WALI KOTA LUBUKLINGGAU
PROVINSI SUMATERA SELATAN

PERATURAN WALI KOTA LUBUKLINGGAU
NOMOR 15 TAHUN 2021

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KOTA LUBUKLINGGAU

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA LUBUKLINGGAU,

Menimbang : a. bahwa dalam rangka mendukung percepatan pengembangan ekonomi dan sosial budaya, serta mewujudkan tata kelola pemerintahan yang baik di Pemerintah Kota Lubuklinggau, perlu didukung oleh kualitas data dan informasi yang baik;

b. bahwa dalam rangka menjamin kualitas dan keamanan informasi di lingkungan Pemerintah Kota Lubuklinggau, perlu dilakukan penyelenggaraan persandian;

c. bahwa berdasarkan Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, penyelenggaraan persandian untuk pengamanan informasi pemerintah daerah merupakan kewenangan pemerintah daerah untuk urusan pemerintahan bidang persandian;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Wali Kota tentang Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Kota Lubuklinggau;

Mengingat : 1. Undang – Undang Nomor 7 Tahun 2001 tentang Pembentukan Kota Lubuklinggau (Lembaran Negara Republik Indonesia Tahun 2001 Nomor 87, Tambahan Lembaran Negara Republik Indonesia Nomor 4114);

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 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);

3. 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 dengan 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);

4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor4846);

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 Presiden Nomor 95 Tahun 2018 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

7. Peraturan Kepala Lembaga Sandi Negara Nomor 9 Tahun 2016 tentang Nomenklatur Perangkat Daerah Dan Unit Kerja Pada Perangkat Daerah Urusan Pemerintahan Bidang Persandian (Berita Negara Republik Indonesia Tahun 2016 Nomor 1314);

8. 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);

9. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);

10. Peraturan Wali Kota Nomor 51 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika Kota Lubuklinggau (Berita Daerah Kota Lubuklinggau Tahun 2016 Nomor 51);

11. Peraturan Wali Kota Nomor 38 Tahun 2018 tentang Sistem Penyelenggaraan Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Lubuklinggau (Berita Acara Kota Lubuklinggau Tahun 2018 Nomor 38).

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KOTA LUBUKLINGGAU.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Pemerintah Kota adalah Pemerintah Kota Lubuklinggau.
2. Wali Kota adalah Wali Kota Lubuklinggau.
3. Perangkat Daerah yang selanjutnya disingkat PD adalah Perangkat Daerah di Lingkungan Pemerintah Kota Lubuklinggau.
4. Kota adalah Kota Lubuklinggau.
5. Dinas Komunikasi dan Informatika yang selanjutnya disebut Dinas adalah Dinas Komunikasi dan Informatika Kota Lubuklinggau.
6. Kepala Dinas Komunikasi dan Informatika yang selanjutnya disebut Kepala Dinas adalah Kepala Dinas Komunikasi dan Informatika Kota Lubuklinggau.

7. 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.

8. Sistem Elektronik adalah serangkaian Perangkat dan Prosedur Elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik.

9. Penyelenggaraan Sistem Elektronik adalah setiap orang penyelenggara negara, badan usaha dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

10. Transaksi elektronik untuk perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer dan/atau media elektronik lainnya.

11. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan dan kenirsangkalan informasi.

12. Sistem manajemen Pengamanan informasi yang selanjutnya disingkat SMPI adalah pengaturan kewajiban bagi penyelenggara sistem elektronik dalam penetapan Manajemen Pengamanan Informasi berdasarkan atas resiko.

13. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah Lembaga pemerintah Republik Indonesia yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan kemanan siber.

14. Pola Hubungan Komunikasi Sandi yang selanjutnya disingkat PHKS adalah bentuk atau pola hubungan antara dua entitas atau lebih dalam proses pengiriman dan penerimaan Informasi secara aman menggunakan Persandian.

15. 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 atau pun non elektronik.

16. Informasi Publik adalah Informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang serta Informasi lain yang berkaitan dengan kepentinganpublik.

17. Informasi yang dikecualikan adalah Informasi yang tidak dapat diakses oleh Pemohon Informasi Publik sebagaimana dimaksud dalam Undang-Undang tentang Keterbukaan Informasi Publik.

18. 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 Sertifikasi Elektronik.

19. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Inforamasi elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentukasi.

Pasal 2

(1) Persandian bertujuan untuk melindungi:
   a. kerahasiaan;
   b. keamanan;
   c. keutuhan;
   d. keautentikan;
   e. ketersediaan; dan
   f. kebertanggungjawaban terhadap Informasi yang disimpan dan dikomunikasikan dalam lingkup Kota.

(2) Penyelenggaraan Persandian merupakan penjabaran atas pelaksanaan kebijakan, program, dan kegiatan di bidang Persandian.

Pasal 3

Ruang lingkup Penyelenggaraan Persandian untuk pengamanan Informasi mencakup:
a. penyusunan kebijakan pengamanan informasi;
b. pengelolaan sumber daya Keamanan Informasi;
c. pengamanan Sistem Elektronik dan Pengamanan informasi nonelektronik;
d. penyediaan layanan Keamanan Informasi; dan
e. pola hubungan komunikasi sandi.

BAB II
PENYELENGGARA PERSANDIAN

Pasal 4

Penyelenggara Persandian untuk pengamanan Informasi di Kota terdiri atas Wali Kota dibantu oleh Dinas.

Pasal 5

(1) Wali Kota sesuai dengan kewenangannya memimpin dan bertanggung jawab atas penyelenggaraan Persandian untuk pengamanan informasi sebagaimana dimaksud dalam pasal 3.

(2) Dinas bertanggung jawab atas kinerja pelaksanaan Persandian sesuai dengan tugas dan fungsinya berdasarkan kebijakan yang ditetapkan oleh Wali Kota.

Pasal 6

Wali Kota dalam memimpin pelaksanaan penyelenggaraan Persandian untuk pengamanan Informasi, melakukan upaya:

a. penguatan kapasitas kelembagaan, sumber daya manusia dan sarana prasarana;
b. mengoordinasikan kegiatan antar PD di Kota;dan
c. kerjasama dengan kabupaten/kota di provinsi lain, serta dengan kabupaten/kota dalam satu provinsi, sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 7

Petunjuk teknis penyelenggaraan persandian untuk pengamanan informasi, tercantum dalam lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan ini.

BAB III
PENYUSUNAN KEBIJAKAN PENGAMANAN INFORMASI

Pasal 8

Dinas menyusun kebijakan Pengamanan Informasi sebagaimana dimaksud dalam pasal 3 huruf a dilakukan dengan :

a. menyusun rencana strategis Pengamanan Informasi;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 9

(1) Rencana stategis sebagaimana dimaksud pada pasal 8 huruf a terdiri atas :
   a. tujuan;
   b. sasaran;
   c. program;
   d. kegiatan;
   e. target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
   f. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.

(2) Rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.

Pasal 10

(1) Wali Kota menetapkan Arsitektur Keamanan Informasi sebagaimana dimaksud dalam pasal 8 huruf a.

(2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
   a. infrastruktur teknologi informasi;
   b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
   c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.

(3) Dalam melakukan penyusunan arsitektur keamanan informasi sebagaimana dimaksud pada ayat (1) dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) Arsitektur keamanan informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

(5) Wali Kota melalui Dinas melakukan evaluasi Arsitektur keamanan informasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai kebutuhan.

Pasal 11

(1) Wali Kota menetapkan tata kelola Keamanan Informasi sebagaimana dimaksud dalam pasal 8 huruf c.

(2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas :
a. keamanan sumber daya teknologi informasi;
b. keamanan akses kontrol;
c. keamanan data dan informasi;
d. keamanan sumber daya manusia;
e. keamanan jaringan;
f. keamanan surat elektronik;
g. keamanan pusat data; dan/atau
h. keamanan komunikasi.

BAB IV
PENGELOLAAN SUMBER DAYA KEAMANAN INFORMASI

Pasal 12

Pengelolaan sumber daya Keamanan Informasi terdiri atas :
a. pengelolaan aset keamanan teknologi informasi dan komunikasi;dan
b. pengelolaan sumber daya.

Pasal 13

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 12 huruf a dilakukan melalui
a. perencanaan,
b. pengadaan,
c. pemanfaatan dan
d. penghapusan terhadap aset keamanan informasi dan komunikasi sandi sesuai dengan ketentuan peraturan perundang-undangan.

(2) Aset keamanan teknologi keamanan informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk:
a. mengidentifikasi,
b. mendeteksi,
c. memproteksi,
d. menganalisis,
e. menanggulangi, dan/atau
f. memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 14

Pengelolaan sumber daya manusia sebagaimana dimaksud dalam pasal 12 huruf b dilakukan melalui :
a. pengembangan kompetensi;
b. pembinaan karir;

c. pendayagunaan; dan
d. pemberian tunjangan pengamanan persandian.

Pasal 15

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 14 huruf a dilaksanakan dengan ketentuan:
   a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, workshop, seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;dan
   b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya,ataupemerintahdaerahmasing-masing.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 14 huruf b dilaksanakan dengan ketentuan:
   a. pembinaan jabatan fungsional di bidang Persandian Keamanan Informasi; dan
   b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.

(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 14 huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Persandian Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja yang ditetapkan.

Pasal 16

(1) Pemberian tunjangan pengamanan persandian sebagaimana dimaksud dalam Pasal 14 huruf d diberikan kepada sumber daya manusia yang bertugas di bidang persandian keamanan informasi.

(2) Pemberian Tunjangan Pengamanan Persandian sebagaimana dimaksud pada ayat (1) diatur dalam ketentuan peraturan perundang-undangan.

BAB V

PENGAMANAN SISTEM ELEKTRONIK DAN PENGAMANAN INFORMASI NON ELEKTRONIK

Pasal 17

Pengamanan Sistem Elektronik yang dilaksanakan terdiri dari:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data dan informasi;
b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 18

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam pasal 17 dilakukan melalui :
   a. identifikasi;
   b. deteksi;
   c. proteksi; dan
   d. penanggulangan dan pemulihan.

(2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.

(3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.

(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan pelindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.

(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 19

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 18 wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.

(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.

(3) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 19 ayat (1) dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai standar yang ditetapkan oleh BSSN.

(2) Pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 21

(1) Pengamanan informasi nonelektronik yang dilaksanakan terdiri dari beberapa tahapan, yaitu :
   a. penerimaan
   b. pemrosesan;
   c. pengiriman dan/atau pendistribusian;
   d. penyimpanan dan/atau pengarsiapan; dan
   e. pemusnahan sesuai jadwal retensi Arsip yang telah ditetapkan.

(2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 22

(1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Kota.

(2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.

(3) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
PENYEDIAAN LAYANAN KEAMANAN INFORMASI

Pasal 23

Layanan Keamanan Informasi disediakan untuk Pengguna Layanan yang meliputi:

a. Wali Kota dan Wakil Wali Kota;
b. PD;
c. pegawai atau aparatur sipil negara pada pemerintah kota; dan
d. pihak lainnya.

Pasal 24

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam pasal 23 meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
d. perlindungan Informasi melalui penyediaan perangkat teknologi Keamanan Informasi dan jaring komunikasi sandi;
e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. audit Keamanan Sistem Elektronik;
g. audit keamanan pelaksanaan sistem manajemen;
h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan pemerintah daerah dan Publik;
i. peningkatan kompetensi sumber daya manusia di bidang Keamanan Informasi dan/atau persandian;
j. pengelolaan pusat operasi Pengamanan Informasi;
k. penanganan insiden Keamanan Sistem Elektronik;
l. perlindungan Informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
m. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan pemerintah daerah melalui kegiatan kontra penginderaan;
n. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
o. jenis Layanan Keamanan Informasi lainnya.

BAB VII
POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 25

(1) Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 3 huruf e ditetapkan oleh Wali Kota.

(2) Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) untuk menentukan jaring komunikasi sandi internal pemerintah kota.

(3) Jaring komunikasi sandi internal pemerintah kota sebagaimana dimaksud pada ayat (2) terdiri atas:
   a. jaring komunikasi sandi antar PD;
   b. jaring komunikasi sandi internal PD; dan
   c. jaring komunikasi sandi pimpinan daerah.

(4) Jaring komunikasi sandi antar PD sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh PD.

(5) Jaring komunikasi sandi internal PD sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal PD.

(6) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Gubernur atau Bupati/Wali Kota, wakil Gubernur atau Bupati/Wali Kota, dan kepala PD.

Pasal 26

(1) Penetapan pola hubungan komunikasi sandi antar PD sebagaimana dimaksud dalam Pasal 25 ayat (1) dilaksanakan melalui:
   a. identifikasi pola hubungan komunikasi sandi; dan
   b. analisis pola hubungan komunikasi sandi.

(2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
   a. pola hubungan komunikasi pimpinan dan pejabat struktural internal pemerintah daerah;
   b. alur informasi yang dikomunikasikan antar PD dan internal PD;
   c. teknologi informasi dan komunikasi;
   d. infrastruktur komunikasi; dan
   e. kompetensi personel.

(3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).

(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
   a. pengguna Layanan yang akan terhubung dalam jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan;
   c. perangkat keamanan teknologi Informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
   d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (5) ditetapkan sebagai pola hubungan komunikasi sandi antar PD provinsi dan kabupaten/kota oleh Gubernur atau Bupati/Wali Kota dalam bentuk keputusan.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat :
   a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
   c. sarana dan prasarana yang digunakan; dan
   d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Wali Kota kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB VIII
PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 27

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah dan penetepan pola hubungan komunikasi sandi antar PD.
(2) PD melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.

(3) PD menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Wali Kota dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 28

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah dan penetapan pola hubungan komunikasi sandi antar PD dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB IX
PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 29

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Kota dan penetepan pola hubungan komunikasi sandi antar PD dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB X
PENDANAAN

Pasal 30

(1) Pendanaan penyelenggaraan Persandian untuk pengamanan Informasi di Kota bersumber dari anggaran pendapatan dan belanja daerah.

(2) Pemerintah Pusat dan Pemerintah Provinsi dapat memberikan bantuan pembiayaan penyelenggaraan Persandian melalui anggaran, pendapatan dan belanja negara sesuai dengan ketentuan peraturan perundang-undangan.

BAB XI
PENUTUP

Pasal 31

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Lubuklinggau.

Ditetapkan di Lubuklinggau
Pada tanggal, 30 maret 2021

WALI KOTA LUBUKLINGGAU

H. S. N. PRANA PUTRA SOHE

Diundangkan Di Lubuklinggau
pada tanggal, 30 maret 2021

SEKRETARIS DAERAH KOTA LUBUKLINGGAU

H.A. RAHMAN SANI

BERITA DAERAH KOTA LUBUKLINGGAU TAHUN 2021 NOMOR 15

LAMPIRAN
PERATURAN WALI KOTA LUBUKLINGGAU
NOMOR 15 TAHUN 2021
TENTANG
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAHKOTA LUBUKLINGGAU

PETUNJUK TEKNIS PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KOTA.

1. Penyediaan kebijakan penyelenggaraan persandian untuk pengamanan informasi.Kebijakan penyelenggaraan persandian untuk pengamanan informasi di Pemerintah Kota berupa Peraturan Kepala Dinas, Pedoman, Petunjuk Pelaksanaan, Petunjuk Teknis, atau *Standard Operational Procedure* (SOP). Kebijakan tersebut dapat meliputi:
   a. Kebijakan tata kelola persandian, diantaranya:
      1) Pengelolaan dan perlindungan informasi berklasifikasi;
      2) Tata cara klasifikasi tingkat kerahasiaan informasi;
      3) Pengendalian akses terhadap informasi;
      4) Pengelolaan jaringan komunikasi sandi.
   b. Kebijakan operasional pengamanan persandian, diantaranya:
      1) Pengamanan kerahasiaan, keutuhan, keaslian, dan nir penyangkalan informasi dan sistem menggunakan sertifikat elektronik;
      2) Pengamanan perangkat dan fasilitas pengolahan data dan informasi;
      3) Pengamanan jaring komunikasi sandi;
      4) Pengamanan informasi elektronik;
      5) Pengamanan informasi siber;
      6) Pelaksanaan dan pengamanan*video conference*;
      7) Pelaksanaan IT Security Assessment, kontrapenginderaan / sterillisasi dan jamming;
      8) Pelayanan satu pintu kirim terima informasi berklasifikasi;
      9) Pelayanan aduan kejahatan siber.
   c. Kebijakan pengelolaan Sumber Daya Persandian, diantaranya ;
      1) Pemenuhan kompetensi dan kuantitas SDM;
      2) Pengendalian akses terhadap materiil sandi dan jaring komunikasi sandi;
      3) Pemeliharaan dan perbaikan umum materiil sandi;
      4) Penyediaan materil sandi dan jaringan komunikasi sandi;
      5) Peningkatan kesadaran, pemahaman akan pengamanan informasi.
   d. Kebijakan pengawasan dan evaluasi penyelenggaraan persandian.
      1) Pengawasan dan evaluasi yang bersifat rutin dan insidentil;
      2) Pengawasan dan evaluasi yang bersifat tahunan;
      3) Pengawasan dan evaluasi informasi digital elektronik/siber;
      4) Mengevaluasi tingkat keamanan IT;
      5) Mengevaluasi tingkat kesadaran, pemahaman kemanan informasi;
      6) Mengevaluasi tingkat ketersediaan sumber daya persandian, SDM dan Peralatan persandian;
2. Penyediaan Analisis Kebutuhan Persandian untuk Pengamanan Informasi.
   Kegiatan analisis kebutuhan penyelenggaraan persandian, meliputi:
   a. Identifikasi pola hubungan komunikasi yang digunakan oleh Pemerintah Kota, diantaranya meliputi

1) Mengidentifikasi pola hubungan komunikasi Wali Kota dan pejabat daerah lainnya yang sedang dilaksanakan.
2) Mengidentifikasi alur informasi yang dikomunikasikan antar PD.
3) Mengidentifikasi dan/atau menyediakan sarana dan prasarana teknologi informasi dan komunikasi yang digunakan oleh Wali Kota dan/atau pejabat daerah lainnya.

b. Analisis pola hubungan komunikasi sandi yang diperlukan berdasarkan hasil identifikasi pola hubungan komunikasi yang sudah ada sebagaimana dimaksud pada huruf a meliputi:
1) Mengidentifikasi pengelola layanan penyelenggaraan persandian Identifikasi pengelola yaitu kegiatan untuk mengidentifikasi personil dan kompetensi yang dibutuhkan dalam menyelenggarakan kegiatan persandian.
2) Mengidentifikasi Sarana danPrasarana
a) Materiil Sandi dan Jaring KomunikasiSandi
1) Materiil Sandi
Identifikasi Materiil Sandi meliputi identifikasi terhadap kebutuhan peralatan sandidan kunci sistem sandi yang didasarkan pada kondisi infrastuktur, jenis komunikasi, dan hierarki komunikasinya.
2) Jaring Komunikasi Sandi (JKS)
Identifikasi JKS meliputi identifikasi terhadap:
(a) PD yang akan terhubung dalam JKS termasuk didalamnya unit kerja dalam PD yang akan mengoperasikan peralatansandi.
(b) Pejabat Pemerintah Kota yang akan terhubung dalam JKS termasuk didalamnya penentuan hierarkikomunikasi.
(c) Infrastruktur komunikasi yang ada di Pemerintah Kota.
b) alat pendukung utama (APU) Persandian
Identifikasi APU Persandian meliputi identifikasi kebutuhan terhadap perangkat yang mendukung penyelenggaran 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) Mengidentifikasi pembiayaan
Identifikasi pembiayaan meliputi identifikasi anggaran yang dibutuhkan oleh penyelenggara persandian di Pemerintah Kota Lubuklinggau dalam periode waktu satu tahun anggaran.
4) Menetapkan hasil identifikasi dan analisis pola hubungan komunikasi sandi melalui Peraturan Kepala Dinas, yang berisi entitas yang terhubung maupun yang tidak terhubung dalam pola hubungan komunikasi tersebut, serta tugas dan tanggung jawab masing-masing entitas terhadap fasilitas dan layanan yang diberikan.

3. Pengelolaan Dan Perlindungan Informasi

Pengelolaan dan perlindungan informasi di Pemerintah Kota 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 InformasiBerklasifikasi
            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 (*logicalsecurity*).
            1.2. Perangkat atau peralatan yang digunakan untuk membuat dan/atau mengkomunikasikan Informasi Berklasifikasi harus milik dinas dan hanya dimanfaatkan untuk kepentingandinas.
            1.3. Konsep Informasi Berklasifikasi tidak boleh disimpan dan harusdihancurkan secara fisik maupun lojik (*logical security*).
            1.4. Dokumen elektronik berklasifikasi yang sudah disahkan disimpandalam bentuk yang tidak dapat diubah/dimodifikasi (*readonly*).
            1.5. Penggandaan dan/atau perubahan Informasi Berklasifikasi dilakukanharus dengan ijin dari Pemilik Informasi atau PengelolaInformasi.

        b) Pemberian Label Informasi Berklasifikasi

        Informasi Berklasifikasi harus diberi label sesuai dengan tingkat klasifikasi informasinya, bergantung pada bentuk dan media penyimpanannya.

            1.1. Dokumen cetak: Label ditulis dengan cap (tidak diketik) berwarna merah pada bagian atas dan bawah setiap halaman dokumen. Jika dokumen tersebut disalin, cap label pada salinan harus menggunakan warna yang sama dengan warna cap pada dokumenasli.
            1.2. Surat elektronik: Label ditulis pada baris *subject* pada*header* surat elektronik.
            1.3. Dokumen Elektronik: Label diberikan dalam metadata dokumen. Dokumen Elektronik yang akan dicetak atau disimpan dalam format .pdf dapat diberikan label pada *header* atau *footer* atau menggunakan *watermark* di setiap halaman termasuk *cover*.
            1.4. *Database* dan aplikasi bisnis: Label diberikan dalam metadatasistem/aplikasi.
            1.5. Media lain, seperti: *cd, dvd, magnetic tape, harddrive*, dsb. Label ditempelkan pada fisik media penyimpanan dan terlihat dengan jelas, kemudian media penyimpanan tersebut dibungkus lagi tanpa diberi label. Label tersebut juga harus

muncul saat informasi yang tersimpan di dalamnya diakses.

c) Pengiriman Informasi Berklasifikasi

1.1. Pengiriman dokumen elektronik berklasifikasi

i Dokumen Elektronik berklasifikasi dikirimkan dengan menggunakan teknik kriptografi dan melalui saluran komunikasi yang aman. Contoh Dokumen elektronik dienkripsi dengan aplikasi enkripsi yang direkomendasikan olehBSSN.

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 kepadapengirim.

1.2. Pengiriman dokumen cetak berklasifikasi

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

ii Dokumen cetak berklasifikasi dimasukkan ke dalam dua amplop. Amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (kilat, sangat segera, segera, dan biasa). Selanjutnya amplop pertama dimasukkan ke dalam amplop kedua dengan tanda-tanda yang sama kecuali cap klasifikasi.

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

d) Penyimpanan Informasi Berklasifikasi

1.1. Penyimpanan Dokumen Elektronik berklasifikasi

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

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

iii Prosedur pengamanan Dokumen Elektronik berklasifikasi harus sesuai denganklasifikasinya.

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

v Penyimpanan Dokumen Elektronik berklasifikasi harus diduplikasi (*backup*) secaraberkala.

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

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

muncul saat informasi yang tersimpan di dalamnya diakses.

c) Pengiriman Informasi Berklasifikasi

1.1. Pengiriman dokumen elektronik berklasifikasi

i Dokumen Elektronik berklasifikasi dikirimkan dengan menggunakan teknik kriptografi dan melalui saluran komunikasi yang aman. Contoh Dokumen elektronik dienkripsi dengan aplikasi enkripsi yang direkomendasikan olehBSSN.

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 kepadapengirim.

1.2. Pengiriman dokumen cetak berklasifikasi

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

ii Dokumen cetak berklasifikasi dimasukkan ke dalam dua amplop. Amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (kilat, sangat segera, segera, dan biasa). Selanjutnya amplop pertama dimasukkan ke dalam amplop kedua dengan tanda-tanda yang sama kecuali cap klasifikasi.

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

d) Penyimpanan Informasi Berklasifikasi

1.1. Penyimpanan Dokumen Elektronik berklasifikasi

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

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

iii Prosedur pengamanan Dokumen Elektronik berklasifikasi harus sesuai denganklasifikasinya.

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

v. Penyimpanan Dokumen Elektronik berklasifikasi harus diduplikasi (*backup*) secaraberkala.

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

1.2. Penyimpanan dokumen cetak berklasifikasi

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

pandangan orang lain.

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

e) Pemusnahan Informasi Berklasifikasi

1.1. Pemusnahan Dokumen Elektronik Berklasifikasi

i. Melakukan penilaian bahwa informasi sudah tidak lagi digunakan

ii. Adanya usulan pemusnahan oleh pejabatberwenang

iii. Pengelola Informasi memberikan persetujuan untuk melakukanpemusnahan

iv. Penerbitan Surat KeputusanPemusnahan

v. Melakukan pemusnahan dengan aplikasi yang aman dan sudah direkomendasikan olehBSSN

vi. Menandatangani BASTPemusnahan

1.2. Pemusnahan Dokumen Cetak Berklasifikasi

i. Melakukan penilaian bahwa informasi sudah tidak lagi digunakan

ii. Adanya usulan pemusnahan oleh pejabatberwenang

iii. Pengelola Informasi memberikan persetujuan untuk melakukanpemusnahan

iv. Penerbitan Surat KeputusanPemusnahan

v. Melakukan pemusnahan secara fisik sesuai dengan ketentuan yangberlaku

2) Menandatangani BAST Pemusnahan. Perlindungan informasi publik yang dikecualikan/informasi berklasifikasi meliputi:

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

(b) Perlindungan administrasi

Pelaksanaan perlindungan administrasi dilakukan dengan berpedoman pada kebijakan, standar, dan prosedur operasional pengamanan informasi publik yang dikecualikan/informasi berklasifikasi.

(c) Perlindungan lojik (*logicalsecurity*)

(1) Perlindungan lojik (logical security) menggunakan teknik kriptografi dan steganografi untuk memenuhi aspek: kerahasiaan, keutuhan, otentikasi, dan nirpenyangkalan.

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

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

1.1. Pemasangan firewall pada jaringan data yang terhubung diserver,

1.2. Pemasangan *ToolsDetection*, Pemasanganantivirus,

1.3. Pengamanan/ pemanfaatan *user/password*,

1.4. Aplikasi keamanan lain yang telah teruji kehandalannya.

(4) Dalam rangka pencegahan dan penanggulangan perlindungan

logic, Bidang Persandian bekerjasama dengan Unit Pengelola Teknologi Informasi di lingkup Pemerintah Kota 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 antipenyangkalan.

(e) Penyelenggaraan Jaring Komunikasi Sandi (JKS) untuk pengamanan informasiberklasifikasi.

(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 dayamanusia
Perencanaan kebutuhan sumber daya manusia yang bertugas di bidang persandian disusun dengan memperhatikan jumlah dan kompetensi yang dibutuhkan. Dalam kegiatan perencanaan ini, Bidang yang menangani persandian dapat menyusun Analisis Beban Kerja dan Formasi Jabatan Fungsional Sandiman serta mengajukan usulan kebutuhan tersebut kepada Badan Kepegawaian dan Pembinaan Sumber Daya Manusia.

(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 Kota dapat difasilitasi oleh BSSN dengan mengajukan permohonan kepada BSSN sesuai hasil analisiskebutuhan.

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

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

(2) Pengelolaan APU Persandian

a) Pengelolaan terhadap APU Persandian meliputi: 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 dengan memperhatikan syarat-syarat keamanan antara lain:

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

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

c) Pemeliharaan

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

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

(a) *Jamming*

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

2) RuangLingkup

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

b) Pelaksana adalah seluruh pejabat/pegawai pada Bidang Persandian di Dinas Kominfo 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 Kota Lubuklinggau.

d) Pengguna pelayanan adalah Pejabat Daerah dan Pejabat Lainnya.

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

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

3) Prosedur Layanan

a) Kegiatan *Jamming* dilakukan dan/atau disesuaikan dengan kebutuhan rapat-rapat dan berdasarkan permintaan;

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 Kota. Kegiatan ini berlangsung sampai

dengan rapat tersebut selesai.

(b) Kontra Penginderaan/*sterillisasi*

1) Kontra Penginderaan dilakukan terhadap ruangan-ruangan yang digunakan oleh Pimpinan Pemerintah Daerah untuk penyampaian informasi berklasifikasi.
2) Kegiatan Kontra Penginderaan dilakukan melalui pemeriksaan fisik ruangan dengan memperhatikan barang-barang di dalam ruangan yang berpotensi menjadi peralatan *surveillance*.
3) RuangLingkup
   a) Unit pelayanan yang menyelenggarakan pengkoordinasian Kontra Penginderaan terhadap Pejabat Daerah dan pejabat lainnya adalah Bidang Persandian di Dinas Kominfo.
   b) Pelaksana kegiatan kontra pengindraan adalah Tim Kontra Pengindraan dari BSSN dan/atau Tim Kontra Pengindraan Dinas Kominfo Provinsi Sumatera Selatan yang mempunyai kualifikasi sandi.
   c) Penanggung jawab pelayanan adalah Kepala Dinas Kominfo
   d) Pengguna pelayanan adalah Pejabat Daerah dan Pejabat Lainnya.
   e) Keluaran (*output)* pelayanan adalah dokumen dan produk naskah dinas kegiatan Kontra Penginderaan.
   f) Kemanfaatan (*outcome)* pelayanan adalah terselenggaranya kegiatan Pejabat Daerah dan Pejabat lainnya dengan aman dari ancaman non fisik berupa penyadapan jaringan komunikasi dengan memanfaatkan kemajuan teknologi yang berkembang saat ini dan masa yang akan datang.
4) Prosedur Layanan
   a) Kegiatan Kontra Penginderaan dilakukan dengan 2 (dua) cara yaitu:
      i. Secara periodik yaitu 2 kali dalam setahun,dan
      ii. Permintaan daripejabat
   b) Kegiatan Kontra Penginderaan tersebut dilakukan dengan terlebih dahulu mengajukan ijin dari pejabat pemilik ruang kerja atau rumah dinas.
   c) Mengajukan surat permohonan fasilitasi kegiatan Kontra Pengindraan ke BSSN/Dinas Kominfo Provinsi Sumatera Selatan.
   d) Untuk waktu pelaksanaan kegiatan disesuaikan dengan permintaan pimpinan dan kegiatan bersifat tertutup (closed).
   e) Hasil pelaksanaan kegiatan, berupa dokumen laporan dan Berita Acara Pelaksanaan Kegiatan disampaikan kepada Dinas untuk ditindaklanjuti.
   f) Setelah melakukan analisis yang mendalam Tim melaporkan hasil dari kegiatan sterilisasi penyadapan itu kepada Pejabat pemilik ruangan atau Rumah dinas dan melakukan evaluasi mengenai kekurangan, kendala, hambatan dan rintangan yang dialami Tim pada tempat kegiatan sterilisasi penyadapan. Tim selanjutnya memberikan solusi pemecahan masalah yang ada untuk memperbaiki agar dikemudian hari bisa menghindari dari resiko penyadapan.

(c) Pelaksanaan Kegiatan Assessment Keamanan Sistem Informasi

1) Kegiatan Assessment Keamanan Sistem Informasi dilakukan dengan melakukan pemeriksaan terhadap ada atau tidaknya celah kerawananan pada Sistem Informasi.
2) Pemerintah Kota Lubuklinggau melakukan kegiatan *Assessment* Keamanan Sistem Informasi setelah berkoordinasi dan mengajukan permohonan *Assessment* Keamanan Sistem Informasi kepada BSSN.
3) RuangLingkup
   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 Kota adalah Bidang Persandian Dinas Kominfo.
   b) Pelaksana adalah seluruh pejabat/pegawai pada Bidang Persandian di Dinas Kominfodan 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 Kota.
   c) Penanggung jawab pelayanan adalah Kepala Dinas Kominfo.
   d) Sasaran yang hendak dicapai adalah terhindarnya data/informasi, aplikasi, database, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Kota dari ancaman dan kerawanan yang mungkin timbul.
   e) Pengguna pelayanan adalah Seluruh PD di Kota.
   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 Kota Lubuklinggau dari ancaman yang ditimbulkan oleh pemanfaatan teknologi Telekomunikasi dan Elektronika berupa *phising, virus, malicious malware* dan lainnya.

4) Prosedur Layanan
   a) Kegiatan *Assessment* Keamanan Sistem Informasi dilakukan terhadap Organisasi PD (OPD) di Pemerintah Kota Lubuklinggau yang mengajukanpermintaan
   b) Setelah terdapat permintaan, pelaksanan kegiatan *Assessment* Keamanan Sistem Informasi akan dikoordinasikan dengan pihak BSSN untukpenjadwalan.
   c) Setelah mendapatkan penjadwalan, Tim akan melaksanakan kegiatan *Assessment* Keamanan Sistem Informasi dengan skenario yang telah disepakatibersama.
   d) Tim menyusun laporan hasil dan rekomendasi darikegiatan*Assessment* Keamanan Sistem Informasi.

(d) Layanan Sertifikat Elektronik
1) Pelaksanaan kegiatan layanan sertifikat elektronik dapat dilakukan oleh Pemerintah Kota Lubuklinggau 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 sertifikatelektronik
   b) Pengembangan aplikasi pendukung penggunaan sertifikat elektronik
   c) Bimbingan teknis dan sosialisasi terkait penggunaan sertifikat elektronik
   d) Pengawasan dan evaluasi penggunaan sertifikat elektronik.

3) Ruang Lingkup
   a) Unit pelayanan yang menyelenggarakan pengkoordinasian kegiatan layanan sertifikat elektronik terhadap data/informasi, aplikasi, data base, server, dan pengolah data lainnya yang dimiliki oleh Pemerintah Kota Lubuklinggau adalah Bidang Persandian di Dinas Komunikasi Informatika Kota Lubuklinggau;
   b) Pejabat Struktural/sandiman yang ditunjuk Kepala Dinas sebagai verifikator sertifikat elektronik
   c) Penanggung jawab pelayanan adalah Kepala Dinas Kominfo;
   d) Sasaran yang hendak dicapai adalah terhindarnya data/informasi, aplikasi, *database, server,* dan pengolah data lainnya yang dimiliki oleh Pemerintah Kabupaten Buleleng dari ancaman dan kerawanan yang mungkintimbul;
   e) Pengguna pelayanan adalah Seluruh PD di Pemerintah Kota;
   f) Keluaran *(output)* laporan jumlah PD yang memanfaatkan Layanan Sertifikat Elektronik.
   g) Kemanfaatan *(outcome)* pelayanan adalah terselenggaranya kegiatan layanan sertifikat elektronik terhadap data/informasi, aplikasi, *database, server,* dan pengolah data lainnya yang dimiliki oleh Pemerintah Kota 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) PD yang akan menerbitkan Sertifikat Elektronik mengajukan surat permohonan kepada kepala dinas dengan melampirkan persyaratan:
      a.1. surat elektronik penerbitan Sertifikat Elektronik dari atasan;
      a.2. scan dan/atau fotocopy KTP;
      a.3. surat keputusan jabatan.
   b) Verifikator mengajukan penerbitan Sertifikat Elektronik ke Balai Sertifikat Elektronik (Bsre) untuk verifikasi.
   c) Bsre menerbitkan sertifikat elektronik, Verifikator menyerahkan Sertifikat Elektronik kepada PD yang mengajukan TTE dengan Berita Acara Serah Terima.
   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

berkerjasama dengan BSSN sebagai instansi pembina dimana infrastruktur SOC pada Pemerintah Kota Lubuklinggau dapat terhubung dengan BSSN, sehingga kegiatan akan berlangsung responsif.

6. Pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh perangkatdaerah

   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 Kota harus terlapor kepada Pemerintah Provinsi Sumatera Selatan agardapatditindaklanjutidenganrencanaperbaikansebagaibahanmasukan bagi penyusunan kebijakan, program, dan kegiatan penyelenggaraan Persandian tahun berikutnya.
   b. Pengawasan dan evaluasi penyelenggaraan Persandian yang dilaksanakanmeliputi:
      1) Pengawasan dan evaluasi yang bersifat rutin dan insidentil sebagaiberikut:
         a) Pemantauan penggunaan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan Persandian lainnya.
         b) Melaksanakan kebijakan manajemen risiko penyelenggaraan Persandian di Pemerintah Kota. Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
            (1) Pemerintah Kota melaksanakan kebijakan manajemen risiko yang ditetapkan oleh BSSN.
            (2) Dinas Kominfo sebagai penyelenggara Persandian melaksanakan fungsi koordinasi pelaksanaan kebijakan manajemen risiko penyelenggaraan Persandian.
            (3) Dalam hal terdapat potensi insiden dan/atau terjadinya insiden penyelenggaraan Persandian dan keamanan informasi, Pemerintah Kota 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 sebagai berikut:
         a) Pengukuran tingkat pemanfaatan layanan Persandian oleh Pemerintah Provinsi Sumatera Selatan.

            Dalam melaksanakan pengukuran tingkat pemanfaatan layanan Persandian perlu memperhatikan hal-hal sebagai berikut:
            (1) Jumlah PD yang memanfaatkan analisis kebutuhan penyelenggaraan persandian untuk pengamananInformasi.
            (2) Jumlah PD yang melaksanakan pengelolaan dan perlindunganInformasi.
            (3) Jumlah PD yang memanfaatkan layanan penyelenggaraan operasional dukungan Persandian untuk pengamananInformasi.
         b) Penilaian mandiri (*self assessment*) terhadap penyelenggaraan Persandian pada Pemerintah Kota.

            Kegiatan pengawasan dan evaluasi ini dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
            (1) Penilaian mandiri (self assessment) merupakan pengukuran

penyelenggaraan Persandian mandiri yang dilaksanakan dengan menggunakan Instrumen Pengukuran Penyelenggaraan Persandian yang telah ditetapkan oleh BSSN.

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

(3) Penilaian mandiri(*self assessment*) dilakukan oleh SDM yang berkualifikasi sandi, menguasai teknikpemeriksaan(audit), dan telah mengikuti bimbingan teknis penggunaan Instrumen Pengukuran Penyelenggaraan Persandian yang ditetapkan oleh BSSN.

(4) Dalam hal PD penyelenggara Persandian memiliki keterbatasan SDM sesuai butir 3 di atas, maka harus berkonsultasi dengan BSSN untuk ditentukan kebijakan lebih lanjut.

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

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

c) Pengukuran tingkat kepuasan PD terhadap layanan Persandian yang dikelola oleh Dinas Kominfo penyelenggara Persandian.

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

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

(2) Pemerintah Kota dapat berkonsultasi kepada BSSN terkait penggunaan instrumen pengukuran kepuasan PD terhadap layananPersandian.

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

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

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

(2) Mengkoordinasikan penyiapan bahan dan melaksanakan penyusunanLP2T.

(3) LP2T Pemerintah Kota disampaikan kepadaPemerintah Provinsi Sumatera Selatan.

7. Koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

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

8. Sarana dan Prasarana OperasionalPersandian

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

1) Tempat kegiatan sandi terdiri dari:
   a. ruang tamu
   b. ruang administrasi
   c. ruang kepala kamar sandi
   d. ruang kamar sandi; dan
   e. toilet.

   Sarana dan Prasarana:
   a. internet
   b. telepon
   c. komputer/PC
   d. brankas;dan
   e. printer
2) Mempunyai peralatan sandi yang disediakan atau direkomendasikan oleh Badan Siber dan Sandi Negara
3) Jaringan internet dan jaringan komunikasi
4) Peralatan pendukung lainnya yang diperlukan

WALI KOTA LUBUKLINGGAU

H. S. N. PRANA PUTRA SOHE