENYIMPANAN INFORMASI BERKLASIFIKASI

1. Setiap *file* yang telah diolah dan disimpan di dalam media penyimpanan (disket, cd rom, *flashsidk*, *hardisk eksternal*) diberi label jelas sesuai tingkat klasifikasinya

2. *File* yang disimpan di dalam media penyimpanan tersebut diberikan aplikasi pengamanan seperti *password* dan aplikasi enkripsi

2. Penyimpanan dokumen cetak berklasifikasi
   a. Dokumen cetak berklasifikasi harus disimpan dalam brankas yang memiliki kunci kombinasi, atau media penyimpanan yang aman, minimal tertutup dari pandangan orang lain.
   b. Dokumen cetak berklasifikasi harus diarsip secara khusus dengan tertib dan rapi sesuai prosedur arsip yang berlaku.

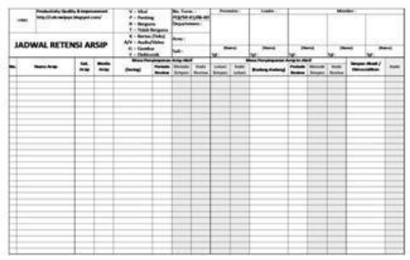
Contoh:

ALUR PROSES PENYIMPANAN DOKUMEN CETAK BERKLASIFIKASI

1. *File* yang ada di dalam arsip dipisahkan antara *file* yang berklasifikasi rahasia dan yang tidak berklasifikasi rahasia

2. *File* baik dalam bentuk *folder*, kertas, surat, dan dokumen berklasifikasi rahasia dipisahkan menurut tingkat klasifikasinya

3. *File* yang telah dipisahkan menurut tingkat klasifikasinya diberi lama retensi arsip sesuai dengan tingkat klasifikasinya



4. *File* berklasifikasi disimpan di dalam folder arsip yang aman atau di dalam brankas

III. PERLINDUNGAN INFORMASI BERKLASIFIKASI DI LINGKUNGAN PEMERINTAH PROVINSI JAWA TENGAH

A. PERLINDUNGAN FISIK

1. Perlindungan fisik dilakukan untuk melindungi keberadaan dan fungsi sarana fisik komunikasi serta segala kegiatan yang berlangsung didalamnya dari ancaman dan gangguan seperti pencurian, perusakan, dan radiasi gelombang elektromagnetik.
2. Perlindungan fisik dilakukan melalui kendali akses ruang, pemasangan teralis dan kunci ganda, pemasangan CCTV, dan penggunaan ruang TEMPEST jika diperlukan.

B. PERLINDUNGAN ADMINISTRASI

1. Perlindungan administrasi dilakukan untuk mencegah dan menanggulangi ancaman seperti kelalaian dan tindakan indisipliner lainnya.
2. Perlindungan administrasi dituangkan dalam bentuk peraturan tertulis yang menerangkan kebijakan, standar, dan prosedur operasional pengamanan informasi berklasifikasi.

3. Peraturan bersifat mengikat, wajib disepakati dan dilaksanakan oleh seluruh jajaran pimpinan, struktural, dan staf.
4. Perlunya dilakukan evaluasi dan penyesuaian peraturan secara berkala sesuai perkembangan kebutuhan dan teknologi informasi komunikasi.

C. PERLINDUNGAN LOJIK (*LOGICAL SECURITY*)

1. Perlindungan lojik (*logical security*) dilakukan untuk mencegah dan menanggulangi ancaman penyadapan dan modifikasi informasi berklasifikasi.
2. Perlindungan lojik (*logical security*) menggunakan teknik kriptografi untuk memenuhi aspek : kerahasiaan, keutuhan, otentikasi, nir penyangkalan, dan jaminan ketersediaan informasi berklasifikasi:
   a. Kerahasiaan berarti informasi tidak dapat diketahui oleh siapapun kecuali pihak yang memiliki otoritas.
   b. Keutuhan berarti informasi tidak dapat diubah oleh siapapun kecuali pihak yang memiliki otoritas.
   c. Otentikasi berhubungan dengan keaslian informasi, identifikasi/ pengenalan baik secara kesatuan sistem maupun informasi itu sendiri.
   d. Nir penyangkalan berarti informasi tidak dapat disangkal oleh pihak pengirim maupun penerima.
   e. Ketersediaan berarti informasi tersedia pada saat dibutuhkan.
3. Perlindungan lojik (*logical security*) yang menggunakan teknik kriptografi harus memenuhi standar dan direkomendasikan oleh Lembaga Sandi Negara.

GUBERNUR JAWA TENGAH,

ttd

GANJAR PRANOWO