Informasi Berklasifikasi

DINAS KOMINFO PROVINSI JAWA TIMUR

TAHUN 2020

Profile

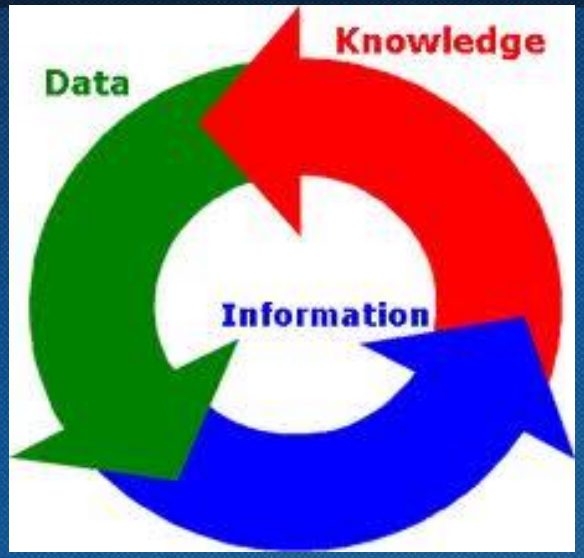
Pendidikan:

1. Teknik Informatika 2003 – 2007 : ITS (Institut Teknologi Sepuluh Nopember)
2. Information System Management 2016 – 2017 : UNSW (University Of New South Wales)

Riwayat Pekerjaan:

1. 2008 - 2009 : Otorita Batam
2. 2009 – 2014 : Kementerian Komunikasi dan Informatika
3. 2015 – sekarang : Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

PENDAHULUAN



- Entitas atau bentuk apa pun yang memberikan jawaban atas pertanyaan tertentu atau menyelesaikan ketidakpastian yang berkaitan dengan data dan pengetahuan
- Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah “information-based society”.

Apa itu keamanan informasi?

Pengertian kemanan informasi

Keamanan informasi adalah kumpulan strategi untuk mengatur seluruh proses, perangkat dan sumber daya manusia untuk mencapai CIA

CiA

Confidential integrity availability

Melindungi informasi terhadap pihak yang tidak berwenang

Melindungi informasi agar tidak diubah oleh pihak yang tidak berwenang

ketersediaan informasi kepada pihak yang berwenang hanya jika diminta.

INFORMASI BERKLASIFIKASI

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA TIMUR

Dasar Hukum

1. Peraturan Kepala Lemsaneg No.10 Tahun 2012 ttg Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah
2. Peraturan Kepala Lemsaneg No. 3 Tahun 2016 ttg Produk Karya Mandiri Lembaga Sandi Negara
3. Peraturan Kepala Lemsaneg No. 6 Tahun 2016 ttg Pengendalian Persandian

Produk Karya Mandiri Lemsaneg Perka No. 3 Tahun 2016

Abstrak: bahwa upaya perlindungan terhadap informasi berklasifikasi milik pemerintah melalui persandian harus dinamis sesuai dengan kebutuhan dan perkembangan teknologi informasi dan komunikasi; dan Lembaga Sandi Negara membangun dan mengembangkan Teknologi Persandian yang mandiri secara bertahap dan berkesinambungan guna mendukung tugas dan fungsi Lembaga Sandi Negara.

Perka ini mengatur tentang :
Produk Karya Mandiri Lemsaneg yang dihasilkan melalui inovasi mandiri Lemsaneg atau melalui kerjasama dengan lembaga pemerintah dan nonpemerintah. Pembangunan dan pengembangan teknologi, perlindungan hak kekayaan intelektual atas produk karya mandiri, dan lain-lain.

Perka Nomor 6 Tahun 2016 tentang Pengendalian Persandian

Abstrak: untuk mendukung penyelenggaraan persandian dalam menjamin keamanan informasi berklasifikasi milik pemerintah atau negara serta menyajikan hasil pengupasan informasi bersandi guna turut serta menjaga keamanan nasional diperlukan upaya pengendalian persandian dan untuk mewujudkan upaya pengendalian persandian yang efektif, efisien, dan terukur atas penyelenggaran persandian pada instansi pemerintah diperlukan pengaturan mengenai pengendalian persandian;

Perka ini mengatur tentang : pengendalian persandian dengan tujuan menjamin penyelenggaraan Persandian sesuai dengan rencana, tujuan, dan sasaran yang telah ditetapkan, mengelola risiko yang timbul dari ATHG penyelenggaraan Persandian, melindungi Sumber Daya Persandian agar terjaga keamanannya; dan mewujudkan kepatuhan terhadap Kebijakan Persandian.

PENGKLASIFIKASIAN INFORMASI

1. Informasi yang bersifat public:

1.1 Informasi yang bersifat terbuka, yaitu informasi yang wajib disediakan dan diumumkan secara berkala, meliputi:

a. Profil yang meliputi seperti sejarah singkat, struktur organisasi, tujuan, kedudukan, tugas dan fungsi, program kerja, dan sebagainya;
b. Informasi mengenai kegiatan dan kinerja Pemerintah Kota Malang, Laporan Akuntabilitas Kinerja dan sebagainya.
c. Informasi mengenai laporan keuangan.
d. Informasi lain yang diatur dalam peraturan perundangan;
e. Informasi yang lebih detil atas permintaan pemohon.

1.2 Informasi yang wajib diumumkan secara serta merta, yaitu informasi yang dapat mengancam hajat hidup orang banyak dan keterkaitan umum, meliputi:

a. Informasi mengenai bencana alam, seperti kekeringan, kebakaran hutan karena faktor alam, hama penyakit tanaman, epidemik, wabah, kejadian luar biasa, kejadian antariksa atau benda-benda angkasa;

b. Informasi mengenai tentang keadaan bencana non-alam seperti kegagalan industri atau teknologi,dampak industri, ledakan nuklir, pencemaran lingkungan dan kegiatan keantariksaan;

c. Bencana sosial seperti kerusuhan sosial, konflik sosial antar kelompok atau antar komunitas masyarakat dan teror;

d. Informasi tentang jenis, persebaran dan daerah yang menjadi sumber penyakit yang berpotensi menular;

e. Informasi tentang racun pada bahan makanan yang dikonsumsi oleh masyarakat;dan/atau

f. Hal lain yang mengancam hajad hidup orang banyak.

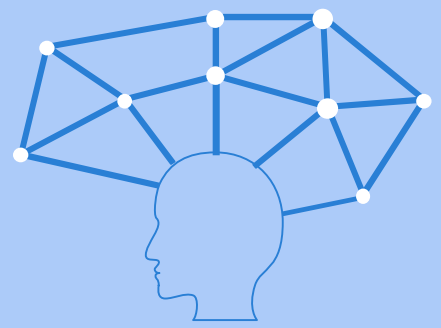
1.3 Informasi publik yang wajib tersedia setiap saat, meliputi:
a. Daftar seluruh informasi publik yang berada di bawah penguasaan Pemerintah Kota Malang; tidak termasuk informasi yang dikecualikan.
b. Seluruh kebijakan yang ada serta dokumen pendukungnya;
c. Rencana kerja program/kegiatan,termasuk perkiraan pengeluaran tahunan Pemerintah Kabupaten Sambas;
d. Prosedur kerja pegawai Pemerintah Kota Malang yang berkaitan dengan pelayanan masyarakat; dan/atau
e. Laporan mengenai pelayanan akses informasi publik sebagaimana diatur dalam Undang-Undang Nomor 14 Tahun 2008.

1 INFORMASI

- Informasi merupakan aset penting bagi suatu organisasi.
- Setiap organisasi memiliki informasi kritis atau sensitif/rahasia yg 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 kerugian organisasi merupakan hal yang mutlak yang harus diperhatikan baik oleh segenap jajaran pemilik, manajemen, maupun karyawan organisasi yang bersangkutan.

2 Informasi Berklasifikasi

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.



TUJUAN

Mekanisme pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah berjalan secara aman, efektif, dan efisien

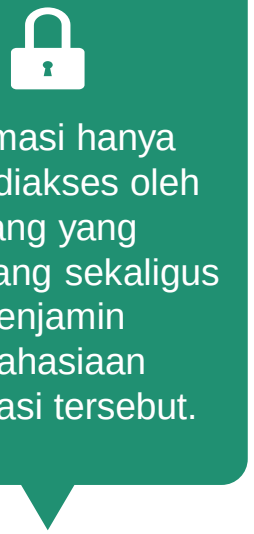
INFORMASI BERKLASIFIKASI

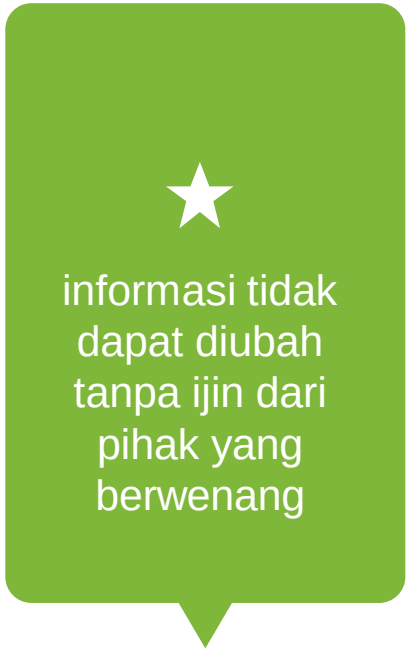
1. Informasi yang telah ditetapkan dan apabila diketahui oleh pihak yang tidak berhak dapat membahayakan keamanan nasional

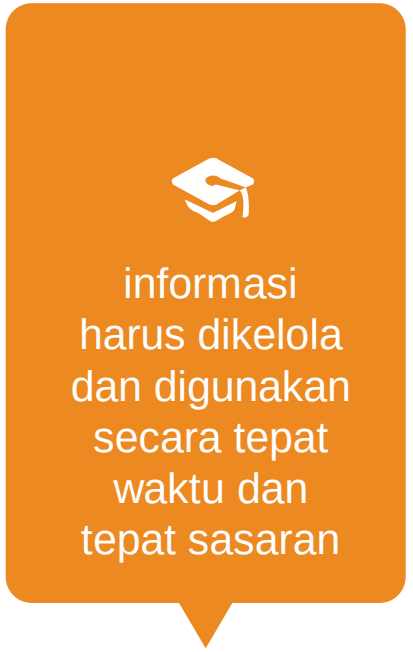
2. Di dalam informasi tersebut harus memenuhi Asas Keamanan, Keutuhan, Ketersediaan, Kecepatan & Ketepatan, serta Efektif & Efisien

Prinsip Informasi Berklasifikasi

Your great subtitle goes here







Informasi Berklasifikasi Milik Pemerintah

1. Pembuatan Informasi Berklasifikasi

- Dikelola oleh Pemilik atau Pengelola Informasi dengan menggunakan sarana dan prasarana yang aman
- Perangkat yang digunakan harus milik dinas dan dimanfaatkan untuk kepentingan dinas
- Konsep Informasi Berklasifikasi tidak boleh disimpan dan harus dihancurkan secara fisik maupun logika
- Dokumen elektronik berklasifikasi yang sah disimpan dalam bentuk yang tidak dapat diubah
- Penggandaan atau perubahan Informasi Berklasifikasi dilakukan dengan ijin Pemilik atau Pengelola Informasi

Informasi Berklasifikasi Milik Pemerintah (lanjutan)

2. Pemberian Label Informasi Berklasifikasi

- Dokumen Cetak : Label ditulis dengan cap (tidak diketik) berwarna merah pada bagian atas dan bawah setiap halaman dokumen
- Surat elektronik : Label ditulis pada baris subject pada header surat
- Dokumen Elektronik : Label diberikan dalam metadata dokumen
- Data base dan aplikasi bisnis : Label diberikan dalam metadata sistem aplikasi
- 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.

Bagaimana informasi diklasifikasikan

1. Mengidentifikasi semua sumber daya informasi yang perlu dilindungi.

2. Mengidentifikasi ukuran pengamanan informasi yang akan diterapkan pada masing-masing kelas informasi. Secara garis besar pengamanan yang diterapkan pada informasi adalah otentikasi, pengendalian akses, penyandian, pengawasan secara administratif, pengawasan secara teknologi dan/atau asuransi.

3. Mengidentifikasi tingkat guna dan nilai informasi.

4. Memetakan ukuran perlindungan informasi untuk masing-masing tingkat informasi.

5. Mengklasifikasi informasi : kebanyakan pengklasifikasian data/informasi terfokus hanya pada kerahasiaan data saja. Namun sesungguhnya pengklasifikasian informasi lebih dari itu, misalnya :

a. Klasifikasi berdasarkan derajat kecepatan, misalnya : prioritas, *urgent*, segera;

b. Klasifikasi berdasarkan tingkat kerahasiaan, misalnya : *top secret*, *secret*, *confidential*;

c. Klasifikasi berdasarkan frekuensi penggunaan, misalnya : sering, kadang, sekali pakai;

d. Klasifikasi berdasarkan waktu pemakaian, misalnya : tahun, bulan, minggu, jam;

e. Klasifikasi berdasarkan kewenangan, misalnya : *edit*, *read only*;

f. Klasifikasi berdasarkan isi, misalnya : keuangan, politik, ekonomi;

g. Klasifikasi lain yang didefinisikan organisasi, misalnya : umum, *pivate*, *client*, *staff only*.

Penyimpanan informasi berklasifikasi

- Penyimpanan Dokumen Elektronik berklasifikasi
- ➢ Dilengkapi kendali akses untuk mencegah risiko kehilangan, kerusakan, dan manipulasi data
- ➢ Data base harus teruji baik secara lojik (logical) maupun fisik sebelum operasional, dilengkapi pula dengan kendali akses dan prosedur operasional yang aman dan komprehensif.
- ➢ Prosedur pengamanan harus sesuai dengan klasifikasinya.
- ➢ Diamankan menggunakan teknik kriptografi serta tidak boleh disimpan di dalam komputer, mobile devices, atau media penyimpanan pribadi.
- ➢ Harus dilakukan duplikasi (backup) secara berkala.
- ➢ Media penyimpanan dilarang digunakan, dipinjam, atau dibawa ke luar ruangan atau kantor tanpa ijin Pengelola Informasi.

ALUR PROSES PENYIMPANAN INFORMASI BERKLASIFIKASI

Step 1

Penyimpanan File

Setiap file yg telah diolah dan disimpan didalam media penyimpanan (cd, flasdisk, cdrom, dsb) diberi label yg jelas sesuai tingkat klasifikasi

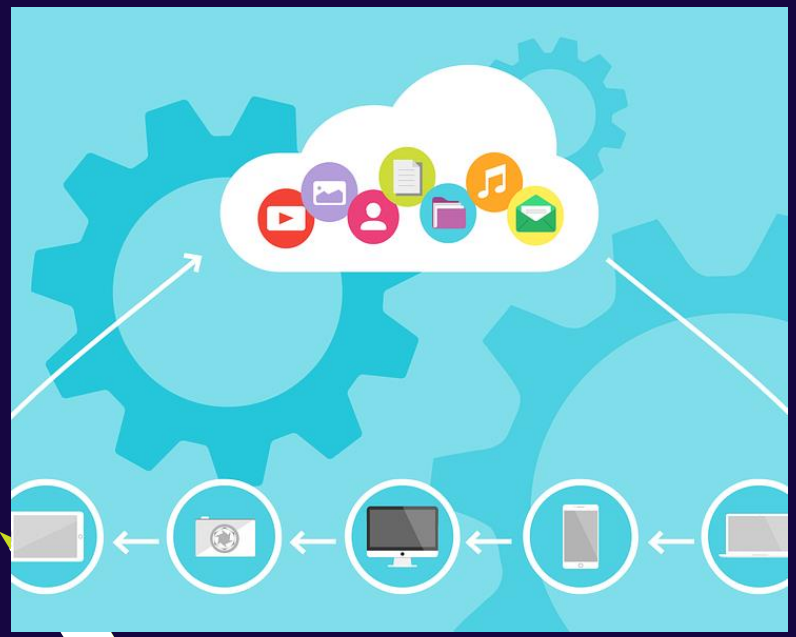
Enkripsi

Step 2

Aplikasi Pengamanan

File yg Disimpan di dalam media penyimpanan tsb diberikan aplikasi pengamanan seperti password dan aplikasi enkripsi

Penyimpanan Informasi Berklasifikasi (lanjutan)



- Penyimpanan Dokumen Cetak berklasifikasi

➢ Disimpan dalam brankas yang memiliki kunci kombinasi, atau media penyimpanan yang aman, minimal tertutup dari pandangan orang lain.

➢ Diarsip secara khusus dengan tertib dan rapi sesuai prosedur arsip yang berlaku

ALUR PROSES PENYIMPANAN DOKUMEN CETAK BERKLASIFIKASI

1. Pengelompokan File

File yg ada didalam arsip dipisahkan antara file yg berklasifikasi rahasia dan yg tidak berklasifikasi rahasia

4. Penyimpanan yg aman

File berklasifikasi disimpan didalam folder yg aman atau didalam brankas

2. Tingkat Klasifikasi

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

3. Lama Retensi

File yg telah dipisahkan menurut tingkat klasifikasinya diberi lama retensi arsip sesuai tingkat klasifikasinya

pencegahan

Macam-macam pencegahan SECARA FISIKAL

TRAINING HUMAN

Access door

Mantrap/doortrap

PENCEGAHAN

SECARA DIGITAL SECURITY DAN INCIDENT RESPON PLAN

- Instalasi dan maintenance firewall
- Enkripsi penyimpanan data
- Membatasi akses data bagi mereka yang memang perlu mengetahui
- Menjaga sistem keamanan selalu “up to date”
- Gunakan dan perbaharui software antivirus
- Menugaskan ID unik untuk orang yang memiliki akses data khusus
- Menelusuri akses data dengan ID unik
- Tidak menggunakan password default dari vendor
- Secara teratur menguji keamanan sistem

DINAS KOMINFO PROV. JAWA TIMUR