BUPATI CIANJUR
PROVINSI JAWA BARAT

PERATURAN BUPATI CIANJUR

NOMOR 24 TAHUN 2021

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI CIANJUR,

Menimbang :

a. bahwa Pemerintah Daerah berkewajiban mengelola dan melindungi informasi publik dan informasi berklasifikasi yang dimilikinya melalui penyelenggaraan persandian;

b. bahwa sesuai dengan ketentuan lampiran Undang-Undang Nomor 23 Tahun 2014 huruf u, penyelenggaraan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah merupakan kewenangan Daerah Kabupaten/Kota;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian Untuk pengamanan Informasi;

Mengingat :

1. 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);

2. 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);

3. 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);

4. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);

5. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara

Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 6041);

6. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi dilingkungan Pemerintah Daerah Provinsi Kabupaten/Kota (Berita Negara Republik Indonesia Tahun 2017 Nomor 758);
7. Peraturan Daerah Kabupaten Cianjur Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Cianjur (Lembaran Daerah Kabupaten Cianjur Tahun 2016 Nomor 8);
8. Peraturan Bupati Nomor 50 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Perangkat Daerah di Lingkungan Pemerintah Kabupaten Cianjur (Berita Daerah Kabupaten Cianjur Tahun 2016 Nomor 50) sebagimana telah diubah beberapa kali, terakhir dengan Peraturan Bupati Cianjur Nomor 74 Tahun 2019 tentang Perubahan Kedua Atas Peraturan Bupati Cianjur Nomor 2 Tahun 2018 tentang Pembentukan Unit Pelaksana Teknis Daerah di Lingkungan Pemerintah Kabupaten Cianjur (Berita Daerah Kabupaten Cianjur Tahun 2019 Nomor 74);
9. Peraturan Bupati Cianjur Nomor 18 Tahun 2018 tentang Pemanfaatan Sertifikat Elektronik di Pemerintah Kabupaten Cianjur (Berita Daerah Kabupaten Cianjur Tahun 2018 Nomor 18);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan:

1. Daerah Kabupaten selanjutnya disebut Daerah adalah Daerah Kabupaten Cianjur.
2. Pemerintah Daerah Kabupaten selanjutnya disebut Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintah daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Cianjur.
4. Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Cianjur yang selanjutnya disebut Dinas adalah Dinas yang menangani urusan Persandian di Kabupaten Cianjur.
5. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
6. Penyelenggaraan Persandian adalah Jaring Komunikasi Sandi yang selanjutnya disebut (JKS) adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
7. 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 nonelektronik. Informasi yang dimaksud adalah informasi publik, informasi berklasifikasi serta informasi elektronik, dan informasi siber.

8. Informasi publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan Negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Peraturan Perundang-undangan serta informasi lain yang berkaitan dengan kepentingan publik.
9. Informasi berklasifikasi adalah informasi yang dikecualikan menurut peraturan Perundang-undangan.
10. Informasi elektronik adalah informasi 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.
11. Informasi siber adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima melalui jaringan internet dunia maya/siber.

BAB II

ASAS PELAKSANAAN

Pasal 2

JKS berazaskan:

a. asas keamanan, merupakan pengelolaan dan perlindungan informasi berklasifikasi milik Pemerintah Daerah dilaksanakan dengan memperhatikan otorisasi bahwa informasi tersebut hanya dapat diakses oleh orang yang berwenang dalam menjamin kerahasiaan informasi yang dibuat, dikirim, dan disimpan;
b. asas keutuhan, merupakan pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah dilaksanakan dengan memastikan bahwa informasi tersebut tidak dapat diubah tanpa ijin dari pihak yang berwenang, menjamin keutuhan informasi dan tata kelolanya;
c. asas ketersediaan, merupakan pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah dilaksanakan untuk menjamin ketersediaan informasi tersebut saat dibutuhkan, dengan memperhatikan kewenangan pengguna informasi;
d. asas kecepatan dan ketepatan, sebagai pendukung kelancaran tugas dan fungsi unit kerja atau satuan organisasi, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah harus dilakukan tepat waktu dan tepat sasaran;
e. asas efektif dan efisien, merupakan asas pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah perlu dilakukan secara efektif dan efisien sesuai dengan klasifikasinya;
f. asas manfaat, merupakan asas pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah dilaksanakan agar mempunyai manfaat sebesar-besarnya untuk mendukung pengelolaan

dan penyelenggaraan Pemerintahan Daerah;

g. asas profesionalitas, merupakan asas pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah dilaksanakan dengan mengutamakan keahlian yang berdasarkan kode etik, ketentuan peraturan perundang-undangan dan akuntabel; dan

h. asas keterpaduan, merupakan asas pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik Pemerintah Daerah dapat dilaksanakan dan dipadukan dalam mendukung tugas Pemerintahan.

BAB III

RUANG LINGKUP

Pasal 3

(1) Penyelenggaraan JKS, meliputi:

a. penyediaanan analisis kebutuhan JKS;
b. penyediaan kebijakan JKS;
c. pengelolaan dan perlindungan informasi elektronik dan informasi siber;
d. pengelolaan sumber daya persandian meliputi sumber daya manusia, materiil sandi dan jaring komunikasi sandi serta anggaran;
e. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi, informasi elektronik, dan informasi siber;
f. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh Perangkat Daerah; dan
g. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi, informasi elektronik, dan informasi siber.

(2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) huruf a dan huruf b, meliputi:

a. pengamanan fisik;
b. pengamanan logis; dan
c. perlindungan secara administrasi.

(3) Pengamanan informasi elektronik sebagaimana dimaksud pada ayat (1) huruf c, meliputi:

a. pengamanan infrastruktur teknologi, informasi dan komunikasi;
b. pengamanan *server*; dan
c. perlindungan secara *digital signature*.

(4) Pengamanan informasi siber sebagaimana dimaksud pada ayat (1) huruf c, meliputi:

a. pengamanan internet;
b. identifikasi, deteksi, proteksi, penanggulangan dan pemulihan;
c. klarifikasi berita *hoax*; dan
d. layanan terhadap aduan kejahatan dunia maya.

(5) Tata Cara JKS untuk pengamanan informasi, sebagaimana tercantum dalam lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Bupati ini.

BAB IV

ORGANISASI, SUMBER DAYA MANUSIA, SARANA DAN PRASARANA

Pasal 4

(1) Bupati melakukan JKS dengan dibantu oleh Dinas.

(2) Penyelenggaraan JKS sebagaimana dimaksud pada ayat (1) dikoordinir oleh sekurang kurangnya 1 (satu) bidang khusus yang menangani JKS.

Pasal 5

(1) Bidang khusus yang menangani JKS sebagaimana dimaksud dalam Pasal 4 ayat (2), memiliki paling sedikit 2 (dua) personil yang telah mempunyai sertifikat kualifikasi ahli sandi.

(2) Sertifikat kualifikasi ahli sandi sebagaimana dimaksud pada ayat (1), diperoleh dengan pendidikan dan latihan ahli sandi yang diselenggarakan oleh Pusat Pendidikan dan Pelatihan Badan Siber dan Sandi Negara.

Pasal 6

Bidang yang menangani urusan persandian harus menyediakan sarana prasarana persandian sesuai dengan ketentuan peraturan perundang-undangan.

BAB V

PEMBIAYAAN

Pasal 7

Pembiayaan JKS dibebankan kepada anggaran pendapatan dan belanja daerah.

BAB VI

PENUTUP

Pasal 8

Peraturan Bupati ini berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan perundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Cianjur.

Ditetapkan di Cianjur
pada tanggal 21 April 2021

Plt. BUPATI CIANJUR,

ttd.

HERMAN SUHERMAN

Diundangkan di Cianjur
pada tanggal 21 April 2021

Pj. SEKRETARIS DAERAH,

DODIT ARDIAN PANCAPANA.

BERITA DAERAH KABUPATEN CIANJUR TAHUN 2021 NOMOR 24

LAMPIRAN PERATURAN BUPATI CIANJUR

NOMOR : 24TAHUN 2021

TENTANG : PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN NFORMASI

TATA CARA

1. Penyediaan kebijakan JKS

   Kebijakan JKS di Daerah meliputi:

   a. Kebijakan tata kelola persandian, diantaranya:

      1) Pengelolaan dan perlindungan informasi berklasifikasi;
      2) Tata cara klasifikasi tingkat kerahasiaan informasi;
      3) Pengendalian akses terhadap informasi;
      4) Pengelolaan jaringan komunikasi sandi.

   b. Kebijakan operasional pengamanan persandian, diantaranya:

      1) Pengamanan kerahasiaan, keutuhan, keaslian, dan nir penyangkalan informasi dan sistem menggunakan sertifikat elektronik;
      2) Pengamanan perangkat dan fasilitas pengolahan data dan informasi;
      3) Pengamanan jaring komunikasi sandi;
      4) Pengamanan informasi elektronik;
      5) Pengamanan informasi siber;
      6) Pelaksanaan dan pengamanan*video conference*;
      7) Pelaksanaan IT Security Assessment, kontra penginderaan/sterillisasi dan *jamming;*
      8) Pelayanan satu pintu kirim terima informasi berklasifikasi;
      9) Pelayanan operasi Patroli Siber;
      10) Pelayanan aduan kejahatan siber.

   c. Kebijakan pengelolaan Sumber Daya Persandian, diantaranya

      1) Pemenuhan kompetensi dan kuantitas SDM;
      2) Pengendalian akses terhadap materiil sandi dan jaring komunikasi sandi;
      3) Pemeliharaan dan perbaikan umum materiil sandi;
      4) Penyediaan materil sandi dan jaringan komunikasi sandi;
      5) Peningkatan kesadaran, pemahaman akan pengamanan informasi.

   d. Kebijakan pengawasan dan evaluasi penyelenggaraan persandian:

      1) Pengawasan dan evaluasi yang bersifat rutin dan insidentil;
      2) Pengawasan dan evaluasi yang bersifat tahunan;
      3) Pengawasan dan evaluasi informasi digital elektronik/siber;
      4) Mengevaluasi tingkat keamanan IT;
      5) Mengevaluasi tingkat kesadaran, pemahaman kemanan informasi;
      6) Mengevaluasi tingkat ketersediaan sumber daya persandian, SDM dan Peralatan persandian.

2. Penyediaan Analisis Kebutuhan Persandian untuk Pengamanan Informasi. Kegiatan analisis kebutuhan penyelenggaraan persandian, meliputi:

   a. Identifikasi pola hubungan komunikasi yang digunakan oleh Pemerintah Daerah, diantaranya meliputi:

      1) Mengidentifikasi pola hubungan komunikasi Bupati dan pejabat

LAMPIRAN PERATURAN BUPATI CIANJUR

NOMOR : 24TAHUN 2021

TENTANG : PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN NFORMASI

TATA CARA

1. Penyediaan kebijakan JKS

   Kebijakan JKS di Daerah meliputi:

   a. Kebijakan tata kelola persandian, diantaranya:

      1) Pengelolaan dan perlindungan informasi berklasifikasi;
      2) Tata cara klasifikasi tingkat kerahasiaan informasi;
      3) Pengendalian akses terhadap informasi;
      4) Pengelolaan jaringan komunikasi sandi.

   b. Kebijakan operasional pengamanan persandian, diantaranya:

      1) Pengamanan kerahasiaan, keutuhan, keaslian, dan nir penyangkalan informasi dan sistem menggunakan sertifikat elektronik;
      2) Pengamanan perangkat dan fasilitas pengolahan data dan informasi;
      3) Pengamanan jaring komunikasi sandi;
      4) Pengamanan informasi elektronik;
      5) Pengamanan informasi siber;
      6) Pelaksanaan dan pengamanan*video conference*;
      7) Pelaksanaan IT Security Assessment, kontra penginderaan/sterillisasi dan *jamming;*
      8) Pelayanan satu pintu kirim terima informasi berklasifikasi;
      9) Pelayanan operasi Patroli Siber;
      10) Pelayanan aduan kejahatan siber.

   c. Kebijakan pengelolaan Sumber Daya Persandian, diantaranya

      1) Pemenuhan kompetensi dan kuantitas SDM;
      2) Pengendalian akses terhadap materiil sandi dan jaring komunikasi sandi;
      3) Pemeliharaan dan perbaikan umum materiil sandi;
      4) Penyediaan materil sandi dan jaringan komunikasi sandi;
      5) Peningkatan kesadaran, pemahaman akan pengamanan informasi.

   d. Kebijakan pengawasan dan evaluasi penyelenggaraan persandian:

      1) Pengawasan dan evaluasi yang bersifat rutin dan insidentil;
      2) Pengawasan dan evaluasi yang bersifat tahunan;
      3) Pengawasan dan evaluasi informasi digital elektronik/siber;
      4) Mengevaluasi tingkat keamanan IT;
      5) Mengevaluasi tingkat kesadaran, pemahaman kemanan informasi;
      6) Mengevaluasi tingkat ketersediaan sumber daya persandian, SDM dan Peralatan persandian.

2. Penyediaan Analisis Kebutuhan Persandian untuk Pengamanan Informasi. Kegiatan analisis kebutuhan penyelenggaraan persandian, meliputi:

   a. Identifikasi pola hubungan komunikasi yang digunakan oleh Pemerintah Daerah, diantaranya meliputi:

      1) Mengidentifikasi pola hubungan komunikasi Bupati dan pejabat

daerah lainnya yang sedang dilaksanakan.

2) Mengidentifikasi alur informasi yang dikomunikasikan antar perangkat daerah; dan

3) Mengidentifikasi dan/atau menyediakan sarana dan prasarana teknologi informasi dan komunikasi yang digunakan oleh Bupati dan/atau pejabat daerah lainnya.

b. Analisis pola hubungan komunikasi sandi yang diperlukan berdasarkan hasil identifikasi pola hubungan komunikasi yang sudah ada sebagaimana dimaksud pada huruf a meliputi:

1) Mengidentifikasi pengelola layanan penyelenggaraan persandian Identifikasi pengelola yaitu kegiatan untuk mengidentifikasi personil dan kompetensi yang dibutuhkan dalam menyelenggarakan kegiatan persandian.

2) Mengidentifikasi Sarana dan Prasarana

a) Materiil Sandi dan JKS

(1) materiil Sandi
Identifikasi Materiil Sandi meliputi identifikasi terhadap kebutuhan peralatan sandidan kunci sistem sandi yang didasarkan pada kondisi infrastuktur, jenis komunikasi, dan hierarki komunikasinya.

(2) JKS
Identifikasi JKS meliputi identifikasi terhadap:

(a) Perangkat Daerah yang akan terhubung dalam JKS termasuk didalamnya unit kerja dalam Perangkat Daerah yang akan mengoperasikan peralatan sandi.

(b) Pejabat Pemerintah Daerah yang akan terhubung dalam JKS termasuk didalamnya penentuan hierarki komunikasi.

(c) Infrastruktur komunikasi yang ada di Pemerintah Daerah.

b) alat pendukung utama Persandian
Identifikasi APU Persandian meliputi identifikasi kebutuhan terhadap perangkat yang mendukung penyelenggaran persandian.

c) tempat kegiatan sandi
Identifikasi Tempat Kegiatan Sandi meliputi identifikasi kebutuhan pengamanan terhadap tempat yang digunakan untuk operasional persandian sesuai dengan jenis komunikasinya.

d) sarana penunjang
Identifikasi Sarana Penunjang meliputi identifikasi kebutuhan terhadap peralatan yang mendukung dalam kegiatan penyelenggaraan persandian, meliputi alat tulis kantor dan sarana pengolah data.

3) identifikasi pembiayaan
Identifikasi pembiayaan meliputi identifikasi anggaran yang dibutuhkan oleh penyelenggara persandian di Pemerintah Daerah dalam periode waktu satu tahun anggaran.

c. Menetapkan hasil identifikasi dan analisis pola hubungan komunikasi sandi melalui Peraturan Kepala Dinas, yang berisi entitas yang terhubung maupun yang tidak terhubung dalam pola hubungan komunikasi tersebut, serta tugas dan tanggung jawab masing-masing entitas terhadap fasilitas dan layanan yang diberikan.

3. Pengelolaan Dan Perlindungan Informasi
Pengelolaan dan perlindungan informasi di Pemerintah Daerah meliputi hal-hal sebagai berikut:

a. Fasilitasi penentuan tingkat kerahasiaan informasi berklasifikasi.

b. Pengelolaan dan perlindungan informasi publik yang dikecualikan/ informasi berklasifikasi.

1) Pengelolaan informasi publik yang dikecualikan/informasi berklasifikasi meliputi pembuatan, pemberian label, pengiriman, penyimpanan dan Pemusnahan.

a) Pembuatan Informasi Berklasifikasi

1.1. 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*).

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

1.3. Konsep Informasi Berklasifikasi tidak boleh disimpan dan harusdihancurkan secara fisik maupun lojik (*logical security*).

1.4. Dokumen elektronik berklasifikasi yang sudah disahkan disimpandalam bentuk yang tidak dapat diubah/ dimodifikasi (*read only*).

1.5. Penggandaandan/atau perubahan Informasi Berklasifikasi dilakukanharus 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.

1.1. 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;

1.2. Surat elektronik: Label ditulis pada baris *subject* pada *header* surat elektronik;

1.3. 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*;

1.4. Database dan aplikasi bisnis: Label diberikan dalam metadata sistem/aplikasi;

1.5. 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.

c) Pengiriman Informasi Berklasifikasi

1.1. Pengiriman dokumen elektronik berklasifikasi

i. Dokumen Elektronik berklasifikasi dikirimkan dengan menggunakan teknik kriptografi dan melalui saluran komunikasi yang aman. Contoh Dokumen elektronik dienkripsi dengan aplikasi enkripsi yang direkomendasikan oleh Badan Siber dan Sandi Nasional.

ii. 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.

1.2. Pengiriman dokumen cetak berklasifikasi:

i. Dokumen cetak berklasifikasi dikirim melalui kurir atau jasa pengiriman tercatat;

ii. 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;

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

d) Penyimpanan Informasi Berklasifikasi:

1.1. Penyimpanan Dokumen Elektronik berklasifikasi

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

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

iii. Prosedur pengamanan Dokumen Elektronik berklasifikasi harus sesuai dengan klasifikasinya;

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

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

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

1.2. Penyimpanan dokumen cetak berklasifikasi

i. Dokumen cetak berklasifikasi harus disimpan dalam brankas yang memiliki kunci kombinasi, atau media penyimpanan yang aman, minimal tertutup dari pandangan orang lain.

ii. Dokumen cetak berklasifikasi harus diarsip secara khusus dengan tertib dan rapi sesuai prosedur arsip yang berlaku.

e) Pemusnahan Informasi Berklasifikasi

1.1. Pemusnahan Dokumen Elektronik Berklasifikasi

i. Melakukan penilaian bahwa informasi sudah tidak lagi digunakan

ii. Adanya usulan pemusnahan oleh pejabat berwenang

iii. Pengelola Informasi memberikan persetujuan untuk melakukan pemusnahan

iv. Penerbitan Surat Keputusan Pemusnahan

v. Melakukan pemusnahan dengan aplikasi yang aman dan sudah direkomendasikan oleh Badan Siber dan Sandi Nasional

vi. Menandatangani BAST Pemusnahan

i. Melakukan penilaian bahwa informasi sudah tidak lagi digunakan

ii. Adanya usulan pemusnahan oleh pejabat berwenang

iii. Pengelola Informasi memberikan persetujuan untuk melakukan pemusnahan

iv. Penerbitan Keputusan Pemusnahan

v. Melakukan pemusnahan secara fisik sesuai dengan ketentuan yang berlaku

vi. Menandatangani BAST Pemusnahan

2) Perlindungan informasi publik yang dikecualikan/informasi berklasifikasi meliputi:

(a) Perlindungan fisik dilakukan melalui kendali akses ruang, pemasangan teralis dan kunci ganda, pemasangan CCTV, IP Camera;

(b) Perlindungan administrasi
Pelaksanaan perlindungan administrasi dilakukan dengan berpedoman pada kebijakan, standar, dan prosedur operasional pengamanan informasi publik yang dikecualikan/informasi berklasifikasi;

(c) Perlindungan lojik (*logical security*):

(1) Perlindungan lojik (*logical security*) menggunakan teknik kriptografi dan steganografi untuk memenuhi aspek: kerahasiaan, keutuhan, otentikasi, dan nir penyangkalan;

(2) Perlindungan lojik (*logical security*) yang menggunakan teknik kriptografi dan steganografi harus memenuhi standar dan direkomendasikan oleh Badan Siber dan Sandi Nasional;

(3) Untuk menambah keamanan database terutama yang disimpan secara elektronik baik di Komputer khusus maupun server, perlu ditambahkan perlindungan lojik antara lain:

1.1. Pemasangan firewall pada jaringan data yang terhubung di server,
1.2. Pemasangan Tools Detection,
1.3. Pemasangan antivirus,
1.4. Pengamanan/pemanfaatan user/password,
1.5. Aplikasi keamanan lain yang telah teruji kehandalannya.

(4) Dalam rangka pencegahan dan penanggulangan perlindungan logic, Bagian/seksi Persandian bekerjasama dengan Unit Pengelola Teknologi Informasi di lingkup Pemerintah Daerah dengan pembinaan dari Badan Siber dan Sandi Nasional.

(d) Pengelolaan dan perlindungan informasi publik/terbuka melalui penerapan sertifikat elektronik untuk menyediakan layanan keutuhan, otentikasi dan anti penyangkalan.

(e) Penyelenggaraan Jaring Komunikasi Sandi (JKS) untuk pengamanan informasi berklasifikasi.

(f) Penerapan sertifikat elektronik dan enkripsi pada informasi berklasifikasi.

4. Pengelolaan Sumber Daya Persandian Pengelolaan Sumber Daya Persandian terdiri atas:

a. Pengelolaan Sumber Daya Manusia

Pengelolaan Sumber Daya Manusia meliputi:

1) Perencanaan kebutuhan sumber daya manusia
Perencanaan kebutuhan sumber daya manusia yang bertugas di bidang persandian disusun dengan memperhatikan jumlah dan kompetensi yang dibutuhkan. Dalam kegiatan perencanaan ini, Bagian yang menangani persandian dapat menyusun Analisis Beban Kerja dan Formasi Jabatan Fungsional Sandiman serta mengajukan usulan kebutuhan tersebut kepada Badan Kepegawaian Daerah.

2) Pengembangan kompetensi sumber daya manusia Pengembangan kompetensi sumber daya manusia yang bertugas
di bidang persandian diantaranya melalui Diklat Fungsional Sandiman (Pembentukan dan Penjenjangan), Diklat Teknis Sandi, Bimbingan Teknis/Asistensi/*Workshop*/Seminar terkait dengan Persandian dan Teknologi Informasi serta bidang ilmu lainnya yang dibutuhkan.

b. Pengelolaan Sarana dan Prasarana, meliputi:

1) Pengelolaan Materiil Sandi dan JKS Pengelolaan terhadap Materiil Sandi dan JKS meliputi:

a) Pemenuhan terhadap kebutuhan materiil sandi yang akan digunakan dalam penyelenggaraan JKS eksternal oleh Pemerintah Daerah dapat difasilitasi oleh Badan Siber dan Sandi Nasional dengan mengajukan permohonan kepada Badan Siber dan Sandi Nasional sesuai hasil analisis kebutuhan.

b) Pemenuhan kebutuhan materiil sandi yang akan digunakan dalam penyelenggaraan jaring komunikasi sandi sesuai dengan analisis kebutuhan.

c) Penyimpanan materiil sandi (peralatan sandi dan kunci sistem sandi) berdasarkan ketentuan yang berlaku.

2) Pengelolaan APU Persandian

Pengelolaan terhadap APU Persandian meliputi:

a) Pemenuhan APU Persandian dapat dilakukan secara mandiri dengan wajib meminta rekomendasi dari Badan Siber dan Sandi Nasional atau dapat mengajukan permohonan pemanfaatan APU Persandian kepada Badan Siber dan Sandi Nasional.

b) Penyimpanan
Penyimpanan APU Persandian dengan memperhatikan syarat-syarat keamanan antara lain:

(1) Lokasi penyimpanan APU Persandian harus dilengkapi kendali akses untuk mencegah risiko kehilangan, kerusakan, dan manipulasi.

(2) APU Persandian dilarang digunakan, dipinjam, atau dibawa ke luar ruang kerja atau kantor tanpa ijin dari Penanggung Jawab pengelola Materiil Sandi.

c) Pemeliharaan
Pemeliharaan APU Persandian dilaksanakan dengan melakukan perawatan dan perbaikan (bila ada kerusakan) sesuai dengan kewenangan yang dimiliki.

5. Penyelenggaraan operasional dukungan persandian untuk pengamanan informasi, yang dapat dilaksanakan Pemerintah Daerah, diantaranya:

(a) *Jamming*

1) *Jamming* merupakan kegiatan mengacak sinyal komunikasi sehingga pelaksanaan rapat tersebut dapat berjalan tertib dan menghindari tindakan-tindakan yang tidak diinginkan melalui pemanfaatan sinyal komunikasi peserta rapat.

2) Ruang Lingkup

a) Unit pelayanan yang menyelenggarakan pengkoordinasian *Jamming* terhadap peserta rapat terbatas adalah Bidang Persandian di Dinas;

b) Pelaksana adalah seluruh pejabat/pegawai pada Bidang Persandian di Dinas dan Pengamanan yang secara teknis dan administratif memiliki tugas dan tanggung jawab langsung dalam pengkoordinasian *Jamming* terhadap kegiatan rapat terbatas;

c) Penanggung jawab pelayanan adalah Kepala Dinas;

d) Pengguna pelayanan adalah Pejabat Daerah dan Pejabat Lainnya;

e) Keluaran (*output*) pelayanan adalah dokumen dan produk naskah dinas kegiatan *Jamming*;

f) Kemanfaatan (*outcome*) pelayanan adalah terselenggaranya *jamming* terhadap rapat terbatas pejabat daerah dan Pejabat Lainnya di Pemerintah Daerah dengan aman dari ancaman non fisik berupa penyadapan jaringan komunikasi dengan memanfaatkan kemajuan teknologi yang berkembang saat ini dan masa yang akan datang.

3) Prosedur Layanan

a) Kegiatan Jamming dilakukan dengan 2 (dua) cara yaitu:

i. Secara periodik yaitu 1 kali dalam sebulan; dan
ii. Permintaan dari pejabat.

b) Kegiatan *jamming* tersebut dilakukan dengan terlebih dahulu mengajukan ijin dari pejabat pemilik ruang rapat.

c) Setelah mendapatkan ijin, Tim akan melaksanakan kegiatan jamming di ruang rapat terbatas pejabat daerah dan Pejabat Lainnya di Pemerintah Daerah. Kegiatan ini berlangsung sampai dengan rapat tersebut selesai.

(b) Kontra Penginderaan/ *sterillisasi*

1) Kontra Penginderaan dilakukan terhadap ruangan-ruangan yang digunakan oleh Pimpinan Pemerintah Daerah untuk penyampaian informasi berklasifikasi;

2) Kegiatan Kontra Penginderaan dilakukan melalui pemeriksaan fisik ruangan dengan memperhatikan barang-barang di dalam ruangan yang berpotensi menjadi peralatan *surveillance*.

3) Ruang Lingkup

a) Unit pelayanan yang menyelenggarakan pengkoordinasian Kontra Penginderaan terhadap Pejabat Daerah dan pejabat lainnya adalah Bidang Persandian di Dinas;

b) Pelaksana adalah seluruh pejabat/pegawai pada Bidang Dinas dan Pengamanan yang secara teknis dan administratif memiliki tugas dan tanggung jawab langsung dalam pengkoordinasian Kontra Penginderaan terhadap Pejabat Daerah dan Pejabat lainnya;

c) Penanggung jawab pelayanan adalah Kepala Dinas Komunikasi Informatika dan Persandian Daerah;

d) Pengguna pelayanan adalah Pejabat Daerah dan Pejabat Lainnya;

e) Keluaran (*output*) pelayanan adalah dokumen dan produk naskah dinas kegiatan Kontra Penginderaan;

f) Kemanfaatan (*outcome*) pelayanan adalah terselenggaranya kegiatan Pejabat Daerah dan Pejabat lainnya dengan aman dari ancaman non fisik berupa penyadapan jaringan komunikasi dengan memanfaatkan kemajuan teknologi yang berkembang saat ini dan masa yang akan datang.

4) Prosedur Layanan

a) Kegiatan Kontra Penginderaan dilakukan dengan 2 (dua) cara yaitu:

i. Secara periodik yaitu 2 kali dalam setahun; dan
ii. Permintaan dari pejabat.

b) Kegiatan Kontra Penginderaan tersebut dilakukan dengan terlebih dahulu mengajukan ijin dari pejabat pemilik ruang kerja atau rumah dinas;

c) Setelah proses pengajuan disetujui Tim akan mengatur jadwal pelaksanaan kegiatan Kontra Penginderaan dengan berkoordinasi dengan Tim Badan Siber dan Sandi Negara. Penentuan jadwal ini bersifat rahasia hanya diketahui oleh Tim Kontra Penginderaan dan Pejabat pemilik ruangan, hal ini dimaksudkan agar proses Kontra Penginderaan berjalan lancar dan hasil yang di dapat lebih akurat;

d) Setelah jadwal ditentukan, Tim akan melaksanakan kegiatan Kontra Penginderaan di ruang kerja atau rumah dinas secara menyeluruh di setiap sudut ruang atau tempat dimana dicurigai ada penyadap. Kegiatan ini berlangsung sampai 1 hari tergantung luas atau banyaknya ruangan;

e) Analisis kegiatan Kontra Penginderaan dilakukan saat melangsungkan kegiatan dan setelah kegiatan. Tujuan analisis ini untuk mengetahui ada tidaknya alat penyadap di tempat tersebut yang terekam alat *Counter Surveillance;*

f) Setelah melakukan analisis yang mendalam Tim melaporkan hasil dari kegiatan sterilisasi penyadapan itu kepada Pejabat pemilik ruangan atau Rumah dinas dan melakukan evaluasi mengenai kekurangan, kendala, hambatan dan rintangan yang dialami Tim pada tempat kegiatan sterilisasi penyadapan. Tim selanjutnya memberikan Solusi pemecahan masalah yang ada untuk memperbaiki agar dikemudian hari bisa menghindari dari resiko penyadapan.

b. Pelaksanaan Kegiatan *Assessment* Keamanan Sistem Informasi

1) Kegiatan *Assessment* Keamanan Sistem Informasi dilakukan dengan melakukan pemeriksaan terhadap ada atau tidaknya celah kerawananan pada Sistem Informasi.

2) Pemerintah Daerah melakukan kegiatan *Assessment* Keamanan Sistem Informasi setelah berkoordinasi dan mengajukan permohonan *Assessment* Keamanan Sistem Informasi kepada Badan Siber dan Sandi Negara.

3) Ruang Lingkup

a) Unit pelayanan yang menyelenggarakan pengkoordinasian kegiatan *Assessment* Keamanan Sistem Informasi terhadap data/ informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah adalah Bidang Persandian Dinas;

b) Pelaksana adalah seluruh pejabat/pegawai pada Bidang Persandian di Dinas dan Pengamanan yang secara teknis dan administratif memiliki tugas dan tanggung jawab langsung dalam pengkoordinasian kegiatan *Assessment* Keamanan Sistem Informasi terhadap data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah;

c) Penanggung jawab pelayanan adalah Kepala Dinas;

d) Sasaran yang hendak dicapai adalah Terhindarnya data/ informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah dari ancaman dan kerawanan yang mungkin timbul;

e) Pengguna pelayanan adalah Seluruh Perangkat Daerah;

f) Keluaran *(output)* pelayanan adalah Laporan teknis dan rekomendasi dari hasil kegiatan *Assessment* Keamanan Sistem Informasi;

g) Kemanfaatan *(outcome)* pelayanan adalah terselenggaranya kegiatan *Assessment* Keamanan Sistem Informasi terhadap data/ informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah dari ancaman yang ditimbulkan oleh pemanfaatan teknologi Telekomunikasi dan Elektronika berupa *phising, virus, malicious malware* dan lainnya.

4) Prosedur Layanan

a) Kegiatan *Assessment* Keamanan Sistem Informasi dilakukan terhadap Perangkat Daerah di Pemerintah Daerah yang mengajukan permintaan;

b) Setelah terdapat permintaan, pelaksanan kegiatan *Assessment* Keamanan Sistem Informasi akan dikoordinasikan dengan pihak BSSN untuk penjadwalan;

c) Setelah mendapatkan penjadwalan, Tim akan melaksanakan kegiatan *Assessment* Keamanan Sistem Informasi dengan skenario yang telah disepakati bersama;

d) Tim menyusun laporan hasil dan rekomendasi dari kegiatan *Assessment* Keamanan Sistem Informasi.

c. Layanan Sertifikat Elektronik

1) Pelaksanaan kegiatan layanan sertifikat elektronik dapat dilakukan oleh Pemerintah Daerah jika telah memenuhi persyaratan dan telah diberikan kewenangan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara;

2) Kegiatan layanan sertifikat elektronik yang dilaksanakan meliputi:

a) Pendaftaran dan permohonan penerbitan, pencabutan dan pembaharuan sertifikat elektronik;

b) Pengembangan aplikasi pendukung penggunaan sertifikat elektronik;

c) Bimbingan teknis dan sosialisasi terkait penggunaan sertifikat elektronik;

d) Pengawasan dan evaluasi penggunaan sertifikat elektronik.

3) Ruang Lingkup

a) Unit pelayanan yang menyelenggarakan pengkoordinasian kegiatan layanan sertifikat elektronik terhadap data/informasi, aplikasi, data base, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah adalah Bidang Persandian di Dinas;

b) Pelaksana adalah seluruh pejabat/pegawai pada bidang persandian yang dibentuk oleh di Dinas dan Pengamanan yang secara teknis dan administratif memiliki tugas dan tanggung jawab langsung dalam pengkoordinasian kegiatan pengamanan siber yang dimiliki oleh Pemerintah Daerah;

c) Penanggung jawab pelayanan adalah Kepala Dinas;

d) Sasaran yang hendak dicapai adalah terhindarnya data/ informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah dari ancaman dan kerawanan yang mungkin timbul;

e) Pengguna pelayanan adalah seluruh Perangkat Daerah di Daerah;

f) Keluaran (*output*) pelayanan adalah Laporan teknis dan rekomendasi dari hasil kegiatan layanan sertifikat elektronik.

g) Kemanfaatan (*outcome*) pelayanan adalah terselenggaranya kegiatan layanan sertifikat elektronik terhadap data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah dari ancaman yang ditimbulkan oleh pemanfaatan teknologi Telekomunikasi dan Elektronika berupa ancaman dari pihak yang tidak sah, kebocoran data, pemalsuan data dan penyangkalan.

4) Prosedur Layanan

a) Kegiatan layanan sertifikat elektronik dilakukan terhadap Perangkat Daerah di Pemerintah Daerah yang mengajukan permintaan;

b) Setelah terdapat permintaan, pelaksanan kegiatan layanan sertifikat elektronik akan dikoordinasikan dengan pihak Badan Siber dan Sandi Negara untuk penjadwalan;

c) Setelah mendapatkan penjadwalan, Tim akan melaksanakan kegiatan layanan sertifikat elektronik dengan skenario yang telah disepakati bersama;

d) Tim menyusun laporan hasil dan rekomendasi dari kegiatan layanan sertifikat elektronik.

d. Penyelenggaraan *Security Operation Center* (SOC)
Penyelenggaraan SOC dapat dilakukan secara mandiri namun tetap berkerjasama dengan Badan Siber dan Sandi Negara sebagai instansi pembina dimana infrastruktur SOC pada Pemerintah Daerah dapat terhubung dengan Badan Siber dan Sandi Negara, sehingga kegiatan akan berlangsung responsif.

6. Pengamanan informasi siber

Penyelenggaraan operasional informasi siber dapat dilaksanakan dengan membentuk tim satuan tugas *Cyber Insident Response Team (CIRT)* diantaranya mempunyai tugas fungsi yang dijabarkan dalam kelompok kerja (pokja) sebagai berikut:

a. Tim satuan tugas *Cyber Incident Renponse Team* (CIRT), yang tugasnnya adalah sebagai berikut :

1) Operasi Patroli Siber; merupakan kegiatan untuk identifikasi, deteksi, proteksi, penanggulangan dan pemulihan serta melaksanakan klarifikasi dari ancaman sesatnya berita Hoax, modus

penipuan dan pembunuhan karakter, pencemaran anama baik, ujaran kebencian, isu sara, pemecah belah NKRI, Bhineka tunggal ika, Pancasila dan UUD 1945;

2) Melaksanakan layanan aduan kejahatan siber, merupakan kegiatan pelayanan kepada masyarakat sebagai korban kejahatan siber, modus penipuan dan pembunuhan karakter;

3) Melaksanakan pembinaan pengamanan informasi siber, merupakan kegiatan usaha merubah mindset generasi millennial sekolah-sekolah, organisasi elemen masyarakat dan jajaran pimpinan/staf perangkat daerah di Daerah dari ancaman hoax;

4) Melaksanakan pengawasan dan evaluasi pengamanan informasi siber, merupakan suatu kegiatan pengawasan dan evaluasi pengamanan informasi siber yang dilaksanakan oleh kelompok kerja satuan tugas *Cyber Insident Renponse Team*;

5) Melaksanakan publikasi dan dokumentasi kegiatan satgas CIRT dalam upaya klarifikasi dan memerangi berita hoax;

b. Ruang Lingkup

1) Unit pelayanan satgas CIRT yang menyelenggarakan pengkoordinasian kegiatan layanan pengamanan siber dalam rangka mengawal generasi millennial dari ancaman berita hoax yang dimiliki oleh Pemerintah Daerah adalah Bidang Persandian di Dinas;

2) Pelaksana adalah seluruh tim stekaholder satgas CIRT yang dibentuk oleh Bidang Persandian di Dinas dan Pengamanan yang secara teknis dan administratif memiliki tugas dan tanggung jawab langsung dalam pengkoordinasian kegiatan pengamanan siber yang dimiliki oleh Pemerintah Daerah;

3) Penanggung jawab pelayanan adalah Kepala Dinas;

4) Sasaran yang hendak dicapai adalah terhindarnya data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah dari ancaman dan kerawanan siber dan hoax yang mungkin timbul;

5) Pengguna pelayanan adalah Seluruh Perangkat Daerah di Daerah;

6) Keluaran (*output*) pelayanan adalah terlaksananya pengamanan informasi siber dari ancaman hoax dan kejahatan siber;

7) Kemanfaatan (*outcome*) pelayanan adalah terselenggaranya pengamanan informasi siber, dan kegiatan layanan aduan kejahatan siber terhadap data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Daerah dari ancaman hoax dan kejahatan siber, modus penipuan dan pembunuhan karater, yang ditimbulkan oleh pemanfaatan teknologi, informasi, telekomunikasi di dunia maya/media sosial berupa ancaman sesatnya hoax dari pihak siber luar.

c. Prosedur layanan

a) Operasi Patroli Siber

1) Membuat akun resmi CIRT Daerah di jejaring media sosial;

2) Melakukan Kegiatan operasi patroli siber oleh tim satgas CIRT

pokja operasi patroli siber di jejaring media sosial;

3) Melakukan identifikasi, deteksi, proteksi, penanggulangan dan pemulihan serta melaksanakan klarifikasi dari ancaman sesatnya berita Hoax, modus penipuan dan pembunuhan karakter, pencemaran anama baik, ujaran kebencian, isu sara, pemecah belah NKRI, Bhineka tunggal ika, Pancasila dan UUD 1945;

4) Membuat laporan hasil dan rekomendasi dari kegiatan operasi Patroli siber.

b) Layanan Aduan Kejahatan Siber

1) Menerima layanan aduan korban kejahatan siber, secara langsung maupun kontak persont;

2) Pengisian form aduan, disertakan id pelapor;

3) Mencatat kronologis kejadian dan bukti screanshort;

4) Mengidentifikasi dan deteksi masalah dan kejahatan siber;

5) Mengirim dokumen ke Polres Cianjur untuk Proses Forensik dan proses pidana hukum;

6) Melakukan penangulangan dan pemulihan;

7) Membuat laporan hasil kegiatan.

c) Pembinaan pengamanan informasi siber

1) Membuat materi TIPS anti hoax;

2) Membuat Video pendek tolak tegas hoax;

3) Membuat materi Sosialisasi, Forum Group Diskusi, dan Kampanye Siber;

4) Memfasilitasi media *frame* photo *booth selfie* dan *groupie*;

5) Menyebarkan video tolak tegas hoax di jejaring media sosial;

6) Menyelenggarakan Sosialisasi Tips cerdas dan cermat dalam bermedia sosial;

7) Menyelenggarakan Sosialisasi pengamanan informasi siber pada generasi millenial di sekolah-sekolah dan jajaran pimpinan/staf perangkat daerah;

8) Menyelenggarakan kegiatan-kegiatan sosial, *outbound* dan camping, dan sebaginya yang bersifat merubahan mental, mindset karakter *building*;

9) Membuat laporan hasil kegiatan.

d) Pengawasan pengamanan informasi siber

1) Membuat materi quesioner guna evaluasi tingkat kesadaran, pemahaman akan keamanan informasi siber pada generasi millenial sekolah-sekolah dan jajaran pimpinan/staf perangkat daerah;

2) Menyebarkan quesioner evaluasi kepada generasi millenial di sekolah-sekolah dan jajaran pimpinan/staf perangkat daerah;

3) Melakukan pengawasan pada pokja satgas CIRT;

4) Membuat dokumen pengawasan keamanan informasi siber pada satgas CIRT;

5) Membuat laporan hasil evaluasi dan pengawasan, secara rutin, berkala dan semester.

e) Publikasi dan dokumentasi pengamanan informasi siber

1) Mempublikasikan seluruh kegiatan tim pokja satgas CIRT;

2) Mempublikasikan materi Tips tolak hoax dan video pendek tolak tegas berita hoax di akun resmi Pemerintah Daerah;

3) Mendukung klarifikasi berita hoax;

4) Mengembalikan citra positif Pemerintah Daerah;

5) Membuat laporan hasil publikasi dan dokumentasi.

7. Pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh perangkat daerah.

Pengawasan dan evaluasi dimaksudkan untuk memantau perkembangan, mengidentifikasi hambatan, dan upaya perbaikan dalam penyelenggaraan Persandian untuk pengamanan Informasi.

a. Pengawasan dan evaluasi penyelenggaraan persandian Pemerintah Daerah harus terlapor kepada Pemerintah Provinsi Jawa Barat agar dapat ditindaklanjuti dengan rencana perbaikan sebagai bahan

masukan bagi penyusunan kebijakan, program, dan kegiatan penyelenggaraan Persandian tahun berikutnya.

b. Pengawasan dan evaluasi penyelenggaraan Persandian yang dilaksanakan meliputi:

1) Pengawasan dan evaluasi yang bersifat rutin dan insidentil sebagai berikut:

a) Pemantauan penggunaan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan Persandian lainnya.

b) Melaksanakan kebijakan manajemen risiko penyelenggaraan Persandian di Pemerintah Daerah. Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

(1) Pemerintah Daerah melaksanakan kebijakan manajemen risiko yang ditetapkan oleh Badan Siber dan Sandi Negara;

(2) Dinas sebagai penyelenggara Persandian melaksanakan fungsi koordinasi pelaksanaan kebijakan manajemen risiko penyelenggaraan Persandian;

(3) Dalam hal terdapat potensi insiden dan/atau terjadinya insiden penyelenggaraan Persandian dan keamanan informasi, Pemerintah Daerah membantu pelaksanaan tugas Pemeriksaan Persandian Khusus (audit khusus) atau Investigasi yang dilaksanakan oleh Badan Siber dan Sandi Negara atas terjadinya insiden penyelenggaraan Persandian dan keamanan Informasi.

2) Pengawasan dan evaluasi yang bersifat tahunan sebagai berikut:

a) Pengukuran tingkat pemanfaatan layanan Persandian oleh Pemerintah Daerah.

Dalam melaksanakan pengukuran tingkat pemanfaatan layanan Persandian perlu memperhatikan hal-hal sebagai berikut:

(1) Jumlah Perangkat Daerah yang memanfaatkan analisis kebutuhan penyelenggaraan persandian untuk pengamanan Informasi;

(2) Jumlah Perangkat Daerah yang melaksanakan pengelolaan dan perlindungan Informasi;

(3) Jumlah Perangkat Daerah yang memanfaatkan layanan penyelenggaraan operasional dukungan Persandian untuk pengamanan Informasi.

b) Penilaian mandiri (*self assessment*) terhadap penyelenggaraan Persandian pada Pemerintah Daerah.

Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

(1) Penilaian mandiri (*self assessment*) merupakan pengukuran penyelenggaraan Persandian mandiri yang dilaksanakan dengan menggunakan Instrumen Pengukuran Penyelenggaraan Persandian yang telah ditetapkan oleh Badan Siber dan Sandi Negara.

(2) Dalam melakukan penilaian mandiri (*self assessment*) diperlukan objektifitas yang tinggi sesuai dengan kondisi penyelenggaraan Persandian di Pemerintah Daerah. Oleh sebab itu diperlukan bukti pendukung yang valid sehingga hasilnya dapat dipertanggungjawabkan.

(3) Penilaian mandiri(*self assessment*) dilakukan oleh SDM yang berkualifikasi sandi, menguasai teknik pemeriksaan

dst

(audit), dan telah mengikuti bimbingan teknis penggunaan Instrumen Pengukuran Penyelenggaraan Persandian yang ditetapkan oleh Badan Siber dan Sandi Negara.

(4) Dalam hal Perangkat Daerah penyelenggara Persandian memiliki keterbatasan SDM sesuai butir 3 di atas, maka harus berkonsultasi dengan Badan Siber dan Sandi Negara untuk ditentukan kebijakan lebih lanjut.

(5) Penilaian mandiri (*self assessment*) akan menghasilkan opini mandiri yang bersifat sementara tentang penyelenggaraan Persandian di Pemerintah Daerah.

(6) Hasil penilaian mandiri (*self assessment*) dilaporkan secara khusus kepada Badan Siber dan Sandi Negara untuk dilakukan validasi melalui *Dekstop Assessment* dan/atau *On Site Assessment*.

c) Pengukuran tingkat kepuasan Perangkat Daerah terhadap layanan Persandian yang dikelola oleh Dinas penyelenggara Persandian.

Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

(1) Penyusunan instrumen pengukuran Perangkat Daerah terhadap layanan Persandian dilaksanakan dengan pendekatan ilmiah dan dilakukan pengujian validitas dan reliabilitasnya. Instrumen pengukuran disusun sesuai dengan objek layanan yang akan diukur kepuasannya.

(2) Pemerintah Daerah dapat berkonsultasi kepada Badan Siber

dan Sandi Negara terkait penggunaan instrumen pengukuran kepuasan Perangkat Daerah terhadap layanan Persandian.

d) Penyusunan Laporan Penyelenggaraan Persandian Tahunan (LP2T) Pemerintah Daerah.

Kegiatan Penyusunan Laporan Penyelenggaraan Persandian Tahunan (LP2T) Pemerintah Daerah ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

(1) LP2T berisi tentang hasil pelaksanaan kebijakan, program, dan kegiatan teknis termasuk hasil kegiatan pengawasan dan evaluasi yang menggambarkan hasil penyelenggaraan urusan pemerintahan di bidang Persandian selama satu tahun.

(2) Mengkoordinasikan penyiapan bahan dan melaksanakan penyusunan LP2T.

(3) LP2T Pemerintah Daerah disampaikan kepada Badan Siber dan Sandi Negara.

8. Koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

Dalam rangka pelaksanaan urusan pemerintahan bidang persandian, unit kerja persandian di Pemerintah Daerah dapat melaksanakan koordinasi dan/atau konsultasi ke Badan Siber dan Sandi Negara, perangkat daerah terkait maupun antar pemerintah daerah lainnya.

9. Sarana dan Prasarana Operasional Persandian

Adapun sarana prasarana yang disediakan dalam menyelenggarakan operasional persandian antara lain sekurang-kurangnya:

1) Mempunyai tempat kegiatan persandian yaitu:
   a. Tempat kegiatan administrasi persandian;
   b. Tempat kegiatan persandian yang juga disebut Kamar Sandi.
2) Mempunyai peralatan sandi yang disediakan atau di rekomendasikan oleh Badan Siber dan Sandi Negara;
3) Jaringan internet dan jaringan komunikasi;
4) Peralatan pendukung lainnya yang diperlukan.

Ditetapkan di Cianjur
pada tanggal

Plt. BUPATI CIANJUR,

ttd.

HERMAN SUHERMAN