



BUPATI MUSI RAWAS

PROVINSI SUMATERA SELATAN
PERATURAN BUPATI MUSI RAWAS

NOMOR 54. TAHUN 2023

TENTANG

PEDOMAN PELAKSANAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MUSI RAWAS,

- Menimbang** : a. bahwa berdasarkan ketentuan Pasal 4 ayat (1) huruf a Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, penyelenggaraan persandian untuk pengamanan informasi pemerintah dalam kabupaten dilaksanakan melalui penyusunan kebijakan pengamanan informasi;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Bupati tentang Pedoman Pelaksanaan Persandian untuk Pengamanan Informasi.
- Mengingat** : 1. Undang-Undang Nomor 28 Tahun 1959 tentang Pembentukan Daerah Tingkat II termasuk Kotapraja, dalam Lingkungan Darah Tingkat I Sumatera Selatan (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Tahun 1821);
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843), sebagaimana telah diubah dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

2

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 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
6. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
7. Peraturan Daerah Kabupaten Musi Rawas Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Musi Rawas (Lembaran Daerah Kabupaten Musi Rawas Tahun 2016 Nomor 10), sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Musi Rawas Nomor 1 Tahun 2021 tentang Perubahan atas Peraturan Daerah Kabupaten Musi Rawas Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Musi Rawas (Lembaran Daerah Kabupaten Musi Rawas Tahun 2021 Nomor 1).

MEMUTUSKAN:

Menetapkan : **PERATURAN BUPATI TENTANG PEDOMAN PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.**

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Musi Rawas.
2. Pemerintahan Daerah adalah Pemerintah Kabupaten Musi Rawas.
3. Perangkat Daerah adalah unsur pembantu Kepala Daerah dan DPRD dalam penyelenggaraan urusan pemerintah yang menjadi kewenangan Daerah.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Musi Rawas.
5. Satuan Kerja Perangkat Daerah yang selanjutnya disingkat SKPD adalah Satuan Kerja di lingkungan Pemerintah Kabupaten Musi Rawas.

6. Dinas Komunikasi, Informatika dan Statistik yang selanjutnya disebut Diskominfo dan Statistik adalah SKPD yang bertanggung jawab terhadap pelaksanaan Persandian untuk pengamanan informasi.
7. Urusan Pemerintahan adalah kekuasaan pemerintahan yang menjadi kewenangan Presiden yang pelaksanaannya dilakukan oleh kementerian negara dan penyelenggara Pemerintahan Daerah untuk melindungi, melayani, memberdayakan dan menyesajahterakan masyarakat.
8. 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.
9. Materil Sandi yang selanjutnya disebut Matsan adalah barang persandian negara yang memiliki klasifikasi rahasia dan berfungsi sebagai alat pengamanan informasi atau alat analisis sinyal atau bahan/perangkat yang berhubungan dengan proses penyelenggaraan pengamanan informasi.
10. Pola Hubungan Komunikasi Sandi adalah bentuk atau pola hubungan antara dua entitas atau lebih dalam proses pengiriman dan penerimaan informasi/pesan/berita secara aman menggunakan persandian.
11. Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik adalah penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data dan informasi, penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintah berbasis elektronik serta penjaminan keutuhan, ketersediaan, dan keaslian.
12. Pengguna Persandian adalah pejabat pada instansi Pemerintah yang memanfaatkan persandian untuk pengamanan informasi.
13. Sumber Daya Manusia Sandi yang selanjutnya disebut SDM Sandi adalah pegawai instansi pemerintah yang bekerja di bidang persandian untuk pengamanan Informasi.
14. Jaring Komunikasi Sandi yang selanjutnya disebut JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
15. Alat Pendukung Utama Persandian yang selanjutnya disebut APU Persandian adalah peralatan pendukung yang digunakan dalam kegiatan pengamanan persandian.
16. *Jamming* adalah kegiatan untuk mengacak sinyal di waktu dan tempat tertentu.

17. Operasi Siaga Kontra Penginderaan yang selanjutnya disebut Kontra Penginderaan adalah kegiatan yang dibatasi waktu untuk melakukan pencegahan terhadap pengawasan pihak lain, termasuk metode-metode yang melibatkan peralatan elektronik seperti *bugsweeping* dan mendeteksi adanya peralatan pengawasan (*surveillance*).
18. *Security Operation Center* yang selanjutnya disebut SOC adalah kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.
19. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
20. Informasi publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara yang berkaitan dengan kepentingan publik.
21. Informasi berklasifikasi adalah informasi publik yang dikecualikan menurut Peraturan Perundang-Undangan.

BAB II MAKSUD, TUJUAN DAN RUANG LINGKUP

Pasal 2

Peraturan Bupati ini dimaksudkan untuk memberikan pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan pelaksanaan persandian untuk pengamanan informasi.

Pasal 3

Peraturan Bupati ini bertujuan untuk:

- a. menciptakan harmonisasi dalam pembagian urusan pemerintahan bidang Persandian;
- b. memfasilitasi Diskominfo dan Statistik dalam pelaksanaan Persandian untuk pengamanan informasi; dan
- c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan pelaksanaan Persandian untuk pengamanan informasi.

Pasal 4

- (1) Pelaksanaan Persandian untuk pengamanan informasi di Pemerintah Daerah meliputi:
 - a. penyediaan analisis kebutuhan pelaksanaan persandian untuk pengamanan informasi;
 - b. penyediaan kebijakan pelaksanaan persandian untuk pengamanan informasi;
 - c. pengelolaan dan perlindungan informasi;
 - 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;
 - f. pengawasan dan evaluasi pelaksanaan pengamanan informasi melalui Persandian di seluruh Perangkat Daerah; dan
 - g. koordinasi dan konsultasi pelaksanaan Persandian untuk pengamanan informasi.
- (2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) mencakup pengamanan fisik, pengamanan logik dan perlindungan secara administrasi.
- (3) Tata Cara pelaksanaan Persandian untuk pengamanan informasi di Daerah sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 5

Ruang lingkup pelaksanaan Persandian untuk pengamanan informasi Pemerintah Daerah meliputi tahap:

- a. perencanaan;
- b. pelaksanaan;
- c. monitoring dan evaluasi;
- d. kerja sama;
- e. pelaporan; dan
- f. pembiayaan, pembinaan dan pengawasan.

Pasal 6

Perencanaan pelaksanaan Persandian untuk pengamanan informasi Pemerintah Daerah diintegrasikan dengan dokumen perencanaan pembangunan daerah berupa Rencana Pembangunan Jangka Panjang Daerah (RPJPD), Rencana Pembangunan Jangka Menengah Daerah (RPJMD) dan Rencana Kerja Pemerintah Daerah (RKPD).

Pasal 7

Pelaksanaan Persandian untuk pengamanan informasi Pemerintah Daerah dipimpin oleh Bupati dengan tugas:

- a. penguatan kapasitas kelembagaan, SDM dan sarana prasarana;
- b. mengoordinasikan kegiatan antar Perangkat Daerah; dan
- c. kerja sama dengan Badan Siber dan Sandi Negara, Perangkat Daerah terkait maupun antar Pemerintah Daerah lainnya.

Pasal 8

- (1) Monitoring dan evaluasi dilaksanakan oleh Bupati.
- (2) Guna kelancaran pelaksanaan tugas sebagaimana dimaksud pada ayat (1) Bupati dapat membentuk tim yang susunan keanggotaannya terdiri dari unsur instansi terkait sesuai kebutuhan.

Pasal 9

- (1) Pelaporan hasil pelaksanaan persandian untuk pengamanan informasi Pemerintah Daerah disampaikan oleh Kepala Diskominfo dan Statistik kepada Bupati.
- (2) Bupati menyampaikan laporan pelaksanaan Persandian untuk pengaman informasi sebagaimana dimaksud pada ayat (1) kepada Kepala Badan Siber dan Sandi Negara sebagai pembina tunggal Persandian Negara dengan tembusan kepada Menteri Dalam Negeri.

BAB III

PEMBIAYAAN, PEMBINAAN DAN PENGAWASAN

Pasal 10

Pembiayaan yang timbul sebagai akibat ditetapkannya Peraturan Bupati ini dibebankan pada:

- a. Anggaran Pendapatan Dan Belanja Daerah; dan
- b. Sumber Dana Lain yang sah dan tidak mengikat.

Pasal 11

Pembinaan dan pengawasan umum serta teknis Pelaksanaan Persandian untuk pengaman informasi Pemerintah Daerah dilaksanakan oleh Bupati sebagai wakil Pemerintah Daerah.

BAB IV
KETENTUAN PENUTUP

Pasal 12

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Musi Rawas.

Ditetapkan di Muara Beliti
pada tanggal, 24 November 2023
BUPATI MUSI RAWAS,

dto

RATNA MACHMUD

Diundangkan di Muara Beliti
pada tanggal, 24 November 2023
Pj. SEKRETARIS DAERAH
KABUPATEN MUSI RAWAS,

dto

AIDIL RUSMAN

BERITA DAERAH KABUPATEN MUSI RAWAS TAHUN 2023 NOMOR 54

SALINAN SESUAI DENGAN ASLINYA
Pj. KEPALA BAGIAN HUKUM



MAYA WIDYA NINGSIH, S.H
Penata Tk. I
NIP. 19710301 200604 2 006

LAMPIRAN PERATURAN BUPATI MUSI RAWAS
NOMOR 54 TAHUN 2023
TENTANG PEDOMAN PELAKSANAAN
PERSANDIAN UNTUK
PENGAMANAN
INFORMASI

TATA CARA PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN
INFORMASI DI LINGKUNGAN PEMERINTAHAN
KABUPATEN MUSI RAWAS

1. Penyediaan kebijakan pelaksanaan persandian untuk pengamanan informasi di Pemerintahan Daerah dapat berupa Peraturan Daerah, Peraturan Kepala Daerah, Peraturan Kepala Dinas, Pedoman, Petunjuk Pelaksanaan, Petunjuk Teknis atau *Standard Operating Procedure* (SOP). Kebijakan tersebut dapat meliputi:
 - a. kebijakan tata kelola persandian, di antaranya:
 - 1) pengelolaan dan perlindungan informasi;
 - 2) tata cara klasifikasi tingkat kerahasiaan informasi;
 - 3) pengendalian akses terhadap informasi; dan
 - 4) pengelolaan jaringan komunikasi sandi.
 - b. kebijakan operasional pelaksanaan persandian untuk pengamanan Informasi, di antaranya:
 - 1) pengamanan kerahasiaan, keutuhan, keaslian dan nir penyangkalan informasi dan sistem menggunakan sertifikat elektronik;
 - 2) pengamanan perangkat dan fasilitas pengolahan data dan informasi;
 - 3) pengamanan jaring komunikasi sandi;
 - 4) pelaksanaan dan pengamanan *video conference*;
 - 5) pelaksanaan kontra penginderaan dan *jamming*; dan
 - 6) pelayanan satu pintu kirim terima informasi.
 - c. kebijakan pengelolaan Sumber Daya Persandian, di antaranya:
 - 1) pemenuhan kompetensi dan kuantitas sdm;
 - 2) pengendalian akses terhadap matsan dan jaring komunikasi sandi;
 - 3) pemeliharaan dan perbaikan umum matsan;
 - 4) penyediaan matsan dan jaringan komunikasi sandi; dan
 - 5) peningkatan kesadaran pengamanan informasi.
 - d. kebijakan pengawasan dan evaluasi pelaksanaan persandian untuk pengaman informasi.
2. Penyediaan analisis kebutuhan Persandian untuk pengamanan informasi kegiatan analisis kebutuhan pelaksanaan Persandian, meliputi:
 - a. identifikasi pola hubungan komunikasi yang digunakan oleh Pemerintah Daerah, di antaranya meliputi:
 - 1) mengidentifikasi pola hubungan komunikasi Bupati dan Wakil Bupati serta 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 Wakil Bupati serta pejabat Daerah lainnya.

- b. langkah-langkah analisis dalam menata pola hubungan komunikasi sandi yang diperlukan berdasarkan hasil identifikasi pola hubungan komunikasi yang sudah ada (poin a di atas) diatur dalam peraturan tersendiri; dan
 - c. menetapkan hasil identifikasi dan analisis pola hubungan komunikasi sandi melalui Keputusan Kepala Daerah, 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, di Pemerintah Daerah meliputi hal-hal sebagai berikut:
- a. fasilitasi penentuan tingkat kerahasiaan informasi berklasifikasi;
 - b. pengelolaan dan perlindungan informasi publik yang dikecualikan/informasi berklasifikasi;
 - 1) pengelolaan informasi publik yang dikecualikan/informasi berklasifikasi meliputi pembuatan, pemberian label, pengiriman, penyimpanan;
 - 2) perlindungan informasi publik yang dikecualikan/informasi berklasifikasi meliputi:
 - a) perlindungan fisik dilakukan melalui kendali akses ruang, pemasangan teralis dan kunci ganda, pemasangan CCTV;
 - b) perlindungan administrasi, dilakukan dengan berpedoman pada kebijakan, standar, dan prosedur operasional pengamanan informasi publik yang dikecualikan/informasi berklasifikasi;
 - c) Perlindungan logik (*logical security*)
 - 1) Perlindungan logik (*logical security*) menggunakan teknik kriptografi dan steganografi untuk memenuhi aspek; kerahasiaan, keutuhan, otentikasi dan nir penyangkalan; dan
 - 2) Perlindungan logik (*logical security*) yang menggunakan teknik kriptografi dan steganografi harus memenuhi standar dan direkomendasikan oleh BSSN.
 - c. pengelolaan dan perlindungan informasi terbuka;
 - d. penyelenggaraan Jaring Komunikasi Sandi (JKS) untuk pengamanan informasi; dan
 - e. penerapan tanda tangan elektronik dan enkripsi pada informasi.
4. Pengelolaan Sumber Daya Persandian, terdiri atas:
- a. Pengelolaan Sumber Daya Manusia, meliputi:
 - 1) Perencanaan kebutuhan SDM, yang bertugas di bidang persandian disusun dengan memperhatikan jumlah dan kompetensi yang dibutuhkan. Dalam kegiatan perencanaan ini, unit yang menangani persandian dapat menyusun Analisis Beban Kerja (ABK) dan Formasi Jabatan Fungsional Sandiman serta mengajukan usulan kebutuhan tersebut kepada Badan Kepegawaian Daerah;
 - 2) Pengembangan kompetensi SDM, yang bertugas di bidang persandian di antaranya melalui Diklat Fungsional Sandiman (Pembentukan dan Penjurusan), Diklat Teknis Sandi, Bimbingan Teknis/Asistensi/*Workshop*/Seminar terkait dengan Persandian dan Teknologi Informasi serta bidang ilmu lainnya yang dibutuhkan;

- 3) Pengajuan Tunjangan Pengamanan Persandian (TPP) sebagai bentuk pemberian kompensasi atas tanggung jawab dalam melaksanakan tugas di bidang penyelenggaraan persandian untuk pengamanan persandian;
 - 4) Pengajuan Tunjangan Jabatan Fungsional Sandiman bagi pegawai yang diangkat dalam Jabatan Fungsional Sandiman; dan
 - 5) Pengajuan usulan pemberian Tanda Penghargaan Bidang Persandian untuk SDM yang bertugas di bidang persandian yang telah memenuhi syarat kepada Kepala BSSN.
- b. Pengelolaan Sarana dan Prasarana, meliputi:
- 1) Pengelolaan Matsan dan JKS, meliputi:
 - a) pemenuhan terhadap kebutuhan matsan yang akan digunakan dalam penyelenggaraan JKS eksternal oleh Pemerintah Provinsi/Kabupaten/Kota dapat difasilitasi oleh BSSN dengan mengajukan permohonan kepada BSSN sesuai hasil analisis kebutuhan;
 - b) pemenuhan kebutuhan matsan yang akan digunakan dalam penyelenggaraan JKS sesuai dengan analisis kebutuhan; dan
 - c) penyimpanan matsan (peralatan sandi dan kunci sistem sandi) berdasarkan ketentuan yang berlaku.
 - 2) Pengelolaan APU Persandian, meliputi:
 - a) pemenuhan APU Persandian dapat dilakukan secara mandiri dengan wajib meminta rekomendasi dari BSSN atau dapat mengajukan permohonan pemanfaatan APU Persandian kepada BSSN;
 - b) penyimpanan APU Persandian dengan memperhatikan syarat-syarat keamanan antara lain:
 1. lokasi penyimpanan APU Persandian harus dilengkapi kendali akses untuk mencegah risiko kehilangan, kerusakan, dan manipulasi; dan
 2. APU Persandian dilarang digunakan, dipinjam, atau dibawa ke luar ruang kerja atau kantor tanpa izin dari Penanggung Jawab pengelola Matsan.
 - c) Pemeliharaan APU Persandian dilaksanakan dengan melakukan perawatan dan perbaikan (bila ada kerusakan) sesuai dengan kewenangan yang dimiliki.
5. Pelaksanaan operasional dukungan persandian untuk pengamanan informasi penyelenggaraan operasional dukungan persandian yang dapat dilaksanakan Pemerintah Provinsi/Kabupaten/Kota, di antaranya:
- a. *Jamming*, dilaksanakan sesuai permohonan dan digunakan sesuai batasannya.
 - b. Kontra Penginderaan:
 - 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 pengawasan (*surveillance*);

- 3) temuan hasil kontra penginderaan berupa barang-barang yang diduga menjadi peralatan pengawasan (*surveillance*) dapat dikonsultasikan ke BSSN;
 - 4) pelaksanaan kegiatan kontra penginderaan dilakukan secara berkala; dan
 - 5) Pemerintah Daerah dapat melakukan kegiatan kontra penginderaan secara mandiri. Apabila tidak dapat melakukan secara mandiri, maka dapat mengajukan permohonan kegiatan kontra penginderaan kepada BSSN.
- c. Pelaksanaan Kegiatan Penilaian Keamanan Sistem Informasi:
- 1) Kegiatan Penilaian Keamanan Sistem Informasi dilakukan dengan melakukan pemeriksaan terhadap ada atau tidaknya celah kerawanan pada Sistem Informasi; dan
 - 2) Pemerintah Daerah dapat melakukan kegiatan Penilaian Keamanan Sistem Informasi secara mandiri. Apabila tidak dapat melakukan secara mandiri, maka dapat mengajukan permohonan Penilaian Keamanan Sistem Informasi kepada BSSN.
- d. Layanan Sertifikat Elektronik:
- 1) pelaksanaan kegiatan layanan sertifikat elektronik dapat dilakukan oleh Pemerintah Provinsi dan Kabupaten/Kota jika telah memenuhi persyaratan dan telah diberikan kewenangan oleh Balai Sertifikasi Elektronik (BSrE), 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; dan
 - d) pengawasan dan evaluasi penggunaan sertifikat elektronik.
 - 3) Tata cara pemanfaatan sertifikat elektronik di lingkungan Pemerintah Daerah diatur dalam peraturan tersendiri.
- e. Pelaksanaan *Security Operation Center* (SOC), dapat dilakukan secara mandiri namun tetap berkerja sama dengan BSSN sebagai instansi pembina dimana infrastruktur SOC pada Pemerintah Kabupaten Musi Rawas dapat terpusat dan terhubung dengan BSSN, sehingga kegiatan akan berlangsung responsif.
6. Pengawasan dan evaluasi pelaksanaan persandian untuk pengamanan informasi di seluruh Perangkat Daerah, dimaksudkan untuk memantau perkembangan, mengidentifikasi hambatan dan upaya perbaikan dalam pelaksanaan Persandian untuk pengamanan Informasi, dengan ketentuan:
- a. pengawasan dan evaluasi pelaksanaan persandian untuk pengamanan informasi Pemerintah Daerah harus terlapor kepada Pemerintah Provinsi agar dapat ditindaklanjuti dengan rencana perbaikan sebagai bahan masukan bagi penyusunan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi tahun berikutnya; dan
 - b. pengawasan dan evaluasi pelaksanaan Persandian untuk pengamanan informasi yang dilaksanakan meliputi:

- 1) Pengawasan dan evaluasi yang bersifat rutin dan insidental sebagai berikut:
 - a) pemantauan penggunaan martsan, aplikasi sandi, dan/atau fasilitas layanan Persandian lainnya;
 - b) melaksanakan kebijakan manajemen risiko pelaksanaan Persandian di Pemerintah Daerah. Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
 1. Pemerintah Daerah melaksanakan kebijakan manajemen risiko yang ditetapkan oleh BSSN;
 2. Perangkat Daerah sebagai pelaksanaan Persandian untuk pengamanan informasi melaksanakan fungsi koordinasi pelaksanaan kebijakan manajemen risiko penyelenggaraan Persandian; dan
 3. dalam hal terdapat potensi insiden dan/atau terjadinya insiden pelaksanaan Persandian dan keamanan informasi, Pemerintah Daerah membantu pelaksanaan tugas Pemeriksaan Persandian Khusus (audit khusus) atau investigasi yang dilaksanakan oleh BSSN atas terjadinya insiden pelaksanaan Persandian untuk keamanan Informasi.
- 2) Pengawasan dan evaluasi yang bersifat tahunan sebagai berikut:
 - a) pengukuran tingkat pemanfaatan layanan Persandian oleh Pemerintah Daerah. Dalam melaksanakan pengukuran tingkat pemanfaatan layanan Persandian perlu memperhatikan hal-hal sebagai berikut:
 1. jumlah Perangkat Daerah yang memanfaatkan analisis kebutuhan pelaksanaan persandian untuk pengamanan Informasi;
 2. jumlah Perangkat Daerah yang melaksanakan pengelolaan dan perlindungan Informasi; dan
 3. jumlah Perangkat Daerah yang memanfaatkan layanan pelaksanaan operasional dukungan Persandian untuk pengamanan Informasi.
 - b) Penilaian mandiri (*self assessment*) terhadap pelaksanaan Persandian pada Pemerintah Daerah, dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
 1. penilaian mandiri (*self assessment*) merupakan pengukuran pelaksanaan Persandian dan pengamanan informasi mandiri yang dilaksanakan dengan menggunakan Instrumen Pengukuran pelaksanaan Persandian untuk pengamanan informasi yang telah ditetapkan oleh BSSN;
 2. dalam melakukan penilaian mandiri (*self assessment*) diperlukan objektivitas yang tinggi sesuai dengan kondisi pelaksanaan Persandian untuk Pengamanan informasi di Pemerintah Daerah. Oleh sebab itu diperlukan bukti pendukung yang valid sehingga hasilnya dapat di pertanggung jawabkan.

3. penilaian mandiri (*self assessment*) dilakukan oleh SDM yang berkualifikasi sandi, menguasai teknik pemeriksaan (audit) dan telah mengikuti bimbingan teknis penggunaan Instrumen Pengukuran pelaksanaan Persandian untuk Pengamanan Informasi yang ditetapkan oleh BSSN;
 4. dalam hal Perangkat Daerah pelaksanaan Persandian dan pengamanan informasi memiliki keterbatasan SDM sesuai butir 3 di atas, maka harus berkonsultasi dengan BSSN untuk menentukan kebijakan selanjutnya;
 5. penilaian mandiri (*self assessment*) akan menghasilkan opini mandiri yang bersifat sementara tentang pelaksanaan Persandian untuk pengamanan informasi di Pemerintah Daerah; dan
 6. hasil penilaian mandiri (*self assessment*) dilaporkan secara khusus kepada BSSN.
- c) pengukuran tingkat kepuasan Perangkat Daerah terhadap layanan Persandian dan pengamanan informasi yang dikelola oleh Perangkat Daerah pelaksana Persandian untuk keamanan informasi, dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
1. penyusunan instrumen pengukuran tingkat kepuasan Perangkat Daerah terhadap layanan Persandian dilaksanakan dengan pendekatan ilmiah dan dilakukan pengujian validitas dan reliabilitasnya. Instrumen pengukuran disusun sesuai dengan objek layanan yang akan diukur kepuasannya; dan
 2. Pemerintah Daerah dapat berkonsultasi kepada BSSN terkait penggunaan instrumen pengukuran tingkat kepuasan Perangkat Daerah terhadap layanan pelaksanaan Persandian.
- d) Penyusunan Laporan pelaksanaan Persandian Tahunan (LP2T) Pemerintah Daerah, dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
1. LP2T berisi tentang hasil pelaksanaan kebijakan, program, dan kegiatan teknis termasuk hasil kegiatan pengawasan dan evaluasi yang menggambarkan hasil pelaksanaan urusan pemerintahan di bidang Persandian selama satu tahun; dan
 2. Mengoordinasikan penyiapan bahan dan melaksanakan penyusunan LP2T.
7. Pelaksana persandian untuk pengamanan informasi dalam rangka pelaksanaan urusan pemerintahan bidang persandian dan unit kerja persandian di Pemerintah Daerah dapat melaksanakan koordinasi dan/atau konsultasi ke BSSN, Perangkat Daerah terkait maupun antar pemerintah daerah lainnya.

BUPATI MUSI RAWAS,

dto

RATNA MACHMUD