

LAMPIRAN
PERATURAN KEPALA LEMBAGA SANDI NEGARA
NOMOR 10 TAHUN 2012
TENTANG PEDOMAN PENGELOLAAN DAN PERLINDUNGAN
INFORMASI BERKLASIFIKASI MILIK PEMERINTAH

**PEDOMAN PENGELOLAAN DAN PERLINDUNGAN
INFORMASI BERKLASIFIKASI MILIK PEMERINTAH**

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Informasi merupakan aset penting bagi suatu organisasi. Setiap organisasi memiliki informasi kritis atau sensitif atau rahasia yang menjadikannya 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-kerugian organisasi merupakan hal yang mutlak yang harus diperhatikan baik oleh segenap jajaran pemilik, manajemen, maupun karyawan 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 informasi berklasifikasi sehingga informasi tersebut dapat terjaga kerahasiaannya, keutuhannya, keasliannya, dan nir penyangkalannya demi kepentingan, keutuhan, dan keamanan negara.

B. MAKSUD DAN TUJUAN

1. Maksud

Pedoman pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah dimaksudkan sebagai acuan bagi instansi pemerintah dalam mengelola dan melindungi informasi berklasifikasi di lingkungan masing-masing.

2. Tujuan

Pedoman pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah bertujuan agar mekanisme pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah berjalan secara aman, efektif, dan efisien.

C. SASARAN

Sasaran pedoman pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah yaitu untuk mencegah terjadinya kebocoran informasi berklasifikasi milik pemerintah melalui pengelolaan dan perlindungan informasi berklasifikasi secara utuh, efisien, efektif, dan akuntabel oleh instansi pemerintah guna mendukung terwujudnya keamanan nasional.

D. ASAS

1. 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.

2. 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.

3. Asas Ketersediaan

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

4. 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.

5. Asas Efektif dan Efisien

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

E. RUANG LINGKUP

BAB I. PENDAHULUAN

BAB II. PENGELOLAAN INFORMASI BERKLASIFIKASI MILIK PEMERINTAH

BAB III. PERLINDUNGAN INFORMASI BERKLASIFIKASI MILIK PEMERINTAH

BAB IV. PENUTUP

F. PENGERTIAN

1. Pengelolaan adalah suatu upaya, pekerjaan, kegiatan, dan tindakan yang meliputi pembuatan, pemberian label, pengiriman, dan penyimpanan.
2. 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.
3. 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.
4. 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.
5. 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.

6. Informasi Berklasifikasi adalah Informasi yang telah ditetapkan dan apabila diketahui oleh pihak yang tidak berhak dapat membahayakan keamanan nasional.
7. Instansi Pemerintah adalah kementerian negara, lembaga pemerintah non kementerian, sekretariat lembaga negara, dan pemerintah daerah.
8. 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.
9. 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.
10. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.
11. Konsep Informasi Berklasifikasi adalah rancangan atau buram surat dari Informasi Berklasifikasi.
12. Metadata adalah Informasi terstruktur yang mendeskripsikan, menjelaskan, menemukan, atau setidaknya membuat suatu informasi mudah untuk ditemukan kembali, digunakan, atau dikelola.

BAB II PENGELOLAAN

INFORMASI BERKLASIFIKASI MILIK PEMERINTAH

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 logik (*logical security*).
2. Perangkat atau peralatan yang digunakan untuk membuat dan/atau mengkomunikasikan 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 logik (*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 Lemsaneg.
4. Dokumen elektronik berklasifikasi yang sudah disahkan disimpan dalam bentuk yang tidak dapat diubah/dimodifikasi (*read only*).
Contoh: Dokumen elektronik 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. PEMBERIAN LABEL INFORMASI BERKLASIFIKASI

Informasi Berklasifikasi harus diberi label sesuai dengan tingkat klasifikasi informasinya, 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	6	7

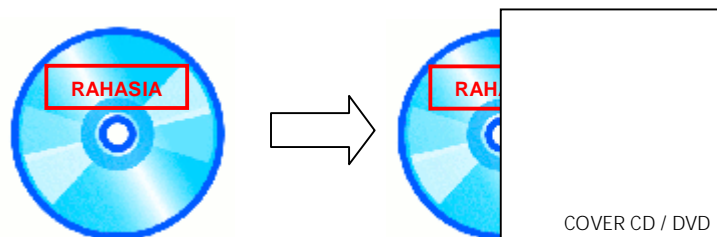
RAHASIA

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:

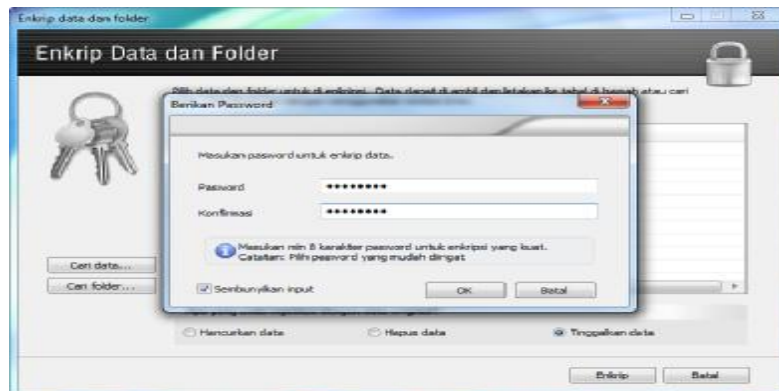


C. PENGIRIMAN INFORMASI BERKLASIFIKASI

1. Pengiriman dokumen elektronik berklasifikasi

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

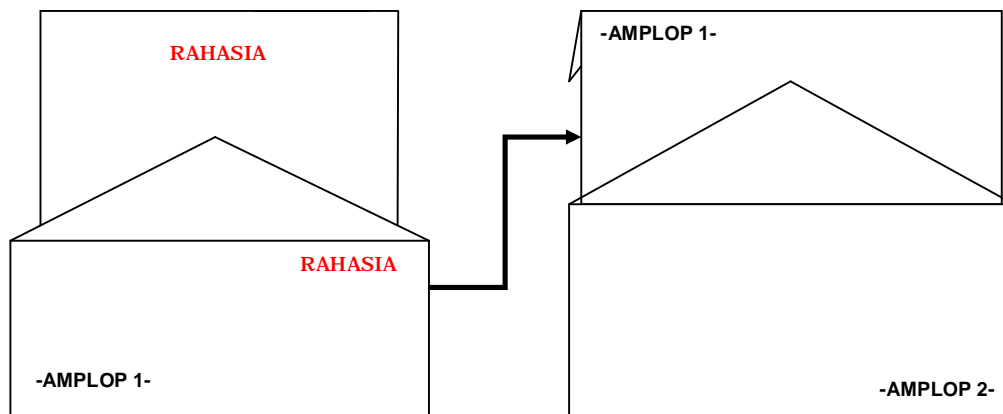
Contoh: Dokumen elektronik dienkripsi dengan aplikasi enkripsi yang direkomendasikan oleh Lemsaneg.





- 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 :



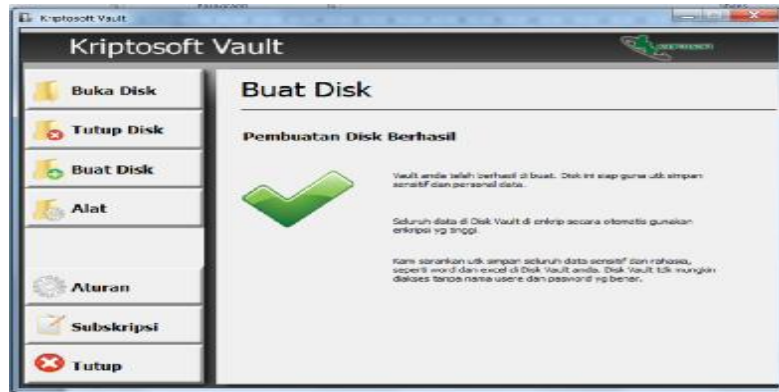
- c. Semua dokumen cetak berklasifikasi yang dikirim dicatat dalam buku ekspedisi sebagai bukti pengiriman atau dibuatkan tanda bukti pengiriman tersendiri.

D. 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 logik (*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, *flashdisk*, *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.

BAB III PERLINDUNGAN

INFORMASI BERKLASIFIKASI MILIK PEMERINTAH

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.

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 logik (*logical security*) dilakukan untuk mencegah dan menanggulangi ancaman penyadapan dan modifikasi informasi berklasifikasi.
2. Perlindungan logik (*logical security*) menggunakan teknik kriptografi untuk memenuhi aspek : kerahasiaan, keutuhan, otentikasi, nir penyangkalan, dan jaminan ketersediaan informasi berklasifikasi.
 - Kerahasiaan berarti informasi tidak dapat diketahui oleh siapapun kecuali pihak yang memiliki otoritas.
 - Keutuhan berarti informasi tidak dapat diubah oleh siapapun kecuali pihak yang memiliki otoritas.
 - Otentikasi berhubungan dengan keaslian informasi, identifikasi/pengenalan baik secara kesatuan sistem maupun informasi itu sendiri.

- Nir penyangkalan berarti informasi tidak dapat disangkal oleh pihak pengirim maupun penerima.
 - Ketersediaan berarti informasi tersedia pada saat dibutuhkan.
3. Perlindungan logik (*logical security*) yang menggunakan teknik kriptografi harus memenuhi standar dan direkomendasikan oleh Lembaga Sandi Negara.

BAB IV

PENUTUP

Pedoman ini diharapkan menjadi acuan bagi Instansi pemerintah dalam mengelola Informasi Berklasifikasi di lingkungan masing-masing sehingga mencegah terjadinya kebocoran Informasi Berklasifikasi guna mendukung terwujudnya keamanan nasional.

KEPALA LEMBAGA SANDI NEGARA,

DJOKO SETIADI