



BUPATI BOMBANA
PROVINSI SULAWESI TENGGARA

PERATURAN BUPATI BOMBANA
NOMOR 61 TAHUN 2018
TENTANG

PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN
INFORMASI
DILINGKUNGAN PEMERINTAH KABUPATEN BOMBANA

DENGAN RAHMAT TUHAN YANG MAHA ESA
BUPATI BOMBANA,

- Menimbang :
- a. bahwa Pemerintah Daerah wajib mengelola informasi publik yang dimilikinya dari penggunaan yang tidak semestinya;
 - b. bahwa untuk melindungi informasi publik perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian guna mengelola informasi publik
 - c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b perlu menetapkan Peraturan Bupati Bombana tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Kabupaten Bombana

- Mengingat :
1. Undang - Undang Nomor 29 Tahun 2003 tentang Pembentukan Kabupaten Bombana, Kabupaten Wakatobi dan Kabupaten Kolaka Utara di Provinsi Sulawesi Tenggara (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 144, Tambahan Lembaran Negara Republik Indonesia Nomor 4339);
 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 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234);
4. 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);
5. Undang-Undang Nomor 30 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
6. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomo 99. Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
7. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara republik Indonesia Nomor 5887);
8. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 6041;

9. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara;
10. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036);
11. Peraturan Daerah Kabupaten Bombana Nomor 3 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Bombana (Lembaran Daerah Kabupaten Bombana Tahun 2016 Nomor 3);
12. Peraturan Daerah Kabupaten Bombana Nomor 2 tahun 2018 tentang Rencana Pembangunan Jangka Menengah Daerah.

MEMUTUSKAN

Menetapkan : PERATURAN BUPATI BOMBANA TENTANG PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN BOMBANA

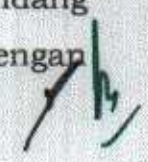
BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati Bombana ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Bombana
2. Pemerintah Daerah adalah Penyelenggaraan Urusan Pemerintahan Oleh Pemerintah Daerah dan Dewan Perwakilan Perwakilan Rakyat Daerah menurut asas otonomi dan tugas pembantuan dengan prinsip Otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
3. Pemerintah Daerah adalah Kepala Daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan Pemerintahan yang menjadi kewenangan Daerah Otonomi

4. Bupati adalah Bupati Bombana
 5. Perangkat Daerah adalah unsur pembantu Bupati dan DPRD dalam penyelenggaraan unsur pemerintahan yang menjadi kewenangan Daerah.
 6. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Bombana.
 7. Urusan Pemerintahan adalah kekuasaan pemerintahan yang menjadi kewenangan Presiden yang pelaksanaannya dilakukan oleh kementerian negara dan penyelenggara Pemerintah Daerah untuk melindungi, melayani, memberdayakan dan mensejahterakan masyarakat.
 8. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni, dan ilmu krypto beserta ilmu pendukung lainnya secara sistematis, metodologis, dan konsisten serta terkait pada etika profesi sandi.
 9. Jaring Komunikasi Sandi selanjutnya disebut JKS adalah keterhubungan antar pengguna persandian melalui jalin telekomunikasi.
 10. 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
 11. Informasi Publik adalah Informasi yang dihasilkan disimpan, dikelola, dikirim dan / atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggaraan dan penyelenggaraan Negara dan / atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik.
- 

12. Informasi bersklasifikasi adalah informasi publik lainnya yang dikecualikan menurut peraturan perundang-undangan yang berlaku.

Pasal 2

Pedoman penyelenggaraan Persandian untuk pengamanan informasi dilingkungan Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi.


Pasal 3

Penyelenggaraan Persandian untuk Pengamanan Informasi dilingkungan Pemerintah Daerah bertujuan :

- a. melaksanakan tata penyelenggaraan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah;
- b. meningkatkan komitmen Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi dilingkungan Pemerintah Daerah;
- c. meningkatkan efektifitas pelaksanaan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan informasi dilingkungan Pemerintah Daerah dan
- d. meningkatkan kinerja kelembagaan yang menangani urusan pemerintahan bidang persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah.

Pasal 4

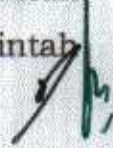
- (1) Penyelenggaraan Persandian untuk Pengamanan Informasi dilingkungan Pemerintah Daerah meliputi :



- a. penyediaan analisis kebutuhan penyelenggaraan persandian untuk pengamanan informasi;
 - b. penyediaan kebijakan penyelenggaraan persandian untuk pengamanan informasi;
 - c. pengelolaan dan perlindungan informasi dan;
 - d. pengelolaan sumber daya persandian meliputi sumber daya manusia, materiil sandi dan jaringan komunikasi sandi serta anggaran;
 - e. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi;
 - f. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian diseluruh Perangkat Daerah dan
 - g. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi;
- (2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) mencakup pengamanan fisik, pengamanan logik dan perlindungan secara administrasi
 - (3) Tata Cara Penyelenggaraan Persandian untuk pengamanan informasi di Kabupaten Bombana sebagaimana tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dalam Peraturan Bupati ini.

Pasl 5

- (1) Penyelenggaraan Persandian merupakan penjabaran atas pelaksanaan kebijakan, program dan kegiatan di bidang persandian
- (2) Tahapan penyelenggaraan persandian untuk pengamanan informasi dilingkungan Pemerintah Daerah adalah sebagai berikut :



- a. Perencanaan;
 - b. Pelaksanaan;
 - c. Pemantauan dan evaluasi
 - d. Pelaporan;
 - e. Pembiayaan dan
 - f. Pembinaan dan Pengawasan.
- (3) Penyelenggaraan persandian untuk pengamanan informasi dilingkungan Pemerintah Daerah adalah Bupati dibantu oleh Dinas Komunikasi, Informatika dan Statistik,

BAB II

PERENCANAAN

Pasal 6

- (1) Dalam rangka melakukan perencanaan penyelenggaraan Urusan Pemerintah Bidang Persandian, Dinas Komunikasi, Informatika dan Statistik menyusun perencanaan penyelenggaraann Urusan pemerintah bidang persandian sesuai dengan kewenangannya.
- (2) Perencanaan penyelenggaraan Urusan Pemerintahan bidang persandian sebagaimana dimaksud pada ayat (1) diintegrasikan kedalam pertencanaan pembangunan daerah.
- (3) Perencanaan pembangunan daerah sebagaimana dimaksud pada ayat dua (2) merupakan bagian integral dari sistem perencanaan pembangunan nasional dan dituangkan dalam dokumen perencanaan pembangunan daerah.
- (4) Dokumen Perencanaan Pembangunan Daerah sebagaimana dimaksud pada ayat (3) berupa Rencana embangunan Jangka Panjang Daerah, Rencana Pembangunan Jangka Menengah Daerah dan Rencana Kerja Pemerintah Daerah.

Pasal 7

- (1) Dalam rangka menjabarkan Rencana Pembangunan Jangka Menengah Daerah sebagaimana dimaksud pada pasal 6 ayat (4) Dinas Komunikasi Informatika dan Statistik, menyusun Rencana Strategis yang memuat tujuan, sasaran, program, dan kegiatan penyelenggaraan urusan pemerintah bidang persandian untuk penanganan informasi di lingkungan Pemerintah Daerah.
- (2) Dalam rangka menjabarkan Rencana Kerja Pemerintah Daerah sebagaimana dimaksud dalam Pasal 6 ayat (4) Dinas Komunikasi Informatika dan Statistik, menyusun Rencana kerja yang memuat program kegiatan, lokasi dan kelompok sasaran berdasarkan layanan urusan pemerintah bidang persandian, disertai indikator kinerja program dan kegiatan, serta penganggaran penyelenggaraan Urusan pemerintahan bidang persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah.

BAB III

PELAKSANAAN

Pasal 8

- (1) Bupati memimpin dan bertanggung jawab atas penyelenggaraan urusan pemerintahan bidang persandian yang menjadi kewenangan daerah.
- (2) Bupati dalam memimpin penyelenggaraan persandian untuk pengamanan informasi sebagaimana dimaksud pada ayat (1), melakukan :
 - a. mengkoordinasikan kegiatan antar perangkat daerah dilingkungan Pemerintah Daerah;
 - b. kerjasama dengan Provinsi dan Kabupaten/ Kota dalam wilayah provinsi Sulawesi Tenggara sesuai dengan ketentuan dan Peraturan Perundang-undangan.

Pasal 9

Tanggung jawab Bupati dalam penyelenggaraan persandian untuk mengamankan informasi sebagaimana dimaksud dalam pasal 8, dilaksanakan oleh Dinas komunikasi, Informatika dan Statistik,

BAB IV

PEMANTAUAN DAN EVALUASI

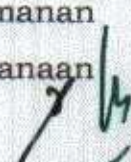
Pasal 10

- (1) Pemantauan dan evaluasi penyelenggaraan urusan pemerintahan bidang persandian dilaksanakan oleh Dinas komunikasi Informatika dan Statistik.
- (2) Pemantauan sebagaimana dimaksud pada ayat (1) bertujuan untuk mengetahui perkembangan dan hambatan dalam penyelenggaraan persandian untuk pengamanan informasi yang dilakukan secara berkala guna dicarikan solusi dan tindak lanjut agar pelaksanaannya dapat berjalan sesuai dengan tujuan.
- (3) Evaluasi penyelenggaraan persandian untuk pengamanan informasi dilakukan setiap berakhirnya tahun anggaran berdasarkan hasil pemantuan.
- (4) Hasil evaluasi digunakan sebagai bahan masukan bagi penyelenggara persandian tahun berikutnya,

BAB V

PELAPORAN

Pasal 11

- (1) Pelaporan bertujuan untuk melihat capaian penyelenggaraan persandian untuk pengamanan informasi di daerah sesuai dengan perencanaan yang sudah ditetapkan;
- 

- (2) Bupati menyampaikan laporan hasil evaluasi penyelenggaraan persandian untuk pengamanan informasi di daerah kepada Menteri Dalam Negeri melalui Gubernur sebagai wakil Pemerintah Pusat dan tembusan kepada Kepala Lembaga Sandi Negara .
- (3) Pelaporan hasil evaluasi sebagaimana dimaksud pada ayat (1) dan (2) memuat capaian kinerja urusan pemerintah bidang persandian.
- (4) Bentuk pelaporan sebagaimana dimaksud pada ayat (1) dan (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.
- (5) Dalam hal-hal tertentu dianggap penting terkait dengna persandian, Bupati dapat menyampaikan laporan langsung kepada Kepala Lembaga Sandi Negara

BAB VI

PEMBIAYAAN

Pasal 12

Pembiayaan penyelenggaraan persandian untuk pengamanan Informasi di Pemerintah Kabupaten Bombana bersumber dari anggaran pendapatan dan belanja daerah Pemerintah Kabupaten Bombana dan sumber lain yang sah sesuai dengan ketentuan peraturan perundang-undangan

BAB VII

PEMBINAAN DAN PENGAWASAN

Pasal 13

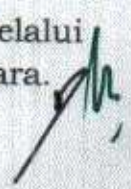
- (1) Pembinaan umum meliputi pembagian urusan Pemerintahan, kelembagaan daerah, kepegawaian pada perangkat daerah, keuangan daerah, pembangunan daerah, pelayanan publik di daerah, kerjasama daerah, kebijakan daerah, Bupati dan Dewan Perwakilan Rakyat Daerah,

LAMPIRAN
PERATURAN BUPATI BOMBANA
NOMOR 61 TAHUN 2018
TENTANG PEDOMAN PENYELENGGARAAN
PERSANDIAN UNTUK
PENGAMANAN INFORMASI DI
LINGKUNGAN PEMERINTAHAN
KABUPATEN BOMBANA

TATA CARA PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN
INFORMASI DI LINGKUNGAN PEMERINTAHAN KABUPATEN BOMBANA

- A. Penyediaan analisis kebutuhan persandian untuk pengamanan informasi analisis kebutuhan penyelenggaraan persandian merupakan proses yang berkelanjutan untuk mengidentifikasi kebutuhan penyelenggaraan persandian guna menjamin keamanan informasi di Pemerintah Daerah. Kegiatan analisis kebutuhan penyelenggaraan persandian, meliputi:
1. Identifikasi pola hubungan komunikasi yang di gunakan oleh Pemerintah Kabupaten Bombana di antaranya meliputi:
 - a. Mengidentifikasi pola hubungan komunikasi pejabat/pimpinan di Pemerintah Kabupaten Bombana yang sedang dilaksanakan;
 - b. Mengidentifikasi alur informasi yang di komunikasikan antar Perangkat Daerah;
 - c. Mengidentifikasi sarana dan prasarana teknologi informasi dan komunikasi yang di gunakan oleh para pejabat/pimpinan di Pemerintah Kabupaten Bombana
 2. Analisis pola hubungan komunikasi sandi yang di perlukan berdasarkan hasil identifikasi pola hubungan komunikasi yang sudah ada (poin a di atas), meliputi:
 - a. Mengidentifikasi pengelola layanan penyelenggaraan persandian identifikasi pengelola yaitu kegiatan untuk mengidentifikasi personil dan kompetensi yang dibutuhkan dalam menyelenggarakan kegiatan persandian.
 - b. Mengidentifikasi sarana dan prasarana
 - 1) Materiil sandi dan jaring Komunikasi sandi
 - a) Materiil sandi
Identifikasi materiil sandi meliputi identifikasi terhadap kebutuhan peralatan sandi dan kunci sistem sandi yang didasarkan pada kondisi infrastruktur, jenis komunikasi, dan hierarki pada komunikasinya.
 - b) Jaringan Komunikasi Sandi (JKS)
Identifikasi JKS meliputi identifikasi terhadap:
 - 1) Dinas Komunikasi, Informatika, dan Statistik yang akan terhubung dalam JKS termasuk didalamnya bidang persandian yang akan mengoperasikan peralatan sandi.

- 2) Pejabat Pemerintah Daerah yang akan terhubung dalam JKS termasuk didalamnya penentuan hierarki komunikasi.
- 3) Infrastruktur komunikasi yang ada di wilayah pemerintah daerah dan di lingkungan kantor Dinas komunikasi dan Informatika.
- 2) Alat Pendukung Utama (APU) Persandian
Identifikasi APU persandian meliputi identifikasi kebutuhan terhadap perangkat yang mendukung penyelenggaraan persandian.
- 3) Tempat Kegiatan Sandi
Identifikasi Tempat Kegiatan Sandi (TKS) meliputi identifikasi kebutuhan pengamanan terhadap tempat yang digunakan untuk operasional persandian sesuai dengan jenis komunikasinya.
- 4) Sarana Penunjang.
Identifikasi sarana penunjang meliputi identifikasi kebutuhan terhadap peralatan yang mendukung dalam kegiatan penyelenggaraan persandian, meliputi alat tulis kantor dan sarana pengolahan data.
- 5) Identifikasi Pembiayaan
Identifikasi pembiayaan meliputi identifikasi anggaran yang di butuhkan oleh penyelenggaraan persandian di Pemerintah Daerah dalam periode waktu satu tahun anggaran.
3. Mengoordinasikan hasil identifikasi dan analisis pola hubungan komunikasi sandi tersebut secara berjenjang mulai dari kabupaten/kota ke provinsi sampai ke Lembaga Sandi Negara untuk melihat dan menjamin keterhubungan (interkoneksi) secara vertikal.
4. Menetapkan hasil identifikasi dan analisis pola hubungan komunikasi sandi melalui Keputusan Bupati, 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 di berikan.
- B. Penyediaan kebijakan penyelenggaraan persandian untuk pengamanan informasi kebijakan penyelenggaraan persandian di maksud adalah aturan-aturan yang digunakan sebagian besar dan acuan dalam penyelenggaraan persandian untuk pengamanan informasi di Pemerintah Daerah.
1. Kebijakan penyelenggaraan persandian untuk pengamanan informasi di Pemerintah Daerah meliputi:
 - a) Kebijakan tata kelola persandian, tentang keseluruhan aspek tata kelola penyelenggaraan persandian, yang meliputi kewenangan, kedudukan, fungsi dan layanan unit kerja persandian di daerah antara lain:
 - 1) Pengelolaan dan perlindungan informasi di Pemerintah Daerah;

- 2) Tata cara klasifikasi tingkat kerahasiaan informasi;
 - 3) Pengendalian akses terhadap informasi;
 - 4) Pengamanan jaringan komunikasi sandi;
 - 5) Dst.
- b) Kebijakan operasional pengamanan persandian, diantaranya:
- 1) Pengamanan jaringan komunikasi sandi;
 - 2) Pengamanan gangguan layanan persandian;
 - 3) Pengelolaan password bagi pengguna layanan persandian;
 - 4) Pengamanan perangkat dan fasilitas pengolahan data dan informasi;
 - 5) Tindakan penanggulangan pengamanan informasi pasca bencana;
 - 6) Pelaksanaan kontra penginderaan dan jamming;
 - 7) Dst.
- c) Pengelolaan sumber daya persandian, yang merupakan kebijakan pengaturan pengelolaan sumber daya manusia (SDM), sarana dan prasarana persandian, diantaranya:
- 1) Pengendalian akses terhadap materiil sandi dan jaring komunikasi sandi
 - 2) Pemeliharaan dan perbaikan umum materiil sandi;
 - 3) Penyediaan materiil sandi dan jaringan komunikasi sandi;
 - 4) Penggunaan materiil sandi;
 - 5) Pemenuhan komputer kopetensi SDM.
- d) Pengawasan dan evaluasi penyelenggaraan persandian merupakan kebijakan pengawasan dan evaluasi pemanfaatan layanan persandian di organisasi perangkat daerah sebagai bagian pengukuran kinerja unit kerja persandian di Pemerintah Daerah.
2. Kebijakan penyelenggaraan persandian pada poin a di atas dapat berupa peraturan daerah, peraturan walikota, peraturan kepala dinas, pedoman, petunjuk pelaksanaan, petunjuk teknis, atau standar operasional dan prosedur (SOP);
3. Penyediaan kebijakan penyelenggaraan persandian untuk pengamanan informasi di pemerintah daerah memperhatikan hal-hal sebagai berikut;
- a) Perumusan kebijakan penyelenggaraan untuk pengamanan informasi milik pemerintah daerah mengacu pada Peraturan Perundang-Undangan yang berlaku;
 - b) Perumusan kebijakan penyelenggaraan persandian di pemerintah daerah harus dapat mendorong terciptanya budaya pengamanan informasi.
 - c) Perumusan kebijakan penyelenggaraan persandian di pemerintah daerah dengan memperhatikan hasil analisis kebutuhan kebijakan dan inovasi Pemerintah Daerah.
 - d) Dalam melakukan kebijakan, dapat dilakukan melalui koordinasi maupun konsultasi kepada Lembaga Sandi Negara.
- 

C. Pengelolaan dan perlindungan informasi

Pengelolaan dan perlindungan informasi di Pemerintah Daerah meliputi hal hal sebagai berikut:

1. Fasilitas penentuan tingkat kerahasiaan informasi berklasifikasi di Dinas Komunikasi dan Informatika dan Statistik Lingkup Pemerintah Kabupaten Bombana

Pelaksanaan fasilitasi mengacu pada ketentuan yang diatur dalam Peraturan Kepala Lembaga Sandi Negara.

2. Pengelolaan dan perlindungan informasi publik yang di kecualikan/informasi berklasifikasi di Pemerintah Daerah.

a) Pengelolaan informasi publik yang di kecualikan/informasi berklasifikasi meliputi pembuatan, pemberian label, pengiriman, dan penyimpanan.

- 1) Pembuatan informasi publik yang dikecualikan/informasi berklasifikasi memperhatikan hal-hal berikut:

- 1) Pengelolaan informasi publik yang di kecualikan/informasi berklasifikasi di lakukan 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 logic (logical security).

- 2) Perangkat atau peralatan yang digunakan untuk membuat dan/atau mengkomunikasikan informasi publik yang dikecualikan/informasi berklasifikasi harus milik dinas dan hanya dimanfaatkan untuk kepentingan dinas. Contoh: komputer/laptop/alat komunikasi milik dinas tidak untuk kepentingan pribadi.

- 3) Konsep informasi publik yang dikecualikan/informasi berklasifikasi tidak boleh disimpan dan harus di hancurkan secara fisik mupun logic (logical security).

Contoh: apabila dokumen/ surat resmi sudah selesai di buat maka konsep surat/dokumen tersebut dihancurkan untuk hardcopy bisa di hancurkan dengan paper shredder, untuk softcopy menggunakan software file shredder yang direkomendasikan oleh Lembaga Sandi Negara;

- 4) Dokumen elektronik yang berisi informasi publik yang di kecualikan/informasikan berklasifikasi yang sudah di sahkan di simpan dalam bentuk yang tidak dapat di ubah/dimodifikasi (read only). Contoh: dokumen elektronik di ubah menjadi berbentuk file *pdf* dan diberikan *watermark*.

- 5) Penggadaan dan/atau perubahan informasi publik yang akan dikecualikan/informasi berklasifikasi harus sesuai dengan ijin dari pemilik informasi atau pengelola informasi.

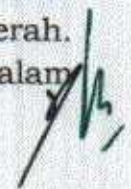
- 2) Pemberian label klasifikasi pada informasi publik yang dikecualikan/informasi berklasifikasi harus sesuai dengan tingkat kerahasiaan informasinya, serta bergantung pada bentuk dan media penyimpanannya.

- 3) Pengiriman informasi publik yang dikecualikan/informasi berklasifikasi
 - 1) Pengiriman dokumen elektronik yang berisi informasi publik yang dikecualikan/informasi berklasifikasi menggunakan teknik kriptografi dan melalui saluran komunikasi yang aman.
 - 2) Pengiriman dokumen cetak yang berisi informasi yang dikecualikan/informasi berklasifikasi dilakukan dengan memasukkannya ke dalam dua amplop
 - (a) Amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (kilat, sangat segera, segera, dan biasa).
 - (b) Selanjutnya amplop pertama dimasukan kedalam amplop kedua dengan tanda-tanda yang sama kecuali cap klasifikasi.
- 4) Penyimpanan informasi publik yang dikecualikan/informasi berklasifikasi berupa dokumen elektronik dan dokumen cetak memperhatikan ketentuan yang telah di atur dalam Peraturan Kepala Lembaga Sandi Negara.
- b) Perlindungan informasi publik yang dikecualikan/diinformasi berklasifikasi meliputi:
 - 1) Perlindungan fisik dilakukan melalui kendali akses ruang, pemasangan teralis dan kunci ganda, pemasangan CCTV.
 - 2) Perlindungan administrasi.

Pelaksanaan perlindungan administrasi di lakukan dengan pedoman kebijakan, standar, dan prosedur oprasional pengaman informasi publik yang dikecualikan/informasi berklasifikasi.
 - 3) Perlindungan logic (*logical security*)
 - (1) Perlindungan logic (*logical security*) menggunakan teknik kriptografi dan steganografi untuk memenuhi aspek;kerahasiaan, keutuhan, otentikasi, dan nir penyakalan.

Contoh:

 - a. Penggunaan aplikasi enkripsi pada master naskah soal ujian CPNS Nasional untuk menjamin kerahasiaan naskah soal tersebut.
 - b. Penggunaan sertifikat digital pada dokumen elektronik yang muat informasi publik yang dikecualikan/informasi berklasifikasi untuk menjamin kerahasiaan, keutuhan, otentikasi, dan nir penyangkalan.
 - (2) Perlindungan lojik (*logic security*) yang menggunakanteknikkriptografidansteganografi harus memenuhi standar dan direkomendasikan oleh lembaga sandi negara.

- (3) Rincian pengelolaan dan perlindungan informasi berklasifikasi di pemerintah daerah mengacu pada ketentuan yang diatur dalam Peraturan Kepala Lembaga Sandi Negara.
3. Pengelolaan dan perlindungan informasi terbuka di Pemerintah Daerah.
- a) Pengelolaan dan perlindungan informasi terbuka meliputi:
- 1) Fasilitas pengiriman informasi terbuka melalui jaringan yang aman;
Contoh: pengiriman dan penerimaan dokumen elektronik melalui *virtual private network* (VPN).
 - 2) Fasilitas perlindungan transaksi elektronik melalui implementasi sertifikat elektronik.
 - 3) Fasilitas implementasi sertifikat elektronik bertujuan untuk menjamin keutuhan, otentikasi dan nir penyangkalan dokumen elektronik tersebut. Tahap fasilitas implementasi sertifikat elektronik tersebut dilakukan melalui:
 - (1) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaharuan dan pencabutan sertifikat elektronik
 - (a) Menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi, rekomendasi dari instansi.
 - (b) Menyetujui/menolak permintaan pendaftaran sertifikat elektronik.
 - (c) Menindak lanjuti permintaan sertifikat elektronik kepada Balai sertifikat elektronik Lembaga Sandi Negara;
 - (d) Menyampaikan sertifikat elektronik kepada pemohon
 - (e) Melakukan pengarsipan berkas pendaftaran sertifikat elektronik (*hardcopy & softcopy*)
 - (2) Fasilitas kegiatan sosialisasi dan bimbingan teknik terkait sertifikat elektronik.
Pemerintah daerah dapat melakukan kegiatan fasilitas implementasi sertifikat elektronik disesuaikan dengan kemampuannya.
- b) Pengelolaan dan perlindungan terhadap informasi terbuka dipemerintah daerah mengacu pada ketentuan yang ada.
4. Penyelenggaraan jaringan komunikasi sandi (JKS) untuk pengamanan informasi berklasifikasi di Pemerintah Daerah. Penyelenggaraan JKS mengacu pada ketentuan yang diatur dalam peraturan kepala lembaga sandi negara.
- 

D. Pengelolaan Sumber Daya Persandian

Pengelolaan Sumber Daya Persandian terdiri atas:

1. Pengeloaan Kebutuhan Sumber Daya Manusia (SDM) pengelolaan SDM meliputi:

a) Perencanaan kebutuhan SDM

Perencanaan kebutuhan SDM yang bertugas di bidang persandian di susun dengan memperhatikan jumlah dan kompetensi yang dibutuhkan. Dalam kegiatan perencanaan ini, unit yang menangani persandian di Pemerintah Daerah dapat menyusun analisis beban kerja (ABK) dan formasi jabatan fungsional sandiman serta mengajukan usulan kebutuhan tersebut kepada bagian kepegawaian daerah.

b) Pengembangan kompetensi SDM

Pengembangan kompetensi SDM 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 di butuhkan.

c) Pengajuan tunjangan pengamanan persandian (TPP) sebagai bentuk pemberian kompensasi atas tanggung jawab dalam melaksanakan tugas di bidang penyelenggaraan persandian untuk pengamanan persandian.

d) Pengajuan tunjangan jabatan fungsional sandiman bagi pegawai yang di angkat dalam jabatan fungsional sandiman.

e) Pengajuan usulan pemberi tanda penghargaan bidang persandian untuk SDM yang bertugas di bidang persandian yang telah memenuhi syarat kepada Kepala Lembaga Sandi Negara.

2. Pengeloaan sarana dan prasarana meliputi:

a) Pengelolaan materiil sandi dan JKS

1) Pemenuhan terhadap kebutuhan materiil sandi yang akan digunakan dalam penyelenggaraan JKS eksternal oleh pemerintah daerah difasilitasi oleh Lembaga Sandi Negara dengan mengajukan permohonan kepada Lembaga Sandi Negara sesuai hasil analisis.

2) Pemenuhan terhadap kebutuhan materiil sandi yang akan digunakan dalam penyelenggaraan JKS internal di pemerintah daerah meliputi:

(1) Pemerintah Daerah mengadakan peralatan sandi secara mandiri dengan syarat bahwa peralatan sandi tersebut telah di sertifikasi oleh lembaga sandi negara dan sesuai dengan kewenangan pola hubungan komunikasi sandi yang telah di tetapkan. Dalam hal Pemerintah Daerah tidak dapat mengadakan peralatan sandi secara mandiri, maka pemerintah daerah dapat mengajukan permohonan peralatan sandi kepada Lembaga Sandi Negara.

- (2) Pemenuhan kebutuhan kunci sistem sandi sesuai dengan pola hubungan komunikasi sandi yang telah ditetapkan dengan mengkonsultasikan dan mengajukan permohonan ke Lembaga Sandi Negara.
- 3) Penyimpanan materiil sandi (peralatan sandi dan kunci sistem sandi) dengan memperhatikan syarat-syarat keamanan antara lain:
 - (1) Lokasi penyimpanan materiil sandi harus dilengkapi kendali akses untuk mencegah resiko kehilangan, kerusakan, dan manipulasi.
 - (2) Materiil sandi dilarang digunakan, dipinjam, atau bawa keluar ruangan kerja atau kantor tanpa ijin dari penanggung jawab pengelola materiil sandi.
 - (3) Mekanisme penyimpanan materiil sandi berdasarkan ketentuan yang berlaku
- 4) Pendistribusian materiil sandi (peralatan sandi dan kunci sistem sandi) ke Dinas Komunikasi Informatika dan Statistik atau Pejabat Pemerintah Daerah dengan memperhatikan ketentuan sebagai berikut:
 - (1) Dilengkapi dengan berita acara penyerahan;
 - (2) Terjamin keamanan dan keutuhannya sehingga terhindar dari kehilangan dan kerusakan;
 - (3) Peralatan sandi dalam keadaan netral atau non aktif (tidak terisi kunci sistem sandi);
- 5) Penggunaan materiil sandi (peralatan sandi dan kunci sistem sandi) di dalam operasional persandian dengan memperhatikan hal sebagai berikut:
 - (1) Memastikan bahwa kunci sistem sandi yang aktif digunakan;
 - (2) Setting parameter peralatan sandi
 - (3) Memastikan peralatan sandi yang terpasang di dinas komunikasi dan informatika atau di pejabat Pemerintah Daerah dalam kondisi siap di operasionalkan.
- 6) Pemeliharaan peralatan sandi dan APU dilaksanakan dengan melakukan perawatan dan perbaikan (bila ada kerusakan) sesuai dengan kewenangan yang dimiliki oleh pemerintah daerah.

Pelaksanaan pemeliharaan dan perbaikan peralatan sandi mengacu pada peraturan Kepala Lembaga Sandi Negara tentang pemeliharaan dan perbaikan peralatan sandi dan APU persandian.
- 7) Penghapusan materiil sandi dilakukan dengan tindakan penghapusan materiil sandi dari daftar barang atau pelaksanaan penghapusan materiil sandi (peralatan sandi dan kunci sistem sandi) mengacu pada peraturan Kepala Lembaga Sandi Negara dan peraturan deputy pengaman persandian Lembaga Sandi Negara.

b) Pengelolaan Alat Pendukung Utama (APU) persandian pengelolaan terhadap APU persandian meliputi:

1) Pemenuhan

Pemerintah Daerah mengadakan APU persandian secara mandiri dengan wajib meminta rekomendasi dari lembaga sandi negara. dalam hal pemerintah daerah tidak dapat mengadakan APU persandian secara mandiri, maka pemerintah daerah dapat mengajukan permohonan pemanfaatan APU persandian kepada Lembaga Sandi Negara, dengan mempertimbangkan:

- (1) prioritas kebutuhan pemerintah daerah;
- (2) ketersediaan sumber daya manusia yang memiliki kemampuan dalam pemanfaatan APU persandian pada pemerintah daerah; dan
- (3) kemampuan lembaga sandi negara dalam memenuhi kebutuhan APU persandian untuk Pemerintah Daerah.

2) Penyimpanan

penyimpanan APU persandian dengan memperhatikan syarat-syarat keamanan antara lain:

- (1) lokasi penyimpanan APU persandian harus di lengkapi kendali akses untuk mencegah resiko kehilangan, kerusakan, dan manupulasi.
- (2) APU persandian dilarang digunakan, dipinjam, atau dibawa keluar ruang kerja atau kantor tanpa ijin dari penanggung jawab pengelola materiil sandi.

3) Pemeliharaan

Pemeliharaan APU persandian dilaksanakan dengan melakukan perawatan dan perbaikan (bila ada kerusakan) sesuai dengan kewenangan yang dimiliki oleh Pemerintah Daerah. Ketentuan lebih lanjut mengenai pemeliharaan dan perbaikan APU persandian mengacu ke peraturan Kepala Lembaga Sandi Negara tentang pemeliharaan dan perbaikan Peralatan Sandi dan Alat Pendukung Utama Persandian;

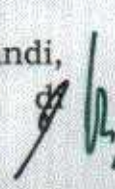
E. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi

kegiatan operasional dukungan tersebut merupakan kegiatan operasional yang tidak terkait dengan kriptografi namun mendukung terciptanya keamanan informasi pemerintah daerah, meliputi hal-hal berikut ini:

1. Jamming

- a) Kegiatan jamming dilakukan untuk mencegah terungkapnya informasi berklasifikasi pada pihak yang tidak berhak selama berlangsungnya rapat terbatas pimpinan pemerintah daerah. contohnya: pengacakan sinyal seluler karena di khawatirkan ada peserta rapat yang melakukan penyadapan.

- b) Selain itu kegiatan jamming juga dapat dilakukan berdasarkan hasil identifikasi kegiatan-kegiatan yang berpotensi untuk timbulnya ancaman dengan gangguan terhadap penyalahgunaan sinyal. contohnya: pengacakan sinyal seluler selama aksi demonstrasi.
 - c) Pelaksanaan kegiatan jamming untuk pengamanan informasi di Pemerintah Daerah mengacu pada ketentuan yang berlaku.
2. Kontra Penginderaan
- a) Kontra Pengindraan bertujuan untuk mencegah adanya pengawasan dari pihak yang tidak berhak terhadap informasi berklasifikasi yang disampaikan oleh pimpinan Pemerintah Daerah.
 - b) Kontra Penginderaan dilakukan terhadap ruangan-ruangan yang digunakan oleh pimpinan pemerintah daerah untuk penyampaian informasi berklasifikasi, contohnya: ruang kerja, ruang rapat, rumah jabatan.
 - c) Kegiatan Kontra Penginderaan dilakukan melalui pemeriksaan fisik ruangan dengan memperhatikan barang-barang di dalam ruangan yang berpotensi menjadi peralatan *surveillance*. contohnya: lukisan, meja kerja, engsel pintu, saklar listrik.
 - d) Temuan hasil kontra penginderaan berupa barang-barang yang di duga menjadi peralatan *surveillance* yang dapat di konsultasikan ke Lembaga Sandi Negara.
 - e) Pelaksanaan kegiatan kontra penginderaan di lakukan secara berkala.
 - f) Pelaksanaan kegiatan kontra penginderaan untuk pengamanan informasi di pemerintah daerah mengacu pada ketentuan yang berlaku.
3. Pelaksanaan kegiatan *assessment* keamanan sistem informasi
- a) Kegiatan *assessment* keamanan sistem informasi untuk mengukur tingkat kerawanan dan keamanan informasi di Pemerintah Daerah.
 - b) kegiatan *assessment* keamanan sistem informasi di lakukan dengan melakukan pemeriksaan terhadap ada atau tidaknya cela kerawanan pada sistem informasi di Pemerintah Daerah.
 - c) Pemerintah Daerah di lakukan kegiatan *assessment* keamanan sistem informasi secara mandiri. dalam hal Pemerintahan Daerah tidak dapat di lakukan kegiatan *assessment* keamanan sistem informasi secara mandiri, maka Pemerintah Daerah dapat mengajukan permohonan *assessment* keamanan sistem informasi kepada Lembaga Sandi Negara.
 - d) Pelaksanaan kegiatan *assessment* keamanan sistem informasi di pemerintah daerah mengacu pada ketentuan yang berlaku.
4. penyelenggaraan kegiatan *security operation center* (SOC)
- a) SOC adalah kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil proses pelaksanaan dan ketersediaan teknologi.

- b) SOC merupakan suatu infrastruktur terpusat dimana di dalamnya terdapat SDM yang bertugas di bidang persandian yang melakukan fungsi SOC seperti mengawasi, melindungi dan menganalisis masalah keamanan informasi untuk melakukan penanggulangan, dengan menggunakan teknologi pengolahan data.
 - c) Penyelenggaraan SOC di pemerintah daerah bertujuan untuk mencegah dan menanggulangi ancaman keamanan informasi dengan berkolaborasi bersama *network operation center* (NOC) pemerintah daerah yang telah terbangun infrastrukturnya.
 - d) Penyelenggaraan SOC di pemerintah daerah dilakukan secara mandiri namun tetap bekerjasama dengan Lembaga Sandi Negara sebagai instansi pembina dimana infrastruktur SOC pada pemerintah daerah dapat terpusat dan terhubung dengan lembaga sandi negara, sehingga kegiatan akan berlangsung responsif.
 - e) Penyelenggaraan SOC di pemerintah daerah mengacu pada ketentuan yang berlaku.
5. Pelaksanaan kegiatan pengamanan informasi lainnya untuk mendukung pengamanan informasi di Pemerintah Daerah.
- F. Pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di dinas komunikasi dan informatika pengawasan dan evaluasi dimaksudkan untuk memantau perkembangan, mengidentifikasi hambatan, dan upaya perbaikan dalam penyelenggaraan persandian untuk pengamanan informasi di Pemerintah Daerah.
- 1. Pengawasan dan evaluasi dilaksanakan dengan memperhatikan ketentuan umum sebagai berikut:
 - a) Pengawasan dan evaluasi dilaksanakan dengan menerapkan fungsi pencegahan, penindakan, serta penanggulangan dan pemulihan sesuai dengan peraturan perundang-undangan.
 - b) Pengawasan dan evaluasi dalam penyelenggaraan persandian di Pemerintah Daerah dilaksanakan oleh perangkat daerah penyelenggaraan persandian untuk pengamanan guna meningkatkan kinerja persandian.
 - c) Pengawasan dan evaluasi harus di tindak lanjuti dengan rencana perbaikan sebagai bahan masukan bagi penyusunan kebijakan, program, dan kegiatan penyelenggaraan persandian tahun berikutnya.
 - 2. Pengawasan dan evaluasi penyelenggaraan persandian yang dilaksanakan oleh pemerintah daerah meliputi:
 - a) Pengawasan dan evaluasi yang bersifat rutin dan insidental sebagai berikut:
 - 1) Pemantauan penggunaan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan persandian lainnya di pemerintah daerah.
- 

1. Pemantauan penggunaan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan persandian lainnya yang dimanfaatkan oleh pengguna (user) atau dinas komunikasi dan informatika.
 2. Dapat dilaksanakan dengan cara melakukan pemantauan langsung di lapangan (on site) dan/atau memanfaatkan teknologi informasi dengan menerapkan sistem pengamanan yang baik dan diaudit secara berkala.
 3. Dilakukan paling sedikit satu kali dalam 3 (tiga) bulan atau sesuai kebutuhan dengan memperhatikan tingkat resiko pemanfaatan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan persandian lainnya.
 4. Hasil kegiatan dapat digunakan sebagai data dukung dalam melakukan evaluasi pemanfaatan layanan persandian oleh dinas komunikasi dan informatika.
- 2) Melaksanakan kebijakan manajemen resiko penyelenggaraan persandian di pemerintah daerah. kegiatan pengawasan dan evaluasi di laksanakan dengan memperhatikan ketentuan sebagai berikut:
- 1) Pemerintah daerah melaksanakan kebijakan manajemen resiko yang di tetapkan Lembaga Sandi Negara.
 - 2) Perangkat Daerah penyelenggaraan persandian melaksanakan fungsi koordinasi pelaksanaan kebijakan manajemen resiko penyelenggaraan persandian.
 - 3) Dalam hal pendapatan 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 lembaga sandi negara atas terjadinya insiden penyelenggaraan persandian dan keamanan informasi.
 - 4) Menyusun laporan pelaksanaan kebijakan manajemen resiko penyelenggaraan persandian.
- b) Pengawasan dan evaluasi yang bersifat tahunan sebagai berikut:
- 1) Pengukuran tingkat pemanfaatan layanan persandian oleh Dinas Komunikasi, Informatika dan Statistik, dalam melaksanakan pengukuran tingkat pemanfaatan layanan persandian oleh Dinas Komunikasi Informatika dan Statistik perlu memperhatikan jumlah perangkat daerah yang melaksanakan pengelolaan dan perlindungan informasi di Pemerintahan Daerah.
 - 2) 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 oleh pemerintah daerah yang dilaksanakan dengan menggunakan instrumen pengukuran penyelenggaraan persandian yang telah ditetapkan oleh Lembaga Sandi Negara.
 - (2) Dalam melakukan penilaian mandiri (*self assessment*) di perlukan objektivitas yang tinggi sesuai dengan kondisi penyelenggaraan persandian di Pemerintah Daerah. oleh sebab itu di perlukan bukti pendukung yang valid sehingga hasilnya dapat di pertanggung jawabkan.
 - (3) Penilaian mandiri (*self assesment*) di lakukan oleh SDM yang berkualitas sandi, menguasai teknik pemeriksaan (audit), yang telah mengikuti bimbingan teknis penggunaan instrumen pengukuran penyelenggaraan persandian yang di tetapkan oleh Lembaga Sandi Negara.
 - (4) Dalam hal Dinas komunikasi dan informatika, penyelenggaraan persandian memiliki keterbatasan SDM sesuai butir 3 diatas, maka pemerintah daerah harus berkonsultasi dengan Lembaga Sandi Negara untuk di tentukan kebijakan lebih lanjut.
 - (5) Penilaian mandiri (*self assesment*) di laporkan secara khusus kepada lembaga sandi negara untuk dilakukan validasi melalui dekstop assessment dan/atau on site assessment.
- 3) Pengukuran tingkat kepuasan Dinas Komunikasi informatika dan Persandian terhadap layanan persandian yang di kelola oleh Dinas Komunikasi Informatika dan Statistik penyelenggaraan persandian. kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
- (1) Penyusunan instrument pengukuran dinas komunikasi dan informatika dan terhadap layanan-layanan persandian dilaksanakan dengan pendekatan ilmiah dan dilakukan pengujian validitas dan reliabilitasnya. instrumen pengukuran di susun sesuai dengan objek layanan yang akan di ukur kepuasannya.
 - (2) Pemerintah Daerah dapat berkonsultasi kepada Lembaga Sandi Negara terkait penggunaan instrumen pengukuran kepuasan perangkat daerah terhadap layanan persandian.
- 4) Penyusunan Laporan Penyelenggaraan Persandian Tahunan (LP2T) Pemerintah Daerah. kegiatan pengawasan dan evaluasi dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
- (1) LP2T berisi tentang hasil pelaksanaan kebijakan, program, dan kegiatan teknis pemerintah daerah termasuk hasil kegiatan pengawasan dan evaluasi yang

menggambarkan hasil penyelenggaraan urusan pemerintah di bidang selama dua tahun.

- (2) Mengoordinasikan penyiapan bahan dan melaksanakan penyusunan LP2T Pemerintah Daerah.
- (3) LP2T Pemerintah Daerah di sampaikan kepada Lembaga Sandi Negara.

G. Koordinasi dan Konsultasi penyelenggaraan persandian untuk pengamanan informasi dalam rangka pelaksanaan urusan pemerintah bidang persandian, unit kerja persandian di Pemerintah Daerah provinsi dan kabupaten/kota dapat melaksanakan koordinasi dan/atau konsultasi ke lembaga sandi negara, dinas komunikasi dan informatika terkait maupun antar pemerintah daerah lainnya.

PARAF KOORDINASI		
NO	UNIT/SATUAN KERJA	PARAF
1	Setda	
2	Asisten I	
3		
4	Plt. Kabag Hukum	
5	Ka. Keminfo	

BUPATI BOMBANA,

H. TAFDIL