BUPATI TIMOR TENGAH UTARA
PROVINSI NUSA TENGGARA TIMUR

PERATURAN BUPATI TIMOR TENGAH UTARA
NOMOR 19 TAHUN 2022
TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI PEMERINTAH DAERAH KABUPATEN TIMOR TENGAH UTARA

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI TIMOR TENGAH UTARA,

Menimbang : a. bahwa setiap pemerintah daerah berkewajiban mengelola informasi publik dan informasi berklasifikasi yang dimilikinya;

b. bahwa untuk melindungi informasi publik dan informasi berklasifikasi perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;

c. bahwa berdasarkan ketentuan Huruf U Lampiran Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimanan telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan Antara Pemerintah Pusat dan Pemerintah Daerah, penyelenggaraan persandian untuk pengamanan infromasi di Lingkungan Pemerintah Daerah Kabupaten adalah merupakan kewenangan Daerah Kabupaten;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah Kabupaten Timor Tengah Utara;

Mengingat : 1. Undang-Undang Nomor 69 Tahun 1958 tentang Pembentukan Daerah-daerah Tingkat II Dalam Wilayah Daerah-daerah Tingkat I Bali, Nusa Tenggara Barat dan Nusa Tenggara Timur (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 122, Tambahan Lembaran Negara Republik Indonesia Nomor 1655);

2. 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 1 Tahun 2022 tentang Hubungan Keuangan Antara Pemerintah Pusat dan Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 1054);
4. Peraturan Daerah Kabupaten Timor Tengah Utara Nomor 6 Tahun 2021 tentang Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2022 (Lembaran Daerah Kabupaten Timor Tengah Utara Tahun 2022 Nomor 6, Tambahan Lembaran Daerah Kabupaten Timor Tengah Utara Nomor 127);
5. Peraturan Bupati Timor Tengah Utara Nomor 36 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik (Berita Daerah Kabupaten Timor Tengah Utara Tahun 2021 Nomor 663);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI PEMERINTAH DAERAH KABUPATEN TIMOR TENGAH UTARA

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Timor Tengah Utara.
2. Bupati adalah Bupati Timor Tengah Utara.
3. Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara yang selanjutnya disebut Dinas adalah dinas yang menangani urusan persandian di Kabupaten Timor Tengah Utara.
4. 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.
5. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan informasi.
6. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.

7. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
8. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikat elektronik.
9. Layanan Keamanan Informasi adalah keluaran dari 1(satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
10. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
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

Penyelenggaraan persandian untuk pengamanan informasi menggunakan asas:
a. asas keamanan, yaitu pengelolaan dan perlindungan informasi berklasifikasi milik pemerintah 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, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik pemerintah dilaksanakan dengan memastikan bahwa informasi tersebut tidak dapat diubah tanpa ijin dari pihak yang berwenang, menjamin keutuhan informasi dan tata kelolanya;
c. asas ketersediaan, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik pemerintah dilaksanakan untuk menjamin ketersediaan informasi tersebut saat dibutuhkan,dengan memperhatikan kewenangan pengguna informasi;
d. asas kecepatan dan ketepatan, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik pemerintah harus dilakukan tepat waktu dan tepat sasaran;
e. asas efektif dan efisien, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik pemerintah daerah harus dilakukan secara efektif dan efisien sesuai dengan klasifikasinya;
f. asas manfaat, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik pemerintah daerah dilaksanakan agar bermanfaat sebesar-besarnya untuk mendukung penyelenggaraan pemerintah daerah;
g. asas profesionalitas, 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, pengelolaan dan perlindungan informasi publik dan informasi berklasifikasi milik pemerintah daerah dilaksanakan dan dipadukan dalam mendukung tugas pemerintah daerah.

BAB III
TUJUAN DAN RUANG LINGKUP

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi pemerintah daerah bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan Persandian untuk pengamanan informasi antara Pemerintah Pusat dan Pemerintah Daerah;
b. meningkatkan komitmen, efektivitas, dan kinerja pemerintah daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan persandian untuk pengamanan infromasi; dan
c. memberikan pedoman bagi pemerintah daerah dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah.

Pasal 4

(1) Penyelenggaraan persandian untuk pengamanan informasi 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 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;
   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, seteksi, proteksi, penanggulangan dan pemulihan;
   c. klarifikasi berita hoax; dan
   d. layanan terhadap aduan kejahatan dunia maya.

(5) Tata cara penyelenggaraan persandian untuk pengamanan informasi pemerintah daerah tercantum dalam lampiran yang merupakan bagian yang tidak terpisahkan dari peraturan bupati ini.

BAB IV
ORGANISASI, SUMBER DAYA MANUSIA, SARANA DAN PRASARANA

Pasal 5

(1) Bupati melakukan penyelenggaraan persandian dengan dibantu oleh Dinas.
(2) Penyelenggaraan persandian di Pemerintah Daerah dikoordinir oleh sekurang-kurangnya 1 (satu) Bidang Khusus yang menangani Persandian dan Keamanan Informasi.

Pasal 6

(1) Bidang khusus yang menangani Persandian dan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (2) memiliki paling sedikit 1 (satu) personil yang telah mempunyai sertifikat kualifikasi ahli sandi dan 2 (dua) personil yang memiliki keahlian di bidang Teknologi Informasi.
(2) Sertifikat kualifikasi ahli sandi sebagaimana dimaksud pada ayat (1) diperoleh dengan mengikuti Diklat Ahli Sandi yang diselenggarakan oleh Badan Siber dan Sandi Negara.

Pasal 7

(1) Bidang yang menangani urusan persandian harus menyediakan sarana prasarana persandian sesuai dengan ketentuan peraturan Perundang-undangan.
(2) Pembiayaan penyelenggaraan persandian untuk pengamanan informasi di daerah bersumber dari Anggaran Pendapatan dan Belanja Daerah.

Pasal 8

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.
Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Timor Tengah Utara.

Ditetapkan di Kefamenanu
pada tanggal 10 Maret 2022
BUPATI TIMOR TENGAH UTARA

JUANDI DAVID

Diundangkan di Kefamenanu
pada tanggal 10 Maret 2022

SEKRETARIS DAERAH KABUPATEN TIMOR TENGAH UTARA,

FRANSISKUS B. FAY

BERITA DAERAH KABUPATEN TIMOR TENGAH UTARA TAHUN 2022 NOMOR 796

LAMPIRAN : PERATURAN BUPATI TIMOR TENGAH UTARA
NOMOR 19 TAHUN 2022
TENTANG
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI PEMERINTAH DAERAH KABUPATEN TIMOR TENGAH UTARA

Tata Cara Penyelenggaraan Persandian untuk Pengamanan Informasi Di Pemerintah Daerah Kabupaten Timor Tengah Utara

1. Penyediaan kebijakan penyelenggaraan urusan persandian untuk pengamanan informasi.
   Kebijakan penyelenggaraan persandian untuk pengamanan informasi di Pemerintah Daerah Kabupaten Timor Tengah Utara berupa Peraturan Kepala Dinas, Pedoman, Petunjuk Pelaksanaan, Petunjuk Teknis, atau Standar Operasional Prosedur (SOP).
   Kebijakan tersebut 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 Jaring Komunikasi Sandi.
   b. Kebijakan operasional pengamanan persandian, diantaranya :
      1) Pengamanan kerahasiaan, keutuhan, keaslian, dan nir penyangkalan infromasi 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 Assesment*, kontra penginderaan/ sterilisasi dan jamming;
      8) Pelayanan satu pintu kirim terima berita 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 materiil sandi dan jaring komunikasi sandi;
      5) Peningkatan kesadaran, pemahaman akan pengamanan informasi.
   d. Kebijakan pengawasan dan evaluasi penyelenggaraan persandian, diantaranya :
      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 keamanan informasi;

6) Mengevaluasi tingkat ketersediaan sumber daya persandian, SDM dan peralatan persandian.

2. Penyediaan Analisis Kebutuhan Persandian untuk Pengamanan Informasi.
Kegiatan análisis kebutuhan penyelenggaraan persandian, meliputi:
   a. Identifikasi pola hubungan komunikasi yang digunakan oleh Pemerintah Kabupaten Timor Tengah Utara, 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 pola 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 Jaring Komunikasi Sandi (JKS)
         Identifikasi materiil sandi meliputi identifikasi terhadap kebutuhan peralatan sandi dan kunci sistema sandi yang didasarkan pada kondisi infrastruktur, jenis komunikasi, dan hierarki komunikasinya
         Identifikasi JKS meliputi identifikasi terhadap:
         - Perangkat Daerah yang akan terhubung dalam JKS termasuk didalamnya unit kerja dalam Perangkat Daerah yang akan mengoperasikan peralatan sandi
         - Pejabat Pemerintah Kabupaten Timor Tengah Utara yang akan terhubung dalam JKS termasuk didalamnya penentuan hierarki komunikasi.
         - Infrastruktur komunikasi yang ada di Pemerintahan Kabupaten Timor Tengah Utara
         b) Alat Pendukung Utama (APU) persandian
         Identifikasi APU Persandian meliputi identifikasi kebutuhan terhadap perangkat yang mendukung penyelenggaraan persandian
         c) Tempat Kegiatan Sandi
         Identifikasi Tempat Kegiatan Sandi (TKS) 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 Kabupaten Timor Tengah Utara dalam periode waktu satu tahun anggaran.

c. Menetapkan hasil identifikasi dan análisis 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 Kabupaten Timor Tengah Utara 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 harus dihancurkan secara fisik maupun lojik (*logical security*).

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

1.5 Penggandaan dan/atau perubahan Informasi Berklasifikasi dilakukan harus dengan ijin dari Pemilik Informasi atau Pengelola Informasi.

b) Pemberian Label Informasi berklasifikasi

Informasi Berklasifikasi harus diberi label sesuai dengan tingkat klasifikasi informasinya tergantung 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 aklan 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, hard drive*, dsb. Label ditempelkan pada fisik media penyimpanan dan terlihat 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 dienkripsi dengan aplikasi enkripsi yang direkomendasikan oleh BSSN

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.

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 resiko 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 dalam komputer, mobil devices, atau media penyimpanan pribadi.

v. Penyimpanan dokumen elektronik berklasifikasi harus diduplikasi (back up) secara berkala.

vi. Media penyimpanan dokumen elektronik berklasifikasi dilarang digunakan, dipinjam, atau dibawa keluar 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 diarsipkan 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 BSSN
vi. Menandatangani BAST Pemusnahan

1.2. Pemusnahan dokumen cetak 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 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, estándar, dan prosedur operasional pengamanan informasi publik yang dikecualikan/informasi berklasifikasi.

c) Perlindungan lojik (*logical security*)

1.1. Perlindungan lojik (logical security) menggunakan teknik kriptografi dan stenografi untuk memenuhi aspek : kerahasiaan, keutuhan, otentikasi, dan nir penyangkalan

1.2. Pelindungan lojik (logical security) yang menggunakan teknik kriptografi dan stenografi harus memenuhi estándar dan direkomendasikan oleh Badan Siber dan Sandi Negara

1.3. Untuk menambah keamanan database terutama yang disimpan secara elektronik baik di komputer khusus maupun server, perlu ditambahkan perlindungan lojik antara lain:

i. Pemasangan firewall pada jaringan data yang terhubung di server,
ii. Pemasangan Tools Detection,
iii. Pemasangan antivirus
iv. Pengamanan/pemanfaatan user/passwor
v. Aplikasi keamanan lain yang telah teruji kehandalannya

1.4. Dalam rangka pencegahan dan penanggulangan perlindungan logic, Bagian/Seksi Persandain bekerjasama dengan Unit Pengelola Teknologi Informasi di lingkup Pemerintah Kabupaten Timor Tengah Utara 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

Pengelolaan Sarana dan Prasarana meliputi:

1) Pengelolaan Materiil Sandi dan Jaring Komunikasi Sandi

Pengelolaan terhadap Materiil Sandi dan Jaring Komunikasi Sandi meliputi:

a) Pemenuhan terhadap kebutuhan materiil sandi yang akan digunakan dalam penyelenggaraan JKS eksternal oleh Pemerintah Kabupaten Timor Tengah Utara dapat difasilitasi oleh BSSN dengan mengajukan permohonan kepada BSSN sesuai hasil análisis kebutuhan.

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

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

2) Pengelolaan Alat Pendukung Utama (APU) Persandian

Pengelolaan terhadap APU Persandian meliputi:

a) Pemenuhan APU

Pemenuhan APU Persandian dapat dilakukan secara mandiri dengan wajib meminta rekomendasi dari BSSN atau dapat mengajukan permohonan pemanfaatan APU Persandian kepada BSSN

b) Penyimpanan

Penyimpanan APU Persandian harus memperhatikan syarat-syarat keamanan antara lain:

(1) Lokasi penyimpanan APU Persandian harus dilengkapi kendali akses untuk mencegah resiko kehilangan, kerusakan dan manipulasi
(2) APU Persandian dilarang digunakan, dipinjam, atau dibawa keluar ruang kerja atau kantor tanpa ijin dari penanggungjawab pengelola Materiil Sandi

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

5. Penyelenggaraan operasional dukungan persandian untuk pengamanan informasi
Penyelenggaraan operasional dukungan persandian persandian yang dapat dilaksanakan Pemerintah Kabupaten Timor Tengah Utara
a. *Jamming*
1) *Jamming* adalah upaya pengamanan sinyal dari ancaman penyalahgunaan sinyal dengan cara mengacak atau memutus sinyal komunikasi untuk menghindari tindakan-tindakan yang tidak diinginkan atau kepentingan yang tidak bertanggung jawab.
2) Ruang Lingkup
a) Unit pelayanan yang menyelenggarakan pengkoordinasian *jamming* terhadap peserta rapat terbatas adalah Bidang Statistik dan Persandian pada Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara.
b) Pelaksana adalah seluruh pejabat/pegawai pada Dinas Komunikasi Informatika dan Statistik yang masuk dalam Tim Pengamanan Persandian, 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 Komunikasi, Informatika dan Statistik.
d) Pengguna pelayanan adalah Pejabat Daerah dan pejabat lainnya.
e) Keluaran (output) pelayanan adalah dokumen dan produk naskali dinas kegiatan *jamming*.
f) Kemanfaatan (outcome) pelayanan adalah terselenggaranya *jamming* terhadap rapat terbatas pejabat daerah dan pejabat lainnya di Pemerintah Kabupaten Timor Tengah Utara 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 Kabupaten Timor Tengah Utara. Kegiatan ini berlangsung sampai dengan rapat selesai.

b. Kontra Penginderaan/sterilisasi

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 di Bidang Statistik dan Persandian pada Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara
   b) Pelaksana adalah seluruh pejabat/pegawai pada Dinas Komunikasi Informatika dan Statistik yang masuk dalam Tim Pengamanan Persandian, 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 Statistik Kabupaten Timor Tengah Utara.
   d) Pengguna layanan adalah pejabat daerah dan pejabat lainnya.
   e) Keluaran (outpu) 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 ruangan kerja atau rumah dinas.
   c) Setelah proses pengajuan disetujui Tim akan mengatur jadwal pelaksanaan kegiatan Kontra Penginderaan dengan berkoordinasi dengan Tim BSSN. 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 didapat 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 análisis ini untuk mengetahui ada tidaknya alat penyadap di tempat tersebut yang terekam alat *Counter Survellance*.

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 di kemudian hari dari resiko penyadapan.

c. Pelaksanaan Kegiatan Assessment Keamanan Sistem Informasi

1) Kegiatan Assessment Keamanan Sistem Informasi dilakukan dengan melakukan pemeriksaan terhadap ada tidaknya celah kerawanan pada Sistem Informasi.
2) Pemerintah Kabupaten Timor Tengah Utara melakukan kegiatan Assessment Keamanan Sistem Informasi setelah berkoordinasi dan mengajukan permohonan Assessment Keamanan Sistem Informasi kepada BSSN.
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 Kabupaten Timor Tengah Utara adalah Bidang Statistik dan Persandian pada Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara.
   b) Pelaksana adalah seluruh pejabat/pegawai pada Dinas Komunikasi Informatika dan Statistik yang masuk dalam Tim Pengamanan Persandian, 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 Kabupaten Timor Tengah Utara.
   c) Penanggung jawab pelayanan adalah Kepala Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara.
   d) Sasaran yang hendak dicapai adalah terhindarnya data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara dari ancaman dan kerawanan yang mungkin timbul.
   e) Pengguna layanan adalah seluruh Organisasi Perangkat Daerah (OPD) di Kabupaten Timor Tengah Utara.
   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 Kabupaten Timor Tengah Utara dari ancaman yang ditimbulkan oleh pemanfaatan teknologi telekomunikasi dan elektronika berupa phising, virus, malware dan lainnya.
4) Prosedur Layanan
   a) Kegiatan Assessment Keamanan Sistem Informasi dilakukan terhadap Organisasi Perangkat Daerah (OPD) lingkup Pemerintah Kabupaten Timor Tengah Utara yang mengajukan permintaan.

b) Setelah terdapat permintaan, pelaksanaan 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.

d. Layanan Sertifikat Elektronik
1) Pelaksanaan kegiatan layanan sertifikat elektronik dapat dilakukan oleh Pemerintah Kabupaten Timor Tengah Utara jika telah memenuhi persyaratan dan telah diberikan kewenangan oleh Balai Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).
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, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara adalah Bidang Statistik dan Persandian di Dinas Komunikasi, Informatika dan Statistik
b) Pelaksana adalah seluruh pejabat/pegawai pada Bidang Statistik dan Persandian di Dinas Komunikasi, Informatika dan Statistik dan pengamanan yang secara teknis dan administratif memiliki tugas tugas dan tanggung jawab langsung dalam pengkoordinasian kegiatan pengamanan siber yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara
c) Penanggung jawab layanan adalah Kepala Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara
d) Sasaran yang hendak dicapai adalah terhindarnya data/ informasi, aplikasi, server dan pengolah data lainnya yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara dari ancaman dan kerawanan yang mungkin timbul
e) Pengguna layanan adalah seluruh Organisasi Perangkat Daerah (OPD) di Pemerintah Kabupaten Timor Tengah Utara
f) Keluaran (output) layanan adalah laporan teknis dan rekomendasi hasil kegiatan layanan sertifikat elektronik
g) Kemanfaatan (outcome) layanan adalah terselenggaranya kegiatan layanan sertifikat elektronik terhadap data/informasi, aplikasi, database, server dan pengolah data lainnya yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara 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 Organisasi Perangkat Daerah (OPD) di Pemerintah Kabupaten Timor Tengah Utara yang mengajukan permintaan
   b) Setelah terdapat permintaan, pelaksanaan kegiatan layanan sertifikat elektronik akan dikoordinasikan dengan pihak BSSN 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

e. Penyelenggaraan Security Operation Center (SOC)
Penyelenggaraan SOC dapat dilakukan secara mandiri namun tetap bekerjasama dengan BSSN sebagai instansi pembina dimana infrastruktur SOC pada Pemerintah Kabupaten Timor Tengah Utara data terhubung dengan BSSN, sehingga kegiatan akan berlangsung responsif

6. Pengamanan Informasi Siber
Penyelenggaraan operasional informasi siber dapat dilaksanakan dengan membentuk tim satuan tugas *Cyber Incident Response Team (CIRT)*.
   a. Tim satuan tugas *Cyber Incident Response Team (CIRT)* mempunyai tugas yang dijabarkan dalam kelompok kerja sebagai berikut:
      1) Operasi Patroli Siber, merupakan kegiatan untuk identifikasi, deteksi, proteksi, penanggulangan dan pemulihan serta melaksanakan klarifikasi dari ancaman sesatnya verita hoax, modus penipuan dan pembunuhan karakter, pencemaran nama baik, ujaran kebencian, isu SARA, pemecah belah NKRI, Bhineka Tunggal Ika, Pancasila dan UUD 1945;
      2) Layanan aduan kejahatan siber, merupakan kegiatan pelayanan kepada masyarakat sebagai korban kejahatan siber, modus penipuan dan pembunuhan karakter;
      3) Pembinaan pengamanan informasi siber, merupakan kegiatan usaha merubah mindset generasi millenial sekolah-sekolah, organisasi elemen masyarakat dan jajaran pimpinan/staf OPD se-Kabupaten Timor Tengah Utara dari ancaman *hoax*;
      4) Pengawasan dan evaluasi pengamanan informasi siber yang dilaksanakan oleh kelom[pok kerja satuan tugas Cyber Incident Response Team;
      5) 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 millenial dari ancaman berita hoax yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara Bidang Statistik dan Persandian pada Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara;
      2) Pelaksana adalah seluruh tim stakeholder Satgas CIRT yang dibentuk oleh Bidang Statistik dan Persandian pada Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara dan Pengamanan yang secara teknis dan administratif memiliki tugas dan tanggung jawab langsung dalam pengkoordinasian kegiatan pengamanan siber yang dimiliki oleh Pemerintah kabupaten Timor Tengah Utara;

3) Penanggung jawab pelayanan adalah Kepala Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara;
4) Sasaran yang hendak dicapai adalah terhindarnya data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Kabupaten Timor Tengah Utara dari ancaman dan kerawanan siber dan hoax yang mungkin timbul;
5) Pengguna pelayanan adalah seluruh Organisasi Perangkat Daerah (OPD) di Pemerintah Kabupaten Timor Tengah Utara;
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 Kabupaten Timor Tengah Utara dari ancaman hoax dan kejahatan siber, modus penipuan dan pembunuhan karakter, yang ditimbulkan oleh pemanfaatan teknologi, informasi, telekomunikasi di dunia maya/ media sosial berupa ancaman sesatnya hoax dari pihak siber luar.

c. Prosedur Layanan
1) Operasi Patroli Siber
   a) Membuat akun resmi CIRT Timor Tengah Utara di jejaring media sosial;
   b) Melakukan kegiatan operasi patroli siber oleh tim Satgas CIRT pokja operasi patroli siber di jejaring media sosial;
   c) Melakukan identifikasi, deteksi, proteksi, penanggulangan dan pemulihan serta melaksanakan klarifikasi dari ancaman sesatnya berita hoax, modus penipuan dan pembunuhan karakter, pencemaran nama baik, ujaran kebencian, isu SARA, pemecah belah NKRI, Bhineka Tunggal Ika, Pancasila dan UUD 1945;
   d) Membuat laporan hasil dan rekomendasi dari kegiatan operasi patroli siber.
2) Layanan Aduan Kejahatan Siber
   a) Menerima layanan aduan korban kejahatan siber, secara langsung maupun kontak person, email satgas, atau whatsap;
   b) Pengisian form aduan, disertakan id pelapor;
   c) Mencatat kronologis kejadian dan bukti screenshot;
   d) Mengidentifikasi dan deteksi masalah dan kejahatan siber;
   e) Mengirim dokumen ke Polres Timor Tengah Utara untuk proses forensik dan proses pidana hukum;
   f) Melakukan penanggulangan dan pemulihan;
   g) Membuat laporan hasil pelayanan aduan kejahatan siber.
3) Pembinaan pengamanan informasi siber
   a) Membuat materi Tips anti hoax;
   b) Membuat video pendek tolak tegas hoax dan menyebarkan di jejaring media sosial;
   c) Membuat materi Sosialisasi, Forum Grup Diskusi, dan kampanye siber;
   d) Menyelenggarakan sosialisasi tips cerdas dan cermat dalam bermedia sosial;
   e) Menyelenggarakan sosialisasi pengamanan informasi siber pada generasi millenial di sekolah-sekolah dan jajaran pimpinan/staf OPD se-Kabupaten Timor Tengah Utara;
   f) Membuat laporan hasil Pembinaan pengamanan informasi siber.

4) Pengawasan pengamanan informasi siber
   a) Membuat materi quesioner guna mengevaluasi tingkat kesadaran, pemahaman akan keamanan informasi siber pada generasi millenial, sekolah-sekolah dan jajaran pimpinan/staf OPD se-Kabupaten Timor Tengah Utara;
   b) Menyebarkan quesioner evaluasi kepada generasi millenial di sekolah-sekolah dan jajaran pimpinan/staf OPD se-Kabupaten Timor Tengah Utara;
   c) Melakukan pengawasan pada pokja satgas CIRT;
   d) Membuat dokumen pengawasan keamanan informasi siber pada satgas CIRT;
   e) Membuat laporan hasil evaluasi dan pengawasan secara rutin, berkala dan semester.
5) Publikasi dan dokumentasi pengamanan informasi siber
   a) Mempublikasikan seluruh kegiatan tim pokja satgas CIRT;
   b) Mempublikasikan materi tips tolak hoax dan video pendek tolak tegas berita hoax di akun resmi Pemerintah Kabupaten Timor Tengah Utara;
   c) Mendukung klarifikasi berita hoax;
   d) Mengembalikan citra positif Pemerintah Kabupaten Timor Tengah Utara;
   e) 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 Kabupaten Timor Tengah Utara harus terlapor kepada Pemerintah Provinsi Nusa Tenggara Timur 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 resiko penyelenggaraan persandian di Pemerintah Kabupaten Timor Tengah Utara. Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
            i. Pemerintah Kabupaten Timor Tengah Utara melaksanakan kebijakan manajemen resiko yang ditetapkan oleh BSSN
            ii. Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara sebagai penyelenggara persandian melaksanakan fungsi koordinasi pelaksanaan kebijakan manajemen resiko penyelenggaraan persandian
            iii. Dalam hal terdapat potensi insiden dan/atau terjadinya insiden penyelenggaraan persandian dan keamanan informasi, Pemerintah Kabupaten Timor Tengah Utara membantu pelaksanaan tugas pemeriksaan persandian khusus (audit khusus) atau investigasi yang dilaksanakan oleh BSSN atas terjadinya insiden penyelenggaraan persandian dan keamanan informasi.

2) Pengawasan dan evaluasi yang bersifat tahunan sebagi berikut:
   a) Pengukuran tingkat pemanfaatan layanan persandian oleh Pemerintah Provinsi Nusa Tenggara Timur. Dalam melaksanakan pengukuran tingkat pemanfaatan layanan persandian perlu memperhatikan hal-hal sebagai berikut:
      i. Jumlah perangkat daerah yang memanfaatkan' análisis kebutuhan penyelenggaraan persandian untuk pengamanan informasi
      ii. Jumlah perangkat daerah yang melaksanakan pengelolaan dan perlindungan informasi
      iii. Jumlah perangkat daerah yang memenfaatkan layanan penyelenggaraan operasional dukungan persandian untuk pengamanan informasi
   b) Penilaian mandiri (self assessment) terhadap penyelenggaraan persandian pada Pemerintah Kabupaten Timor Tengah Utara.
      Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
      i. Penilaian mandiri (self assessment) merupakan pengukuran penyelenggaraan persandian mandiri yang dilaksanakan dengan menggunakan instrumen pengukuran penyelenggaraan persandian yang telah ditetapkan oleh BSSN
      ii. Dalam melakukan penilaian mandiri (self assessment) diperlukan objektivitas yang tinggi sesuai dengan kondisi penyelenggaraan persandian di Pemerintah Daerah. Oleh sebab itu dibutuhkan bukti pendukung yang valid sehingga hasilnya dapat dipertanggungjawabkan
      iii. Penilaian mandiri (self assessment) dilakukan oleh Sumber Daya Manusia yang berkualifikasi sandi, menguasai teknik pemeriksaan (audit), dan telah mengikuti bimbingan teknis penggunaan instrumen pengukuran penyelenggaraan persandian yang ditetapkan oleh BSSN
      iv. Dalam hal perangkat daerah penyelenggara persandian memiliki keterbatasan SDM sesuai butir iii di atas, maka harus berkonsultasi dengan BSSN untuk ditentukan kebijakan lebih lanjut
      v. Penilaian mandiri (self assessment) akan menghasilkan opini mandiri yang bersifat sementara tentang penyelenggaraan persandian di Pemerinrah Kabupaten Timor Tengah Utara
      vi. Hasil penilaian mandiri (self assessment) dilaporkan secara khusus kepada BSSN untuk dilakukan validasi melalui Desktop Assesssment dan/atau Onsite Assessment.

   c) Pengukuran tingkat kepuasan perangkat daerah terhadap layanan persandian yang dikelola oleh Dinas Komunikasi, Informatika dan Statistik Kabupaten Timor Tengah Utara.
      Kegiatan ini dilaksanakan dengan memperhatikan ketentuan sebagi berikut:
      i. Penyusunan instrumen pengukuran perangkat daerah terhadap layanan persandian dilaksanakan dengan pendekatan ilmiah dan dilakukan pengujian validitas dan realibilitasnya. Instrumen pengukuran disusun sesuai dengan objek layanan yang akan diukur kepuasannya.
      ii. Pemerintah Kabupaten dapat berkonsultasi kepada BSSN terkait penggunaan instrumen pengukuran kepuasan perangkat daerah terhadap layanan persandian.

(LP2T) Pemerintah Daerah

Kegiatan penyusunan LP2T Pemerintah Daerah ini dilaksanakan dengan memperhatikan ketentuan sebagi berikut:

i. LP2T berisi tentang hasil pelaksanaan kebijakan, program, dan kegiatan teknis termasuk hasil kegiatan pengawasan dan evaluasi yang menggambarkan hasil penyelenggaraan urusan pemerintahan di bidang persandain selama satu tahun
ii. Mengkoordinasikan penyiapan bahan dan melaksanakan penyusunan
iii. LP2T Pemerintah Daerah disampaikan kepada Gubernur

8. Koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi

   Dalam rangka pelaksanaan urusan pemerintahan bidang persandian, unit kerja persandian melaksanakan koordinasi dan/atau konsultasi ke BSSN, perangkat daerah terkait maupun antar pemerintah daerah lainnya.

9. Sarana dan Prasarana Operasional Persandian

   Adapun saran prasarana yang disediakan dalam menyelenggarakan operasional persandian antara lain:

   a. Mempunyai tempat kegiatan persandian, yaitu:
      1) Tempat kegiatan administrasi persandian
      2) Tempat kegiatan persandian yang disebut Kamar Sandi (KASA)
   b. Mempunyai peralatan sandi yang disediakan atau direkomendasikan oleh Badan Siber dan Sandi Negara
   c. Jaringan internet dan jaringan komunikasi
   d. Peralatan pendukung lainnya yang diperlukan

BUPATI TIMOR TENGAH UTARA

JUANDI DAVID