GUBERNUR SULAWESI TENGGARA

PERATURAN GUBERNUR SULAWESI TENGGARA

NOMOR 42 TAHUN 2017

TENTANG

PEDOMAN PENGAMANAN PENGELOLAAN INFORMASI

DI LINGKUNGAN PEMERINTAH PROVINSI SULAWESI TENGGARA

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR SULAWESI TENGGARA,

Menimbang:

a. bahwa dalam rangka menjamin jumlah, mutu informasi milik pemerintah;
b. bahwa dalam rangka mencegah kebocoran informasi berklasifikasi milik pemerintah yang menyangkut keberlangsungan hidup bernegara, keutuhan dan ketentraman hidup masyarakat diperlukan pedoman untuk mengelola informasi berklasifikasi;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a dan huruf b maka perlu menetapkan Peraturan Gubernur tentang Pedoman Pengamanan Pengelolaan Informasi Di Lingkungan Pemerintah Provinsi Sulawesi Tenggara.

Mengingat:

1. Undang-Undang Nomor 13 Tahun 1964 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 1964 tentang Pembentukan

Daerah Tingkat I Sulawesi Tengah dan Daerah Tingkat I Sulawesi Tenggara dengan mengubah Undang-Undang Nomor 47 Prp. Tahun 1960 tentang Pembentukan Daerah Tingkat I Sulawesi Utara – Tengah dan Daerah Tingkat I Sulawesi Selatan – Tenggara (Lembaran Negara Republik Indonesia Tahun 1964 Nomor 94, Tambahan Lembaran Negara Republik Indonesia Nomor 2687);

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 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071);
5. 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 kedua kalinya 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);
6. Peraturan Pemerintah Nomor 28 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembara Negara Republik Indonesia

Tahun 2012 Nomor 53, Tambahan Lembaran Negara Republik Indonesia Nomor 5286);

7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 80 Tahun 2012 tentang Pedoman Tata Naskah Dinas Instansi Pemerintah;
8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 tentang Pedoman Umum Tata Naskah Dinas Elektronik di Lingkungan Instansi Pemerintah;
9. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah;
10. Peraturan Kepala Arsip Nasional Nomor 17 Tahun 2011 tentang Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis;
11. Peraturan Kepala Arsip Nasional Nomor 37 Tahun 2016 tentang Pedoman Penyusutan Arsip.

MEMUTUSKAN:

Menetapkan: PERATURAN GUBERNUR TENTANG PEDOMAN PENGAMANAN PENGELOLAAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI SULAWESI TENGGARA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan ini yang dimaksud dengan:

1. Daerah adalah Provinsi Sulawesi Tenggara.
2. Pemerintah Daerah adalah Pemerintah Provinsi Sulawesi Tenggara.
3. Gubernur adalah Gubernur Sulawesi Tenggara.

4. 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 maupun non elektronik.
5. Informasi Elektonik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foro, *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.
6. 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.
7. 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.
8. Dokumen Konvensional adalah dokumen yang informasinya terekam dalam media kertas berupa tulisan tangan atau ketikan.

9. Tingkat Klasifikasi Informasi adalah pengelompokan informasi dalam tingkatan tertentu berdasarkan dampak yang ditimbulkan apabila informasi yang terdapat didalamnya diketahui oleh pihak yang tidak berhak.
10. Sangat Rahasia adalah klasifikasi informasi yang apabila informasi tersebut diketahui oleh pihak yang tidak berhak dapat membahayakan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan/atau keselamatan bangsa.
11. Rahasia adalah klasifikasi informasi yang apabila informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya fungsi penyelenggaraan negara, sumber daya nasional dan/atau ketertiban umum.
12. Terbatas adalah klasifikasi informasi yang apabila informasi tersebut diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya pelaksanaan tugas dan fungsi lembaga pemerintahan.
13. Biasa/Terbuka adalah klasifikasi informasi yang apabila informasi terebut diketahui oleh publik tidak merugikan siapapun.
14. Pemilik Informasi adalah pegawai maupun pejabat Instansi Pemerintah yang karena fungsi dan jabatannya bertanggungjawab atas semua Informasi yang dihasilkan serta dikelola dan/atau dikumpulkannya selama bekerja dan atas nama instansinya.
15. Amat segera/kilat adalah batas waktu pemprosesan surat/informasi dalam waktu 24 jam setelah surat diterima.
16. Segera adalah batas waktu pemprosesan surat/informasi dalam waktu 2 x 24 jam setelah surat diterima.
17. Penting adalah batas waktu pemprosesan surat/informasi dalam kurun waktu 3 x 24 jam setelah surat diterima.

18. Biasa adalah batas waktu pemprosesan surat/informasi dalam kurun waktu 5 hari kerja setelah surat diterima.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

Pedoman pengamanan pengelolaan Informasi dimaksud untuk menjadi pedoman dalam mengelola dan melindungi Informasi di lingkungan karja masing-masing.

Pasal 3

Tujuannya adalah

Sebagai panduan bagi pemerintah daerah dalam mengelola dan melindungi Informasi di masing-masing Organisasi Perangkat Daerah sehingga dapat berjalan aman, efektif, efisien dan menjamin kualitas Informasi dengan kriteria terjaminnya kerahasiaan, keutuhan dan ketersediaan.

BAB III

SISTEMATIKA

Pasal 4

(1) Sistematika penyusunan Pedoman Pengamanan Pengelolaan Informasi terdiri dari:
   a. Bab I Pendahuluan
   b. Bab II Ketentuan Umum
   c. Bab III Tahapan Pengelolaan Informasi
   d. Bab IV Penutup

(2) Dokumen Pedoman Pengamanan Pengelolaan Informasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I, yang merupakan bagian yang tidak terpisahkan dari Peraturan Gubernur.

BAB IV

KETENTUAN PENUTUP

Pasal 5

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Kendari
Pada tanggal 14 - 10 - 2017

Plt. GUBERNUR SULAWESI TENGGARA,

H. M SALEH LASATA

LA ODE ALVDI PILI, ST	Ass. II	
Drs. H. KUSNARDI, MSi	KADIS	
EFFENDI KALIMUDDIN SH, MH	Kabag Hukum	

Diundangkan di Kendari
Pada tanggal 2017

SEKRETARIS DAERAH
PROVINSI SULAWESI TENGGARA,

LUKMAN ABUNAWAS

BERITA DAERAH PROVINSI SULAWESI TENGGARA TAHUN 2017 NOMOR:

LAMPIRAN: PERATURAN GUBERNUR SULAWESI TENGGARA
NOMOR : 42
TANGGAL : 14 - 10 - 2017

PEDOMAN PENGAMANANPENGELOLAAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI SULAWESI TENGGARA

BAB I
PENDAHULUAN

A. LATAR BELAKANG

Kedudukan Informasi dalam suatu organisasi merupakan salah satu unsur penting yang memberikan kemungkinan hidup, perkembangan dan memperlancar kegiatan organisasi baik pada tingkat pembuatan kebijakan maupun pada tingkat operasional. Informasi diakui sebagai salah satu sumber daya utama organisasi yang menghendaki tindakan manajemen yang memadai terhadapnya. Aliran Informasi dari satu unit ke unit yang lain dalam organisasi memungkinkan unit-unit ini dapat berfungsi dengan lancar dalam suatu harmoni. Informasi berpotensi mengikat unit-unit organisasi untuk bertindak secara tertentu atas dasar pijakan informasi yang sama. Dengan demikian keberadaan Informasi dengan jumlah dan mutu yang memadai adalah suatu kebutuhan demi kelangsungan hidup organisasi.

Dalam kenyataan Informasi dengan jumlah dan mutu yang memadai untuk keperluan organisasi tidak dengan sendirinya tercipta, Informasi lahir dari kondisi dengan kualitas tertentu. Kondisi yang menjadi prasyarat lahirnya Informasi ini meliputi berbagai unsur dalam organisasi, seperti unsur sumber daya manusia (SDM), perangkat keras, dan perangkat lunak.

Guna menjamin jumlah dan mutu Informasi maka perlu ada usaha pengamanan dengan tujuan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), otentikasi (*authentication*), nir-sangkal (*non-repudiation*), dan keandalan (*reliability*) terhadap Informasi tersebut.Pengamanan terhadap Informasi meliputi pengamanan pada proses pembuatan, pelabelan, penyimpanan,

pengiriman/publikasi, pengarsipan dan pemusnahan. Pengamanan yang dilakukan meliputi Informasi Elektronik dan Informasi Non Elektronik.

B. SASARAN

Sasaran Pedoman Pengelolaan dan Perlindungan Informasi di Lingkungan Pemerintah Provinsi Sulawesi Tenggara yaitu untuk mencegah terjadinya kebocoran maupun modifikasi Informasi sesuai dengan Tingkat Klasifikasi Informasi yang terdiri dari klasifikasi Biasa/Terbuka, Terbatas, Rahasia maupun Sangat Rahasia guna mendukung ketersediaan Informasi yang bermutu untuk kegiatan kedinasan di lingkungan Pemerintah Provinsi Sulawesi Tenggara.

BAB II
KETENTUAN UMUM

A. KEBIJAKAN PENGAMANAN PENGELOLAAN INFORMASI

Pengamanan pengelolaan Informasi harus ditetapkan dan didukung oleh pimpinan pencipta informasi/Pemilik Informasi. Pencipta/Pemilik Informasi yang dimaksud adalah Gubernur, Wakil Gubernur, Sekretaris Daerah, Inspektur, Asisten Daerah, Kepala Dinas, Kepala Badan, dan Pejabat Fungsional.

B. PRINSIP DASAR PENGAMANAN PENGELOLAAN INFORMASI

Prinsip dasar dalam pengamanan pengelolaan Informasi adalah:

1. Memperhatikan tingkat keseriusan dari dampak yang ditimbulkan apabila Informasi yang sifatnya kedinasan, baik yang berklasifikasi Biasa/Terbuka, Terbatas, Rahasia, dan Sangat Rahasia itu disalahgunakan oleh pihak-pihak yang tidak berhak untuk tujuan dan kepentingan yang tidak sah.
2. Pengamanan pengelolaan Informasi harus dituangkan dalam suatu ketetapan pimpinan berupa kebijakan umum maupun kebijakan teknis sebagai dasar bagi pegawai di lingkungan Pemerintah Provinsi Sulawesi Tenggara dalam mengelola Informasi.

BAB III
TAHAPAN PENGELOLAAN INFORMASI

A. PEMBUATAN

Dalam pembuatan Informasi terdapat hal-hal yang perlu diperhatikan, antara lain:

1. Keamanan Tempat Pembuatan Informasi

   Keamanan tempat pembuatan Informasi meliputi kriteria aman secara fisik. Aman secara fisik meliputi perlindungan terhadap personil, perangkat keras, perangkat lunak, jaringan, data/informasi dari usaha fisik dan kejadian yang dapat menyebabkan kerugian atau kerusakan bagi instansi pemerintah. Aman secara fisik meliputi juga perlindungan terhadap ancaman kebakaran, kebanjiran, bencana alam, pencurian, vandalisme, dan terorisme.

   Contoh:

   1) Ruangan tempat pembuatan Informasi dilengkapi dengan kunci/gembok, dilengkapi dengan *Closed Circuit Television* (CCTV);
   2) Pada area depan kantor diterdapat penjaga keamanan;
   3) Pegawai kantor menggunakan tanda pengenal dan untuk tamu dilengkapi dengan tanda tamu serta mengisi buku tamu;
   4) Ruangan pembuatan informasi dengan ruangan untuk menerima tamu dipisah.
   5) Terdapat pembagian area akses, seperti area UMUM dan area TERBATAS.
   6) Komputer/laptop yang digunakan untuk mengolah dan membuat Informasi dilengkapi dengan kode masuk (password).
   7) Layar komputer/laptop tidak mengarah ke tempat yang menjadi lalu lintas orang/tempat menunggu tamu.
   8) Menggunakan software/aplikasi yang asli/berlisensi.
   9) Komputer/laptop yang digunakan dilengkapi dengan antivirus yang *update*/terbaru.
   10) Jaringan internet hanya untuk pegawai organisasi yakni dengan memasang password pada wifi atau hanya komputer/laptop yang telah didaftarkan yang dapat mengaksesnya.
   11) Komputer/laptop hanya diinstal aplikasi yang berhubungan dengan kepentingan dinas/pekerjaan.
   12) Ruangan pejabat/pembuatan informasi bebas dari adanya peralatan sadap.

2. Perangkat/peralatan yang digunakan merupakan milik kantor/dinas dan hanya digunakan untuk kepentingan dinas.Bila dalam hal kantor/dinas tidak dapat memfasilitasi perangkat/peralatan dan pegawai menggunakan perangkat/peralatan milik pribadi maka perlu diatur ketentuan mengenai penggunaanya, seperti tidak boleh meminjam pakaikan perangkat/peralatan milik pribadi tersebut ke orang lain tanpa pengawasan karena didalam perangkat/peralatan tersebut terdapat dokumen/Informasi kedinasan.

3. Konsep Informasi yang sudah tidak digunakan harus dihancurkan secara fisik maupun lojik.

   Contoh:

   Untuk Dokumen Konvensional dihancurkan dengan mesin penghancur kertas/*paper shredder* atau dibakar. Sedangkan untuk Dokumen Elektronik dihancurkan menggunakan aplikasi *file shredder.*

4. Dokumen Konvensional yang dialihmediakan menjadi Dokumen Elektronik disimpan dalam bentuk yang tidak dapat diubah/dimodifikasi (*read only*). Dokumen Elektronik dapat diberikan tanda tangan digital.

   Contoh:

   Dokumen Konvensionaldi *scan* menjadi Dokumen Elektronik dalam bentuk file .pdf diberikan tanda tangan elektronik sehingga dokumen tersebut tidak dapat diubah/dimodifikasi, adapun jika berhasil diubah/dimodifikasi akan muncul notifikasi yang menyatakan bahwa dokumen tersebut telah diubah/dimodifikasi.

5. Penggandaan dan/atau perubahan Informasi harus seizin Pemilik Informasi/pengelola Informasi.

B. PELABELAN

Pelabelan terhadap Informasi disesuaikan dengan Tingkat Klasifikasi Informasi. Tingkat klasifikasi terhadap informasi meliputi Sangat Rahasia (SR), Rahasia (R), Terbatas (T), dan Biasa/Terbuka (B) maupun

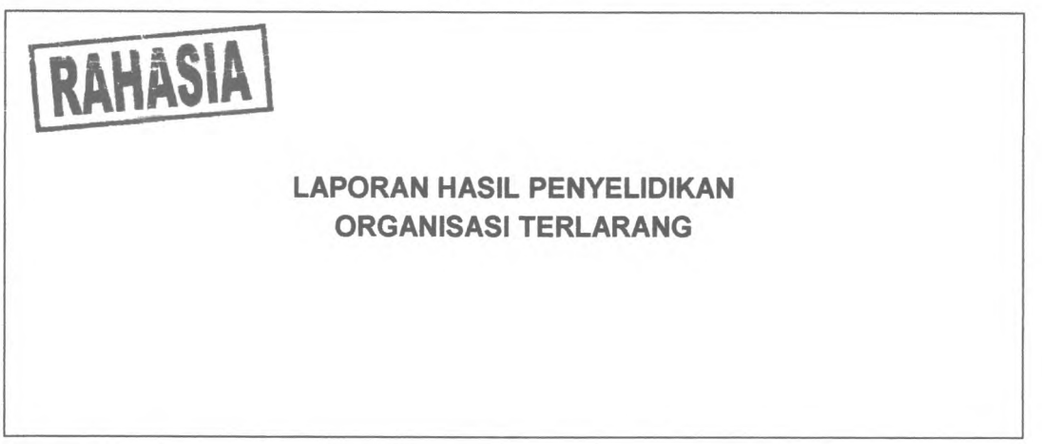
tingkat kepentingan/kecepatan penyampaian informasi seperti Biasa (B), Segera (S), dan Sangat Segera (SS).

Contoh:

1. Pada nomor surat dapat di tulis kode Tingkat Klasifikasi Informasi, misal: **SR**.001/xxx/2017, **R**.002/xxx/2017, **T**.003/xxx/2017, **B**.003/xxx/2017;
2. Pada perihal surat ditulis sifat surat dan derajat surat

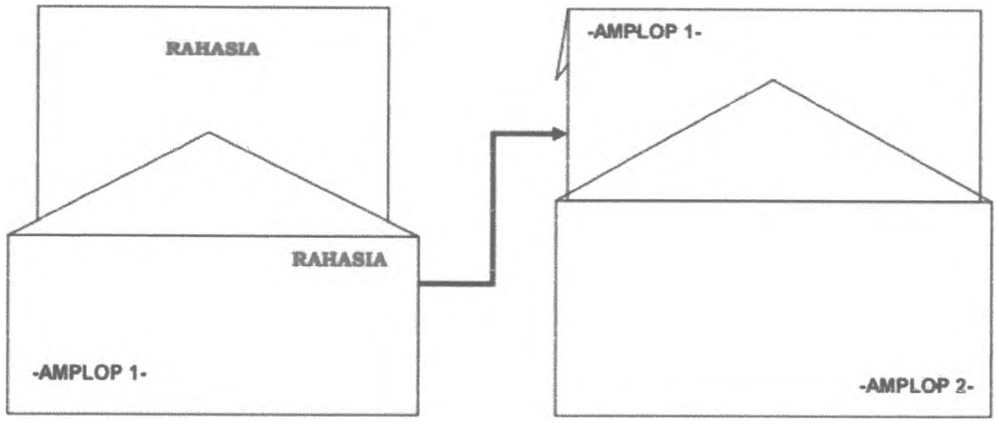
Nomor	: T. 001/xx/04/2019
Lampiran	: 1 berkas
Perihal	: Penyampaian Laporan Bulanan
Sifat	: **TERBATAS** dan **SEGERA**

3. Pada Dokumen Konvensional dapat dicap dengan tulisan SANGAT RAHASIA, RAHASIA, TERBATAS, BIASA.



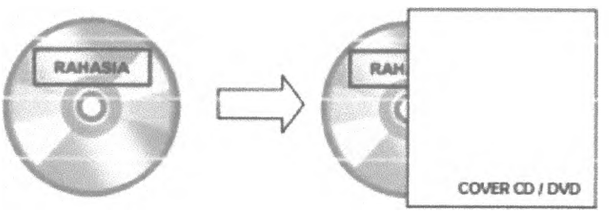
4. Dokumen Kovensional berklasifikasi dimasukkan ke dalam 2 (dua) amplop. Amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (Kilat, Sangat Segera, Segera, dan Biasa). Selanjutnya amplop pertama dimasukkan ke dalam amplop kedua dengan tanda-tanda yang sama kecuali cap klasifikasi.

Contoh:



5. Pada Dokumen Elektronik diberikan label pada *header* atau *footer*atau menggunakan *watermark* di setiap halaman termasuk *cover* kemudian dicetak dan dimintakan pengesahan dengan membubuhkan tanda tangan. Setelah menjadi dokumen cetak dapat dialih mediakan menjadi Dokumen Elektronik kembali dengan menjadi .pdf.

6. Pada Dokumen Elektronik yang dihasilkan oleh sebuah sistem informasi/sistem elektronik, pemberian label dapat di*setting* pada sistem/aplikasi yang digunakan.
7. Media lain, seperti: cd, dvd, magnetic tape, harddrive, dan lain sebagainya. Label ditempelkan pada fisik media penyimpanan dan terlihat dengan kelas, kemudian media penyimpanan tersebut dibungkus lagi tanpa diberi label. Label tersebut juga harus muncul saat informasi yang tersimpan di dalamnya diakses.



C. PENYIMPANAN/PENGARSIPAN

Penyimpanan/pengarsipan dalam rangka penanganan terhadap fisik maupun isi Informasi sesuai dengan Tingkat Klasifikasi Informasi dengan memperhatikan media Informasi. Ketentuan mengenai pengamanan penyimpanan Informasi yakni sebagai berikut:

1. Informasi Dengan Klasifikasi Biasa/Terbuka

   a. Informasi Dalam Bentuk Dokumen Konvensional

Dokumen	:	Tidak ada persyaratan dan prosedur khusus
Pengguna	:	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses
Prasarana dan Sarana	:	Tidak memerlukan prasarana dan sarana khusus

   b. Informasi Dalam Bentuk Dokumen Elektronik

Dokumen	:	*Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitasinformasi
Pengguna	:	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses
Prasarana dan Sarana	:	Tidak memerlukan prasarana dan sarana khusus

2. Informasi Dengan Klasifikasi Terbatas

   a. Informasi Dalam Bentuk Dokumen Konvensional

Dokumen	:	Ada persyaratan dan prosedur dengan memberikan label/cap "TERBATAS"

Pengguna	:	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum
Prasarana dan Sarana	:	Diperlukan tempat penyimpanan yang aman

b. Informasi Dalam Bentuk Dokumen Elektronik

Dokumen	:	1) *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autensitas dokumen. 2) File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau pihak-pihak eksternal, misal diberi *password*.
Pengguna	:	1) Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum 2) Autentikasi pengguna (nama pengguna/password atau ID digital) 3) Penggunaan untuk *log in* pada tingkat individual
Prasarana dan Sarana	:	1) Autentikasi server 2) Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3) *Firewall* dan sistem-sistem serta prosedur-prosedur deteksi terhadap upaya masuk ke dalam sistem informasi/aplikasi tanpa izin.

3. Informasi Dengan Klasifikasi Rahasia

a. Informasi Dalam Bentuk Dokumen Konvensional

Dokumen	:	1) Ada persyaratan dan prosedur rahasia dengan memberikan cap "RAHASIA" pada fisik informasi/dokumen 2) Tidak sembarangan meletakkan dokumen yang bersifat rahasia
Pengguna	:	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum
Prasarana dan Sarana	:	Lokasi aman dengan akses yang terbatas

b. Informasi Dalam Bentuk Dokumen Elektronik

Dokumen	:	1) *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas/otentikasi informasi. 2) File-file elekronik (termasuk database) harus dilindungi terhadap penggunaan internal atau pihak-pihak eksternal, misal diberi *password*.
Pengguna	:	1) Hanya staf yang ditunjuk oleh organisasi dan tingkat di atasnya yang dapat mengakses dokumen tersebut. 2) Autentikasi pengguna (nama pengguna/ *password* atau ID Digital). 3) Penggunaan untuk log in pada tingkat individual.
Prasarana dan Sarana	:	1) Langkah-langkah keamanan dengan *Operating Sytem* khusus atau aplikasi khusus. 2) *Firewall* serta sistem-sistem dan

		prosedur-prosedur deteksi terhadap upaya masuk ke dalam sistem informasi/aplikasi tanpa izin. *Firewall* adalah sistem untuk melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk mengakses komputer atau jaringan.

4. Informasi Dengan Klasifikasi Sangat Rahasia

a. Informasi Dalam Bentuk Dokumen Konvensional

Dokumen	:	1) Ada persyaratan dan prosedur rahasia dengan memberikan cap "SANGAT RAHASIA" pada file arsip. 2) Tidak sembarangan meletakkan dokumen yang bersifat sangat rahasia.
Pengguna	:	Dibatasi hanya untuk Penentu Kebijakan, Pengawasan, dan Penegak Hukum.
Prasarana dan Sarana	:	1) Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses. 2) Penerapan kebijakan "meja harus bersih"

b. Informasi Dalam Bentuk Dokumen Elektronik

Dokumen	:	1) *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas dokumen; 2) *File-file* elektronik (termasuk *database*) harus dilindungi terhadap penggunaan internal oleh pihak-pihak eksternal, misal diberi *password.*

Pengguna	:	1) Hanya staf yang ditunjuk oleh organisasi dan tingkat di atasnya yang dapat mengakses dokumen tersebut 2) Autentikasi pengguna (nama pengguna/*password* atau *ID digital*). 3) Penggunaan untuk *log in* pada tingkat individual.
Prasarana dan Sarana	:	1) Autentikasi server. 2) Langkah-langkah keamanan dengan *operating system* khusus atau aplikasi khusus. 3) *Firewall* dan sistem-sistem atau prosedur deteksi terhadap upaya masuk ke dalam sistem informasi/aplikasi tanpa izin.

Catatan:
Ketentuan tentang *back up* pada Dokumen Elektronik yang berlaku pada dokumen dengan klasifikasi sangat rahasia meliputi juga ketentuan yang berlaku pada dokumen dengan ketentuan rahasia dan terbatas. Ketentuan tentang *back up* pada Dokumen Elektronik yang berlaku pada dokumen dengan klasifikasi terbatas dengan metode back up sesuai dengan Tingkatan Klasifikasi Keamanan.

D. PENGIRIMAN/PUBLIKASI

Pengiriman/penyampaian informasi dalam rangka penanganan terhadap fisik dan isi informasi sesuai dengan tingkat klasifikasi dapat dilakukan melalui pengiriman yang dilindungi. Prosedur pengamanan pengiriman informasi tersebut yakni:

1. Informasi Dengan Klasifikasi Biasa/Terbuka
   a. Informasi Dalam Bentuk Dokumen Konvensional
      Tidak ada persyaratan/prosedur khusus
   b. Informasi Dalam Bentuk Dokumen Elektronik
      Tidak ada prosedur khusus

2. Informasi Dengan Klasifikasi Terbatas
   a. Informasi Dalam Bentuk Dokumen Konvensional

      Amplop segel
   b. Informasi Dalam Bentuk Dokumen Elektronik

      Dikirim menggunakan e-mail yang dilengkapi denganpersandian dan email yang digunakanuntuk kirim terima menggunakan email khusus.

      Contoh:

      1) Misalnya pada e-mail dinas dilengkapi dengan sertifikat elektronik yang berfungsi memberikan fitur keamanan tambahan terhadap pesan yang dikirim berupa enkripsi pesan dan tanda tangan digital pada pesan.
      2) Menggunakan e-mail dengan jalur tertutup yang digunakan khusus untuk komunikasi instansi pemerintah seperti e-mail sanapati.net

3. Informasi Dengan Klasifikasi Rahasia
   a. Informasi Dalam Bentuk Dokumen Konvensional
      1) Menggunakan warna kertas yang berbeda atau kertas dengan karakateristik keamanan tertentu.
      2) Diberi label 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 informasi/dokumen rahasia.
   b. Informasi Dalam Bentuk Dokumen Elektronik
      1) Harus ada konfirmasi dari penerima pesan elektronik atau email.
      2) Menggunakan perangkat yang dikhususkan bagi pesan elektronik atau email rahasia.
      3) Menggunakan persandian atau kriptografi.

4. Informasi Dengan Klasifikasi Sangat Rahasia
   a. Informasi Dalam Bentuk Dokumen Konvensional
      1) Menggunakan warna kertas yang berbeda atau kertas dengan karakateristik keamanan tertentu.
      2) Menggunakan amplop dobel bersegel.
      3) Audit jejak untuk setiap titik akses (misal: tandatangan).
      4) Harus dikirim melalui orang yang sudah diberi wewenang dan tanggng jawab terhadap pengendalian informasi/dokumen rahasia.
   b. Informasi Dalam Bentuk Dokumen Elektronik
      1) Harus ada konfirmasi dari penerima pesan elektronik atau email.
      2) Menggunakan perangkat yang dikhususkan bagi pesan elektronik atau email rahasia.
      3) Menggunakan persandian atau kriptografi.
      4) Harus ada pelacakan akses informasi untuk suatu pesan elektronik atau email.

Sedangkan untuk informasi dalam bentuk dokumen elektronik yang akan dipublikasi melalui ***website*/situs Pemerintah Daerah**, meskipun isi informasinya berklasifikasi "BIASA" atau "TERBUKA" namun untuk tetap menjaga keaslian dan keotentikan informasi, maka dokumen elektronik tersebut dapat diberi tanda tangan elektronik.

Contoh pemanfaatan tanda tangan elektronik dalam mengamankan dokumen elektronik:

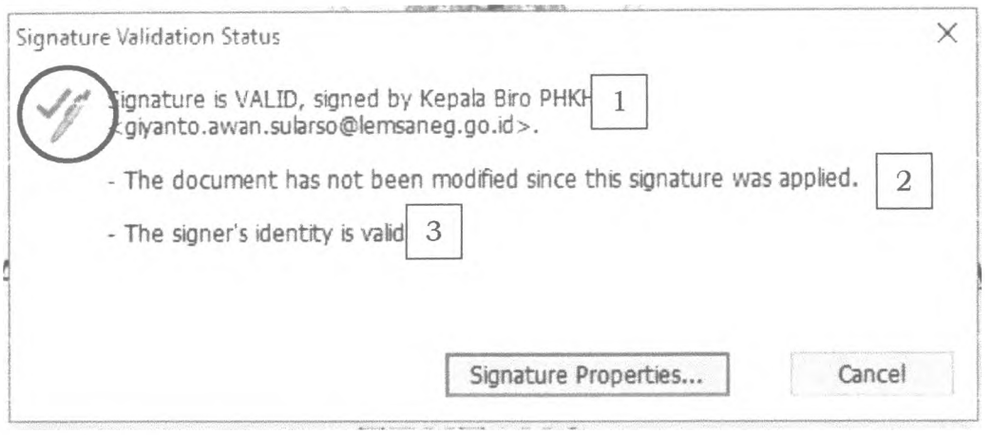
Tanda Tangan Elektonik

Signature valid

Digitally signed by Kepala Biro PHKH
Date: 2017.05.30 14:23:15 +07:00
Reason: Dokumen Lemsaneg
Location: Jakarta

PERATURAN KEPALA LEMBAGA SANDI NEGARA
NOMOR 5 TAHUN 2017
TENTANG
PERUBAHAN KETUJUH ATAS
PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 1 TAHUN 2009

Jika tanda tangan elektronik tersebut kita klik, maka akan muncul notifikasi sebagai berikut:



Keterangan:

Menunjukan bahwa dokumen elektronik Peraturan Kepala Lembaga Sandi Negara tersebut adalah "VALID" dengan rincian sebagai berikut:

1. Menunjukan bahwa, setelah diberikan tanda tangan elektronik, dokumen elektronik tersebut belum pernah di modifikasi alias asli, sehingga isinya dapat dipertanggungjawabkan.
2. Menunjukan bahwa si penandatangan identitasnya adalah valid, karena pada saat pendaftaran tanda tangan elektronik sudah dilakukan verifikasi data e-ktp dan surat keterangan jabatan oleh penyedia layanan dalam hal ini Balai Sertifikat Elektronik (Bsre) Lemsaneg.

   Pada dokumen elektronik yang telah ditandatangani secara elektronik, juga dapat dilihat notifikasi jika dokumen elektronik tersebut sudah pernah di rubah/diedit/dimodifikasi.

PERATURAN KEPALA LEMBAGA SANDI NEGARA
NOMOR 5 TAHUN 2017
TENTANG
PERUBAHAN KETUJUH ATAS
PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 12 TAHUN 2009
TENTANG TATA CARA PENILAIAN DAN PENETAPAN NILAI
TINGKAT PENGAMANAN PERSANDIAN

Keterangan:

Pada contoh di atas, dokumen elektroik tersebut sudah di edit, pada dokumen yang asli berbunyi:

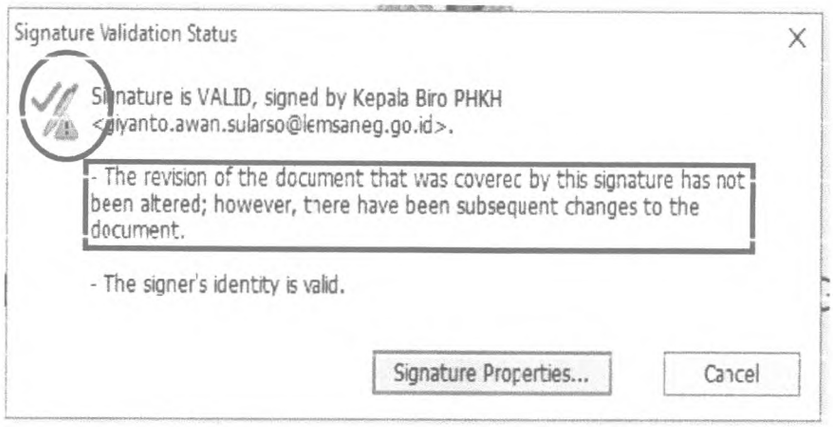
"PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 5 TAHUN 2017 TENTANG PERUBAHAN KETUJUH ATAS PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 1 TAHUN 2009 TENTANG TATA CARA PENILAIAN DAN PENETAPAN NILAI TINGKAT PENGAMANAN PERSANDIAN"

Di edit, sehingga berbunyi:

"PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 5 TAHUN 2017 TENTANG PERUBAHAN KETUJUH ATAS PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 12 TAHUN 2009 TENTANG TATA CARA PENILAIAN DAN PENETAPAN NILAI TINGKAT PENGAMANAN PERSANDIAN"

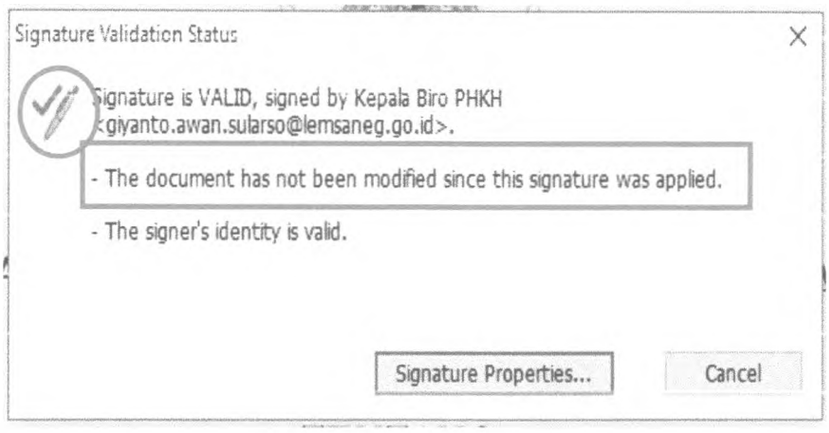
Pada tanda tangan elekronik, saat ada modifikasi/edit/rubah dokumen maka ketika tanda tangan elektronik tersebut di klik maka akan muncul notifkasi yang menyatakan bahwa dokumen tersebut kemungkinan telah dirubah setelah dilakukan penandatangan secara elektronik.

Perbedaan notifikasi tersebut adalah sebagai berikut:



Notifkasi pada dokumen elektronik yang sudah di rubah

Jika dibandingkan maka akan ada notifikasi yang berbeda, yakni



Notifkasi pada dokumen elektronik yang ASLI

E. PEMUSNAHAN

Pemusnahan nformasi merupakan kegiatan untuk menghancurkan Informasi dengan tujuan agar Informasi yang sudah dihancurkan tidak dapat dipulihkan.

Kegiatan pemusnahan Informasi dilakukan terhadap Informasi yang sudah dinyatakan tidak berlaku atau arsip inaktif sesuai dengan masa retensi. Arsip inaktif yang akan dimusnahkan terlebih dahulu harus ditetapkan sebagai daftar arsip musnah dan setelah pelaksanaan pemusnahan harus dibuatkan berita acara. Ketentuan pengamanan terhadap pemusnahan arsip yakni sebagai berikut:

1. Untuk Arsip Dalam Bentuk Dokumen Konvensional
   a. Dihancurkan dengan menggunakan mesin *shredder* dengan model *crosscut.*

b. Dibakar, dengan dipastikan bahwa dokumen yang dibakar telah menjadi abu.

2. Untuk Arsip Dalam bentuk Dokumen Elektronik
   a. Dihancurkan dengan menggunakan aplikasi *file shredder*;
   b. Jika dokumen disimpan dalam media penyimpanan seperti flasdisk/hardisk, media penyimpanan tersebut dapat dihancurkan dengan metode dipotong-potong, dipatahkan, dibakar atau disinari ultraviolet.

BAB IV

PENUTUP

Pedoman ini diharapkan menjadi acuan bagi Perangkat Daerah di lingkungan Pemerintah Provinsi Sulawesi Tenggara guna menjamin jumlah dan mutu Informasi serta mencegah terjadinya kebocoran atau modifikasi Informasi yang dapat disalahgunakan oleh pihak-pihak yang tidak sah.

Plt. GUBERNUR SULAWESI TENGGARA

H. M SALEH LASATA

1	LA ODE ADDI PILI, SE	ASS. II	
2	Drs. H. KUSNADI, MSi	KADIS	
3			
4	EFFENDI KALIMUDDIN SH, MH	KABID HUKUM	