BUPATI BARITO UTARA
PROVINSI KALIMANTAN TENGAH

PERATURAN BUPATI BARITO UTARA
NOMOR 26 TAHUN 2020

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA
BUPATI BARITO 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 sebagaimana telah beberapa kali diubah, terakhir 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 Kabupaten/kota menjadi kewenangan Pemerintah Daerah Kabupaten/kota;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian untuk Pengamanan Informasi;

Mengingat :

1. Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1953, Nomor 9) sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 72, Tambahan Lembaran Negara Republik Indonesia Nomor 1820), sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 8 Tahun 1965 tentang Pembentukan Daerah Tingkat II Tanah Laut, Daerah Tingkat II Tapin dan Daerah Tingkat II Tabalong dengan Mengubah Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat

Nomor 3 Tahun 1953 tentang Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 51, Tambahan Lembaran Negara Republik Indonesia Nomor 2756);

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 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 2011 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);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
5. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
6. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
7. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100);
8. Peraturan Menteri Komunikasi dan Informatika Nomor 41 Tahun 2017 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi (TIK) Nasional;
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 18 Tahun 2019 tentang Jabatan Fungsional Sandiman;
10. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaring Komunikasi Sandi (Berita Negara Republik Indonesia Tahun 2010 Nomor 292);

11. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah (Berita Negara Republik Indonesia Tahun 2012 Nomor 808);
12. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik (Berita Negara Republik Indonesia Tahun 2017 Nomor 907);
13. 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);
14. Peraturan Komisi Informasi Nomor 1 Tahun 2017 tentang Pengklasifikasian Informasi Publik (Berita Negara Republik Indonesia Tahun 2017 Nomor 429);
15. Peraturan Daerah Kabupaten Barito Utara Nomor 2 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Barito Utara (Lembaran Daerah Kabupaten Barito Utara Tahun 2016 Nomor 7, Tambahan Lembaran Daerah Kabupaten Barito Utara Nomo 6);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Provinsi adalah Provinsi Kalimantan Tengah.
2. Kabupaten adalah Kabupaten Barito Utara.
3. Pemerintah Kabupaten adalah Pemerintah Kabupaten Barito Utara.
4. Bupati adalah Bupati Barito Utara.
5. Wakil Bupati adalah Wakil Bupati Barito Utara.
6. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dalam penyelenggaraan Pemerintahan Daerah yang terdiri atas sekretariat daerah, sekretariat dewan perwakilan rakyat daerah, dinas daerah dan badan daerah dalam lingkup pemerintah Kabupaten.
7. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah profesi bagi pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang bekerja pada instansi Pemerintah.
8. Pegawai Negeri Sipil yang selanjutnya disingkat PNS adalah warga negara Indonesia yang memenuhi syarat tertentu diangkat sebagai pegawai ASN secara tetap oleh Pejabat Pembina Kepegawaian untuk menduduki jabatan Pemerintahan.

9. 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.
10. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
11. 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 kepentingan publik.
12. Tingkat Kerahasiaan Informasi adalah tingkatan yang ditentukan dan ditetapkan terhadap Informasi Berklasifikasi berdasarkan akibat yang dapat ditimbulkan bila Informasi tersebut diketahui oleh pihak yang tidak berhak mengetahuinya.
13. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
14. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subyek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Balai Sertifikasi Elektronik pada Badan Siber dan Sandi Negara.
15. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memilki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
16. Kriptografis adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan Informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.
17. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara Otoritas Sertifikat Digital (OSD) Badan Siber dan Sandi Negara yang berada di bawah dan bertanggung jawab kepada Kepala Lembaga Sandi Negara.

BAB II
MAKSUD DAN TUJUAN

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai acuan bagi Pemerintah Kabupaten dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi di Pemerintah Kabupaten.

Pasal 3

Peraturan Bupati ini bertujuan:

a. menciptakan keamanan informasi di Kabupaten sesuai dengan Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah Provinsi dan Kabupaten/Kota yang telah dijelaskan pada Peraturan Badan Siber dan Sandi Negara;
b. menciptakan harmonisasi dalam bidang Persandian di Pemerintah Kabupaten;
c. membantu PD dalam melaksanakan tata cara penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Kabupaten
d. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi; dan
e. meningkatkan kinerja PD yang menangani Urusan Pemerintahan Bidang Persandian untuk pengamanan informasi.

BAB III
PENYELENGGARAAN PERSANDIAN

Pasal 4

Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintahan Kabupaten meliputi:

a. pengelolaan dan perlindungan informasi berklasifikasi dan informasi publik;
b. pengelolaan sumber daya persandian;
c. penyediaan kebutuhan penyelenggaraan persandian untuk pengamanan informasi melalui identifikasi dan analisis pola hubungan komunikasi sandi;
d. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi;
e. pemanfaatan layanan sertifikat elektronik;
f. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh PD; dan
g. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

Pasal 5

Penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Kabupaten terdiri atas Bupati dibantu oleh PD pelaksana Urusan Pemerintahan Bidang Persandian.

Pasal 6

(1) Bupati memimpin dan bertanggung jawab atas penyelenggaraan Persandian yang menjadi kewenangan Kabupaten.
(2) PD pelaksana Urusan Pemerintahan Bidang Persandian bertanggung jawab atas kinerja pelaksanaan Urusan Pemerintahan bidang Persandian sesuai dengan tugas dan fungsinya.

Pasal 7

(1) PD pelaksana Urusan Pemerintahan bidang Persandian menyusun perencanaan penyelenggaraan Persandian sesuai dengan kewenangannya.
(2) Perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam perencanaan pembangunan daerah.
(3) Perencanaan pembangunan daerah sebagaimana dimaksud pada ayat (2) merupakan bagian integral dari sistem perencanaan pembangunan nasional dan dituangkan dalam dokumen perencanaan pembangunan daerah.
(4) Dokumen perencanaan pembangunan daerah sebagaimana dimaksud pada ayat (3) berupa Rencana Pembangunan Jangka Panjang Daerah, Rencana Pembangunan Jangka Menengah Daerah dan Rencana Kerja Pemerintah Daerah Kabupaten.

Pasal 8

(1) Dalam rangka menjabarkan Rencana Pembangunan Jangka Menengah Daerah sebagaimana dimaksud dalam Pasal 7 ayat (4), PD pelaksana Urusan Pemerintahan Bidang Persandian menyusun rencana strategis PD yang memuat tujuan, sasaran, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintahan Kabupaten.
(2) Dalam rangka menjabarkan Rencana Kerja Pemerintah Daerah Kabupaten sebagaimana dimaksud dalam Pasal 7 ayat (4), PD pelaksana Urusan Pemerintahan Bidang Persandian menyusun rencana kerja PD yang memuat program, kegiatan, lokasi dan kelompok sasaran berdasarkan layanan urusan pemerintahan bidang Persandian, disertai indikator kinerja program dan kegiatan, serta penganggaran penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Kabupaten.

BAB IV
PENGELOLAAN DAN PERLINDUNGAN INFORMASI

Bagian Kesatu
Penyediaan Layanan Keamanan Informasi

Pasal 9

(1) Penyelenggaraan operasional dukungan persandian untuk pengamanan informasi sebagaimana dimaksud dalam Pasal 4 huruf d dilaksanakan oleh PD.
(2) Penyelenggaraan operasional dukungan persandian untuk pengamanan informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
    a. Bupati dan Wakil Bupati;
    b. PD;
    c. ASN pada pemerintah kabupaten; dan
    d. pihak lainnya.

Pasal 10

Jenis Layanan Keamanan Informasi 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 JKS;
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 kabupaten 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. forensik digital;
m. perlindungan Informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan pemerintah daerah melalui kegiatan kontra penginderaan;
o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
p. jenis Layanan Keamanan Informasi lainnya.

Bagian Kedua
Pengelolaan Informasi Berklasifikasi

Pasal 11

(1) Pengelolaan Informasi Berklasifikasi di lingkungan Pemerintah Kabupaten harus menggunakan pengamanan Informasi.
(2) Pengelolaan Informasi Berklasifikasi sebagaimana dimaksud pada ayat (1) terdiri dari:
    a. pembuatan;
    b. pemberian label;
    c. pengiriman dan penerimaan; dan
    d. penyimpanan.

Paragraf 1
Pembuatan Informasi Berklasifikasi

Pasal 12

(1) Pembuatan Informasi Berklasifikasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dilakukan oleh pemilik Informasi atau pengelola Informasi.
(2) Pembuatan Informasi Berklasifikasi harus menggunakan sarana dan prasarana milik PD yang hanya dimanfaatkan untuk kepentingan dinas.
(3) Sarana dan prasarana sebagaimana dimaksud ayat (2) harus memiliki kriteria aman secara fisik, administrasi, dan lojik.
(4) Konsep Informasi Berklasifikasi tidak boleh disimpan dan harus dihancurkan baik dalam bentuk tercetak maupun elektronik.
(5) Dokumen elektronik yang berisi Informasi Berklasifikasi yang telah disahkan harus disimpan dalam bentuk yang tidak bisa diubah atau dimodifikasi dengan menggunakan Tanda Tangan Elektronik.
(6) Penggandaan dan/atau perubahan Informasi Berklasifikasi harus mendapat persetujuan dari pemilik Informasi.

Paragraf 2
Pemberian Label Informasi Berklasifikasi

Pasal 13

(1) Pemberian label sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b dilakukan pada Informasi Berklasifikasi yang telah disahkan dan media penyimpanannya sesuai dengan Tingkat Kerahasiaan Informasinya.
(2) Tingkat Kerahasiaan Informasi sebagaimana dimaksud pada ayat (1) di suatu PD harus diperlakukan sama tingkat kerahasiaannya oleh PD lainnya.

(3) Tingkat Kerahasiaan Informasi sebagaimana dimaksud pada ayat (1) diklasifikasikan dalam 3 (tiga) tingkatan, yaitu:
a. terbatas;
b. rahasia; dan
c. sangat rahasia.

Pasal 14

(1) Label sebagaimana dimaksud dalam Pasal 13 diberikan dengan ketentuan:
a. dokumen cetak:
1. label ditulis dengan cap berwarna merah pada bagian atas dan bawah setiap halaman; dan
2. dalam hal dokumen cetak sebagaimana dimaksud pada huruf a disalin, cap label pada salinan harus menggunakan warna yang sama dengan warna cap pada dokumen asli.
b. label ditulis pada baris subjek pada header surat elektronik;
c. label diberikan dalam metadata Dokumen Elektronik pada *header* atau *footer* atau menggunakan *watermark* di setiap halaman termasuk *cover*;
d. label diberikan dalam metadata sistem/aplikasi pada basis data dan aplikasi; dan/atau
e. media penyimpanan lain:
1. label ditempelkan pada fisik media penyimpanan;
2. label terlihat dengan jelas;
3. media penyimpanan yang telah diberi label dibungkus sekali lagi tanpa diberi label; dan
4. label harus muncul saat Informasi yang tersimpan di dalamnya diakses.

(2) Format label sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Paragraf 3
Pengiriman dan Penerimaan Informasi Berklasifikasi

Pasal 15

(1) Pengiriman dan penerimaan Dokumen Elektronik yang berisi Informasi Berklasifikasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c harus menggunakan Persandian dan dikirim melalui jalur komunikasi yang aman.

(2) Pengiriman dokumen cetak yang berisi Informasi Berklasifikasi menggunakan pengamanan fisik berlapis dengan memasukkannya ke dalam dua amplop, yaitu:
a. amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan

derajat kecepatan seperti kilat, sangat segera, segera, dan biasa; dan

b. amplop pertama sebagaimana dimaksud pada huruf a dimasukkan ke dalam amplop kedua dengan tanda yang sama kecuali cap klasifikasi.

(3) Pengiriman dokumen cetak yang berisi Informasi Berklasifikasi sebagaimana dimaksud ayat (2) harus tercatat dalam buku ekspedisi sebagai bukti pengiriman atau dibuatkan tanda bukti pengiriman tersendiri.

Paragraf 4
Penyimpanan Informasi Berklasifikasi

Pasal 16

Penyimpanan Informasi Berklasifikasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf d disimpan dalam bentuk Dokumen Elektronik dan/atau dokumen cetak.

Pasal 17

Penyimpanan Informasi Berklasifikasi dalam bentuk Dokumen Elektronik sebagaimana dimaksud dalam Pasal 16 dilakukan dengan ketentuan:

a. diamankan dengan Persandian;
b. lokasi penyimpanan harus dilengkapi kendali akses untuk mencegah risiko kehilangan, kerusakan, dan manipulasi data;
c. tidak boleh disimpan di dalam komputer, perangkat *mobile*, atau media penyimpanan pribadi;
d. melakukan perekaman data (*backup*) secara berkala; dan
e. media penyimpanan dilarang digunakan, dipinjam, atau dibawa keluar ruangan atau keluar kantor tanpa izin pengelola Informasi.

Pasal 18

Penyimpanan Informasi Berklasifikasi dalam bentuk dokumen cetak sebagaimana dimaksud dalam Pasal 16 dilakukan dengan ketentuan:

a. lokasi penyimpanan harus dilengkapi kendali akses untuk mencegah risiko kehilangan dan kerusakan;
b. disimpan dalam brankas yang memiliki kunci kombinasi atau media penyimpanan yang aman; dan
c. diarsip secara khusus dengan tertib dan rapi sesuai prosedur arsip yang berlaku.

Bagian Kedua
Perlindungan Informasi Berklasifikasi

Pasal 19

Perlindungan Informasi Berklasifikasi di lingkungan Pemerintah Kabupaten dan Kabupaten meliputi:

a. perlindungan fisik;
b. perlindungan administrasi; dan
c. perlindungan lojik.

Paragraf 1
Perlindungan Fisik

Pasal 20

(1) Perlindungan fisik sebagaimana dimaksud dalam Pasal 19 huruf a dilakukan untuk melindungi keberadaan dan fungsi sarana fisik komunikasi serta segala kegiatan yang berlangsung di dalamnya dari ancaman dan gangguan seperti pencurian perusakan, dan radiasi gelombang elektromagnetik.
(2) Perlindungan fisik sebagaimana dimaksud dalam Pasal 19 huruf a dilakukan melalui:
    a. kendali akses ruang;
    b. pemasangan teralis;
    c. penggunaan kunci ganda;
    d. pemasangan CCTV; dan/atau
    e. penggunaan ruang TEMPEST.

Paragraf 2
Perlindungan Administrasi

Pasal 21

(1) Perlindungan administrasi sebagaimana dimaksud dalam Pasal 19 huruf b dilakukan untuk mencegah kelalaian dan tindakan indisipliner.
(2) Perlindungan administrasi sebagaimana dimaksud pada ayat (1) dituangkan dalam bentuk peraturan tertulis yang menerangkan kebijakan, standar, dan prosedur operasional dalam pengamanan Informasi Berklasifikasi.

Paragraf 3
Perlindungan Lojik

Pasal 22

(1) Perlindungan lojik sebagaimana dimaksud dalam Pasal 19 huruf c dilakukan dengan menggunakan perlindungan lojik menggunakan teknik Kriptografi dan steganografi untuk memenuhi aspek kerahasiaan, keutuhan, otentikasi, dan nir penyangkalan.
(2) Perlindungan lojik yang menggunakan teknik Kriptografi dan steganografi sebagaimana dimaksud pada ayat (1) harus memenuhi standar dan direkomendasikan oleh Badan Siber dan Sandi Negara.

Bagian Ketiga
Pengelolaan dan Perlindungan Informasi Publik

Pasal 23

(1) Pengelolaan dan perlindungan Informasi
(2) Publik di Pemerintah Kabupaten meliputi:
    a. pengiriman Informasi yang terbuka melalui jaringan yang aman.
    b. pengamanan transaksi elektronik melalui implementasi Sertifikat Elektronik.
(3) Implementasi Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) huruf b bertujuan untuk menjamin keutuhan, autentikasi dan nir-penyangkalan dokumen elektronik.

BAB V
PENGELOLAAN SUMBER DAYA PERSANDIAN

Bagian Kesatu
Pengelolaan Sumber Daya Manusia

Pasal 24

(1) PD pelaksana Urusan Pemerintah Bidang Persandian harus melakukan pengelolaan sumber daya Persandian.
(2) Pengelolaan sumber daya Persandian sebagaimana dimaksud dalam ayat (1), terdiri dari:
    a. pengelolaan sumber daya manusia; dan
    b. pengelolaan sarana dan prasarana.

Pasal 25

Penetapan kebutuhan PNS dalam Jabatan Fungsional Sandiman dihitung berdasarkan beban kerja yang ditentukan dari indikator antara lain:

a. kompleksitas layanan keamanan informasi, keamanan siber, dan persandian yang diselenggarakan; dan
b. tingkat kerawanan dan risiko keamanan informasi, keamanan siber, dan persandian yang dikelola.

Pasal 26

(1) PNS yang menduduki Jabatan Fungsional Sandiman harus memenuhi standar kompetensi sesuai dengan jenjang jabatan.
(2) Standar Kompetensi sebagaimana dimaksud pada ayat (1) meliputi :
    a. kompetensi teknis;
    b. kompetensi manajerial; dan
    c. kompetensi sosial kultural.

Pasal 27

(1) Untuk meningkatkan kompetensi dan profesionalisme Sandiman diikutsertakan pada pelatihan.

(2) Pelatihan yang diberikan bagi Sandiman sebagaimana dimaksud pada ayat (1) disesuaikan dengan hasil analisis kebutuhan pelatihan dan penilaian kinerja.
(3) Pelatihan yang diberikan kepada Sandiman sebagaimana dimaksud pada ayat (1) antara lain dalam bentuk:
    a. pelatihan fungsional; dan
    b. pelatihan teknis bidang keamanan informasi, keamanan siber, dan/atau persandian.
(4) Selain pemberian pelatihan sebagaimana dimaksud pada ayat (3) Sandiman dapat mengembangkan kompetensinya melalui program pengembangan kompetensi lainnya.
(5) Program pengembangan kompetensi sebagaimana dimaksud pada ayat (4) meliputi:
    a. mempertahankan kompetensi sebagai Sandiman (*maintain rating*);
    b. seminar;
    c. lokakarya (*workshop*); atau
    d. konferensi.
(6) Ketentuan mengenai pelatihan dan pengembangan kompetensi serta pedoman penyusunan analisis kebutuhan pelatihan fungsional Sandiman sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur oleh Instansi Pembina.

Pasal 28

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf a meliputi perencanaan dan pengembangan sumber daya manusia.
(2) Dalam hal pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1), Pemerintah Kabupaten memberikan kompensasi atas tanggung jawab dalam melaksanakan tugas di bidang Persandian untuk pengamanan Informasi.
(3) Kompensasi sebagaimana dimaksud pada ayat (2) berupa:
    a. diklat Sandiman untuk peningkatan Sumber Daya Manusia pada Bidang Persandian;
    b. pemberian tunjangan; dan
    c. pengusulan pemberian tanda penghargaan bidang Persandian.
(4) Tunjangan sebagaimana dimaksud pada ayat (3) huruf b meliputi Tunjangan Pengamanan Persandian dan Tunjangan Jabatan Fungsional Sandiman.
(5) Kompensasi sebagaimana dimaksud pada ayat (3) diberikan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 29

Perencanaan sumber daya manusia sebagaimana dimaksud dalam Pasal 28 ayat (1) disusun dengan ketentuan:
a. memperhatikan jumlah dan kompetensi yang dibutuhkan sesuai dengan hasil analisis beban kerja serta formasi jabatan;

b. memperhatikan standar kompetensi yang telah ditetapkan oleh Badan Siber dan Sandi Negara; dan
c. mengusulkan kebutuhan sumber daya manusia kepada Badan Kepegawaian.

Pasal 30

(1) Pengembangan sumber daya manusia sebagaimana dimaksud dalam Pasal 28 ayat (1) dilakukan melalui:
    a. pendidikan dan pelatihan Fungsional Sandiman;
    b. pendidikan dan pelatihan teknis sandi;
    c. bimbingan teknis; dan
    d. kegiatan pengembangan kompetensi lain yang terkait dengan Persandian dan teknologi informasi serta bidang ilmu lainnya yang dibutuhkan.
(2) Pengembangan sumber daya manusia sebagaimana dimaksud pada ayat (1) merupakan pengembangan sumber daya manusia yang terkait dengan ilmu Persandian dan teknologi Informasi serta bidang ilmu lainnya yang dibutuhkan.

Pasal 31

Sumber daya manusia yang sudah tidak melaksanakan tugas pada PD pelaksana Urusan Pemerintah Bidang Persandian harus disesuaikan kewenangannya, yaitu:
a. pencabutan atau pemutusan hak akses terhadap Informasi dan fasilitas pemroses Informasi Berklasifikasi; dan
b. pelaksanaan prosedur pengamanan (serah terima) materiil sandi.

Bagian Kedua
Pengelolaan Sarana dan Prasarana

Pasal 32

(1) Pengelolaan sarana dan prasarana Persandian sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf b meliputi:
    a. materiil sandi;
    b. tempat kegiatan sandi; dan
    c. alat pendukung utama (APU) Persandian.
(2) Pengelolaan sarana dan prasarana Persandian dilaksanakan oleh Aparatur Sipil Negara Pemerintah Kabupaten yang berada pada bidang atau seksi penyelenggara Persandian pada PD pelaksana Urusan Pemerintahan Bidang Persandian.
(3) Ketentuan mengenai pengelolaan sarana dan prasarana mengacu pada Peraturan Kepala Badan Siber dan Sandi Negara.

Pasal 33

Pengelolaan materiil sandi yang dilaksanakan oleh Pemerintah Kabupaten sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf a yaitu pengelolaan peralatan sandi.

Pasal 34

Pengelolaan peralatan sandi yang dilaksanakan oleh Pemerintah Kabupaten sebagaimana dimaksud dalam Pasal 33 adalah:

a. perencanaan kebutuhan;
b. penggunaan;
c. pemeliharaan;
d. perbaikan;
e. pendistribusian; dan
f. pengawasan dan pengendalian.

Bagian Ketiga
Perencanaan Kebutuhan Peralatan Sandi

Pasal 35

(1) Pemerintah Kabupaten merumuskan rencana kebutuhan peralatan sandi dan menetapkannya sebagai peralatan sandi kebutuhan Pemerintah Kabupaten.
(2) Perumusan rencana kebutuhan peralatan sandi harus bersadarkan pada peralatan sandi yang telah direkomendasikan oleh Badan Siber dan Sandi Negara.
(3) Hasil penetapan peralatan sandi diajukan Pemerintah Kabupaten kepada Badan Siber dan Sandi Negara untuk permohonan pemenuhan peralatan sandi kebutuhan Pemerintah Kabupaten.

Bagian Keempat
Penggunaan Peralatan Sandi

Pasal 36

(1) Peralatan sandi digunakan untuk kepentingan pengamanan Informasi.
(2) Penggunaan peralatan sandi dilaksanakan menurut peraturan perundang-undangan.

Bagian Kelima
Pemeliharaan Peralatan Sandi

Pasal 37

(1) Pemeliharaan peralatan sandi dilakukan berdasarkan prinsip kehati-hatian dan ketepatan.
(2) Pemeliharaan peralatan sandi yang dilakukan Pemerintah Kabupaten mencakup:
    a. memastikan peralatan sandi bebas dari debu/kotoran atau benda lain yang memicu gangguan operasional peralatan sandi;

b. menjaga ketersediaan dan kestabilan arus listrik sesuai persyaratan pada peralatan sandi;
c. menjaga dan memonitor ketersediaan koneksi saluran telekomunikasi pada peralatan sandi;
d. memastikan peralatan sandi dapat berfungsi sebagaimana mestinya;
e. menjaga kestabilan suhu ruangan tempat peletakkan Peralatan sandi;
f. meletakkan peralatan sandi pada tempat yang aman dari kemungkinan bencana, pencurian, dan kehilangan.
g. memastikan kelengkapan perangkat; dan
h. memastikan kelengkapan dokumen serah terima barang, berita acara serah terima dan/atau penarikan.

(3) Kegiatan pemasangan kunci sistem sandi ke dalam peralatan sandi harus dilakukan oleh Aparatur Sipil Negara berkualifikasi sandi yang bertugas secara penuh di bidang persandian.

(4) Kunci sistem sandi yang diterima Pemerintah Kabupaten tidak boleh diubah atau digandakan.

(5) Kunci sistem sandi harus disimpan pada tempat yang aman dan kuat dalam brankas atau *strong room* atau lemari besi dengan perkuatan kunci kombinasi.

(6) Jangka waktu penyimpanan kunci sistem sandi dilakukan sampai dengan pelaksanaan pemusnahan.

(7) Pemeliharaan dan perawatan kunci sistem sandi merupakan kegiatan merawat kunci sistem sandi agar mutu kunci sistem sandi tetap terjaga dan/atau tidak mengalami kerusakan.

Bagian Keenam
Perbaikan Peralatan Sandi

Pasal 38

(1) Kategori perbaikan peralatan sandi meliputi:
a. perbaikan umum; dan
b. perbaikan khusus.

(2) Perbaikan umum sebagaimana dimaksud pada ayat (1) huruf a, merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis.

(3) Perbaikan khusus sebagaimana dimaksud pada ayat (2) huruf b, merupakan perbaikan yang berkaitan dengan aspek kriptografis.

Pasal 39

(1) Perbaikan peralatan sandi yang dilakukan oleh Pemerintah Kabupaten adalah perbaikan umum.

(2) Dalam hal melakukan perbaikan umum peralatan sandi, Pemerintah Kabupaten mengirimkan surat pemberitahuan kerusakan yang ditujukan kepada Kepala Badan Siber dan Sandi Negara.

(3) Surat pemberitahuan kerusakan sebagaimana dimaksud pada ayat (2), memuat keterangan mengenai nama peralatan sandi nomor seri, deskripsi kerusakan dan pernyataan untuk diperbaiki.
(4) Dalam hal Pemerintah Kabupten tidak dapat melaksanakan perbaikan umum peralatan sandi, Pemerintah Kabupaten mengajukan surat permohonan perbaikan peralatan sandi kepada Badan Siber dan Sandi Negara.

Pasal 40

(1) Dalam hal perbaikan khusus peralatan sandi, Pemerintah Kabupaten mengirimkan surat permohonan perbaikan yang ditujukan kepada Kepala Badan Siber dan Sandi Negara.
(2) Surat permohonan perbaikan sebagaimana dimaksud pada ayat (1), memuat keterangan mengenai nama peralatan sandi, nomor seri, deskripsi kerusakan dan pernyataan untuk diperbaiki.

Bagian Ketujuh
Pendistribusian Peralatan Sandi

Pasal 41

Pendistribusian peralatan sandi kepada PD dan/atau pejabat/pimpinan Pemerintah Kabupaten wajib memperhatikan ketentuan sebagai berikut:
a. dilengkapi dengan berita acara penyerahan;
b. terjamin keamanan dan keutuhannya sehingga terhindar dari kehilangan dan kerusakan; dan
c. dalam keadaan netral atau non aktif (tidak terisi kunci sistem sandi).

Bagian Kedelapan
Pengawasan dan Pengendalian

Pasal 42

(1) Pengawasan dan pengendalian peralatan sandi harus dilakukan secara menyeluruh, terus menerus dan berkesinambungan.
(2) Pengawasan dan Pengendalian sebagaimana dimaksud pada ayat (1) dilaksanakan setiap 1 (satu) bulan sekali.
(3) Pemerintah Kabupaten harus membuat laporan rutin tentang pelaksanaan pengawasan dan pengendalian peralatan sandi berdasarkan kewenangan dan tanggungjawab masing-masing paling sedikit 1 (satu) bulan sekali dan/atau sewaktu-waktu diperlukan.

Pasal 43

Tempat kegiatan sandi Pemerintah Kabupaten harus mengikuti standar tempat kegiatan sandi yang diatur oleh ketentuan Badan Siber dan Sandi Negara.

Pasal 44

Pengelolaan Alat Pendukung Utama (APU) Persandian yang dilaksanakan oleh Pemerintah Kab upaten sebagaimana dimaksud dalam 32 ayat (1) huruf c adalah:

a. pemeliharaan; dan
b. perbaikan.

Pasal 45

(1) Pemeliharaan Alat Pendukung Utama (APU) Persandian dilakukan berdasarkan prinsip kehati-hatian dan ketepatan.
(2) Pemeliharaan Alat Pendukung Utama (APU) Persandian yang dilakukan Pemerintah Kabupaten mencakup:
    a. memastikan peralatan sandi bebas dari debu/kotoran atau benda lain yang memicu gangguan operasional Peralatan sandi;
    b. menjaga ketersediaan dan kestabilan arus listrik sesuai persyaratan pada peralatan sandi;
    c. menjaga dan memonitor ketersediaan koneksi saluran telekomunikasi pada Peralatan sandi;
    d. memastikan peralatan sandi dapat berfungsi sebagaimana mestinya;
    e. menjaga kestabilan suhu ruangan tempat peletakkan Peralatan sandi;
    f. meletakkan peralatan sandi pada tempat yang aman dari kemungkinan bencana, pencurian, dan kehilangan.
    g. memastikan kelengkapan perangkat;
    h. memastikan kelengkapan dokumen serah terima barang, berita acara serah terima dan/atau penarikan.

Pasal 46

(1) Perbaikan Alat Pendukung Utama (APU) Persandian hanya meliputi perbaikan yang bersifat umum.
(2) Perbaikan umum sebagaimana dimaksud pada ayat (1), merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis.
(3) Dalam hal melakukan perbaikan umum Alat Pendukung Utama (APU) Persandian, Pemerintah Kabupaten mengirimkan surat pemberitahuan kerusakan yang ditujukan kepada Kepala Badan Siber dan Sandi Negara.
(4) Surat pemberitahuan kerusakan sebagaimana dimaksud pada ayat (3), memuat keterangan mengenai nama peralatan sandi, nomor seri, deskripsi kerusakan dan pernyataan untuk diperbaiki.
(5) Dalam hal Pemerintah Kabupaten tidak dapat melaksanakan perbaikan umum terhadap Alat Pendukung Utama (APU), Pemerintah Kabupaten mengajukan surat permohonan perbaikan peralatan sandi kepada Badan Siber dan Sandi Negara.

BAB VI
POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 47

(1) Penyelenggaraan JKS untuk pengamanan informasi berklasifikasi di Pemerintah Kabupaten diterapkan melalui penetapan pola hubungan komunikasi sandi.
(2) Untuk JKS di lingkungan Pemerintah Kabupaten mengacu pada peraturan perundang-undangan.

Pasal 48

Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 47 ayat (1) dilakukan melalui tahapan:
a. identifikasi;
b. analisis; dan
c. penetapan hasil.

Pasal 49

Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 48 huruf a, meliputi:
a. identifikasi pola hubungan komunikasi pejabat/pimpinan di Pemerintah Kabupaten yang sedang dilaksanakan;
b. identifikasi alur Informasi yang dikomunikasikan antar PD;
c. identifikasi dan/atau penyediaan sarana dan prasarana teknologi Informasi dan komunikasi yang digunakan oleh pejabat/pimpinan di Pemerintah Kabupaten;
d. infrastruktur komunikasi yang ada di wilayah Pemerintah Kabupaten; dan
e. kompetensi personil yang dibutuhkan.

Pasal 50

(1) Analisis pola hubungan komunikasi sandi yang diperlukan sebagaimana dimaksud dalam Pasal 48 huruf b dilakukan berdasarkan hasil identifikasi pola hubungan komunikasi, meliputi:
    a. identifikasi pengelola layanan penyelenggaraan persandian;
    b. identifikasi alur informasi internal perangkat daerah;
    c. identifikasi sarana dan prasarana; dan
    d. identifikasi pembiayaan.
(2) Identifikasi pengelola layanan penyelenggaraan persandian sebagaimana dimaksud pada ayat (1) huruf a yaitu kegiatan untuk mengidentifikasi personil dan kompetensi yang dibutuhkan dalam menyelenggarakan kegiatan Persandian.
(3) Identifikasi alur informasi internal perangkat daerah sebagaimana dimaksud pada ayat (1) huruf b yaitu Informasi yang diterima maupun yang diolah dan merupakan informasi yang berklasifikasi sehingga akan di golongkan berdasarkan tingkat klasifikasinya. Informasi yang berklasifikasi tersebut setelah diproses sesuai dengan

kebutuhan, maka dapat disimpan atau pun disampaikan kepada Perangkat Daerah yang membutuhkan.

(4) Identifikasi sarana dan prasarana sebagaimana dimaksud pada ayat (1) huruf c, meliputi:
   a. materiil sandi;
   b. jaringan komunikasi sandi;
   c. alat pendukung utama (APU) persandian;
   d. tempat kegiatan sandi; dan
   e. sarana penunjang.

(5) Identifikasi pembiayaan sebagaimana dimaksud pada ayat (1) huruf d meliputi identifikasi anggaran yang dibutuhkan oleh penyelenggara Persandian di Pemerintah Kabupaten dalam periode waktu satu tahun anggaran.

Pasal 51

(1) Identifikasi materiil sandi sebagaimana dimaksud dalam Pasal 50 ayat (3) huruf a meliputi identifikasi terhadap kebutuhan peralatan sandi dan kunci sistem sandi yang didasarkan pada kondisi infrastruktur, jenis komunikasi, dan hierarki komunikasinya.

(2) Identifikasi jaringan komunikasi sandi sebagaimana dimaksud dalam Pasal 50 ayat (3) huruf b meliputi identifikasi terhadap:
   a. PD yang akan terhubung dalam jaringan komunikasi sandi termasuk di dalamnya unit kerja dalam Pemerintah Kabupaten yang akan mengoperasikan peralatan sandi;
   b. Pejabat Pemerintah Kabupaten yang akan terhubung dalam jaringan komunikasi sandi termasuk di dalamnya penentuan hierarki komunikasi; dan
   c. infrastruktur komunikasi yang ada di lingkungan Pemerintah Kabupaten.

(3) Identifikasi Alat Pendukung Utama (APU) Persandian sebagaimana dimaksud dalam pasal 50 ayat (3) huruf c meliputi identifikasi kebutuhan terhadap perangkat yang mendukung penyelenggaran Persandian.

(4) Identifikasi tempat kegiatan sandi sebagaimana dimaksud dalam Pasal 50 ayat (3) huruf d meliputi identifikasi kebutuhan pengamanan terhadap tempat yang digunakan untuk operasional Persandian sesuai dengan jenis komunikasinya.

(5) Identifikasi sarana penunjang sebagaimana dimaksud dalam Pasal 50 ayat (3) huruf e meliputi identifikasi kebutuhan terhadap peralatan yang mendukung dalam kegiatan penyelenggaraan Persandian, meliputi alat tulis kantor dan sarana pengolah data.

Pasal 52

PD pelaksana Urusan Pemerintahan Bidang Persandian mengoordinasikan hasil identifikasi dan analisis pola hubungan

komunikasi sandi sebagaimana dimaksud dalam Pasal 49 dan Pasal 50 secara berjenjang sampai ke Badan Siber dan Sandi Negara untuk melihat dan menjamin keterhubungan (interkoneksitas) secara vertikal.

Pasal 53

(1) Hasil identifikasi dan analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 48 ditetapkan dengan Keputusan Bupati.
(2) Hasil identifikasi dan analisis pola hubungan komunikasi sandi yang akan ditetapkan sebagaimana dimaksud pada ayat (1) paling sedikit berisi:
    a. entitas yang terhubung; dan
    b. tugas dan tanggung jawab setiap entitas terhadap fasilitas dan layanan yang diberikan.

Pasal 54

Setiap pejabat yang telah ditetapkan sebagai entitas dalam pola hubungan komunikasi sandi harus menggunakan peralatan sandi dalam melakukan setiap komunikasi yang mengandung Informasi Berklasifikasi.

BAB VII
OPERASIONAL DUKUNGAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Pasal 55

(1) Operasional dukungan Persandian untuk pengamanan Informasi merupakan kegiatan operasional yang tidak terkait dengan Kriptografi namun mendukung terciptanya keamanan Informasi.
(2) Operasional dukungan Persandian untuk pengamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi:
    a. pengamanan gelombang frekuensi (*jamming*);
    b. kontra penginderaan; dan
    c. penilaian keamanan sistem Informasi.
(3) Pelaksana kegiatan operasional dukungan Persandian untuk pengamanan Informasi ialah aparatur sipil negara di Pemerintah Kabupaten yang berada pada Bidang atau Seksi penyelenggara Persandian pada PD pelaksana Urusan Pemerintahan Bidang Persandian.
(4) Pelaksanaan operasional dukungan Persandian untuk pengamanan Informasi Pemerintah Provinsi mengacu pada ketentuan peraturan perundang-undangan.

Pasal 56

(1) Pengamanan gelombang frekuensi (*jamming*) sebagaimana dimaksud dalam Pasal 55 ayat (2) huruf a merupakan upaya pengamanan sinyal dari ancaman penyalahgunaan

sinyal untuk kepentingan yang tidak bertanggung jawab dengan cara menutup/memutus frekuensi.

(2) Pengamanan gelombang frekuensi (*jamming*) dilakukan berdasarkan hasil identifikasi pada kegiatan Pemerintah Kabupaten yang berpotensi timbulnya ancaman penyalahgunaan sinyal.

Pasal 57

(1) Kontra penginderaan sebagaimana dimaksud dalam Pasal 55 ayat (2) huruf b merupakan upaya melakukan deteksi dari pengawasan oleh pihak yang tidak berwenang pada objek ruang tertentu.

(2) Kontra penginderaan sebagaimana dimaksud pada ayat (1) dilakukan pada objek ruang milik Pemerintah Kabupaten yang digunakan untuk melakukan komunikasi terkait Informasi Berklasifikasi.

Pasal 58

Pelaksanaan kontra penginderaan sebagaimana dimaksud dalam Pasal 57 dilakukan secara berkala.

Pasal 59

(1) Temuan hasil kontra penginderaan berupa barang yang diduga menjadi peralatan penginderaan (*surveillance*) dapat dikonsultasikan ke Badan Siber dan Sandi Negara.

(2) Hasil pelaksanaan kontra penginderaan harus ditindaklanjuti oleh Pemerintah Kabupaten sebagai bahan evaluasi dan perbaikan penyelenggaraan Urusan Pemerintahan Bidang Persandian.

Pasal 60

(1) Penilaian keamanan sistem Informasi sebagaimana dimaksud dalam Pasal 55 ayat 2 huruf c merupakan upaya untuk mengukur tingkat kerawanan dan keamanan dari sistem Informasi di Pemerintah Kabupaten.

(2) Penilaian keamanan sistem Informasi dilakukan pada sistem Informasi milik Pemerintah Kabupaten.

Pasal 61

(1) Pemerintah Kabupaten melakukan kegiatan penilaian keamanan sistem Informasi secara mandiri.

(2) Dalam hal Pemerintah Kabupaten tidak dapat melakukan kegiatan penilaian keamanan sistem Informasi secara mandiri sebagaimana dimaksud pada ayat (1), Pemerintah Kabupaten mengajukan permohonan penilaian keamanan sistem Informasi kepada Badan Siber dan Sandi Negara.

Pasal 62

Hasil pelaksanaan Penilaian keamanan sistem Informasi sebagaimana dimaksud dalam Pasal 61 harus ditindaklanjuti

oleh Pemerintah Kabupaten sebagai bahan evaluasi dan perbaikan penyelenggaraan Urusan Pemerintahan Bidang Persandian.

BAB VIII
LAYANAN SERTIFIKAT ELEKTRONIK

Pasal 63

Layanan Sertifikat Elektronik di Pemerintah Kabupaten bertujuan untuk menjamin keutuhan, otentikasi dan nir penyangkalan Dokumen Elektronik.

Pasal 64

(1) Layanan Sertifikat Elektronik dapat dimanfaatkan oleh Pemerintah Kabupaten jika telah memenuhi persyaratan dan telah diberikan kewenangan oleh Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara sesuai ketentuan peraturan perundang-undangan.
(2) Setiap aparatur sipil negara Pemerintah Kabupaten dapat memiliki Sertifikat Elektronik yang digunakan selama melaksanakan tugas kedinasan.
(3) Kepemilikan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) difasilitasi oleh PD pelaksana Urusan Pemerintahan Bidang Persandian.

Pasal 65

Tugas kedinasan sebagaimana dimaksud dalam Pasal 64 ayat (2) meliputi:

a. pengiriman dan pembuatan surat elektronik (*email*);
b. pembuatan dokumen persuratan elektronik; dan/atau
c. pembuatan Dokumen Elektronik lainnya yang menggunakan aplikasi dan sistem elektronik.

Pasal 66

Aplikasi dan Sistem Elektronik yang dimiliki oleh Pemerintah Kabupaten harus memanfaatkan layanan Sertifikat Elektronik dalam rangka pengamanan Informasi.

Pasal 67

(1) Proses pemanfaatan Layanan Sertifikat Elektronik dilakukan melalui:
    a. pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan Sertifikat Elektronik;
    b. pengembangan aplikasi pendukung penggunaan Sertifikat Elektronik;
    c. fasilitasi kegiatan sosialisasi dan bimbingan teknis terkait Sertifikat Elektronik; dan
    d. pengawasan dan evaluasi penggunaan Sertifikat Elektronik.

(2) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) huruf a, meliputi:
   a. menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi, dan rekomendasi dari instansi;
   b. menyetujui /menolak permintaan pendaftaran Sertifikat Elektronik;
   c. menindaklanjuti permintaan Sertifikat Elektronik kepada BSrE;
   d. menyampaikan Sertifikat Elektronik kepada pemohon; dan
   e. melakukan pengarsipan berkas pendaftaran Sertifikat Elektronik (*hardcopy* dan *softcopy*).

BAB IX
PEMANTAUAN DAN EVALUASI

Pasal 68

Pemantauan dan evaluasi penyelenggaraan Persandian merupakan upaya untuk memantau perkembangan, mengidentifikasi hambatan, dan upaya perbaikan dalam penyelenggaraan Persandian untuk pengamanan Informasi di Pemerintah Kabupaten.

Pasal 69

(1) Pemantauan dan evaluasi penyelenggaraan Persandian di Pemerintah Kabupaten sebagaimana dimaksud dalam Pasal 68 dilaksanakan oleh PD pelaksana Urusan Pemerintahan bidang Persandian meningkatkan kinerja Persandian.
(2) Pemantauan dan evaluasi harus ditindaklanjuti dengan rencana perbaikan sebagai bahan masukan bagi penyusunan kebijakan, program, dan kegiatan penyelenggaraan Persandian tahun berikutnya.

Pasal 70

(1) Pemantauan dan evaluasi penyelenggaraan Persandian sebagaimana dimaksud dalam Pasal 68 meliputi:
   a. pengawasan dan evaluasi yang bersifat rutin dan sewaktu waktu; dan
   b. pengawasan dan evaluasi yang bersifat tahunan.
(2) Pengawasan dan evaluasi yang bersifat rutin sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan setiap 1 (satu) tahun sekali.

Pasal 71

Pemantauan dan evaluasi yang bersifat rutin dan sewaktu waktu sebagaimana dimaksud dalam Pasal 70 huruf a terdiri dari:

a. pemantauan penggunaan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan Persandian lainnya di Pemerintah Kabupaten; dan
b. pelaksanaan kebijakan manajemen risiko penyelenggaraan Persandian di Pemerintah Kabupaten.

Pasal 72

Pemantauan dan evaluasi yang bersifat tahunan sebagaimana dimaksud dalam Pasal 70 huruf b terdiri dari:
a. pengukuran tingkat pemanfaatan layanan Persandian oleh PD di Pemerintah Kabupaten;
b. penilaian mandiri terhadap penyelenggaraan Persandian di Pemerintah Kabupaten;
c. pengukuran tingkat kepuasan PD di Pemerintah Kabupaten terhadap layanan Persandian yang dikelola oleh PD pelaksana Urusan Pemerintahan Bidang Persandian; dan
d. penyusunan Laporan Penyelenggaraan Persandian Tahunan Pemerintah Kabupaten.

BAB X
KOORDINASI DAN KONSULTASI

Pasal 73

Dalam rangka pelaksanaan Urusan Pemerintahan Bidang Persandian, PD pelaksana Urusan Pemerintahan Bidang Persandian di Kabupaten dapat melaksanakan koordinasi dan/atau konsultasi ke Badan Siber dan Sandi Negara, PD terkait maupun antar Pemerintah Daerah lainnya.

BAB XI
PELAPORAN

Pasal 74

(1) Laporan hasil evaluasi penyelenggaraan Persandian untuk pengamanan informasi Pemerintah Kabupaten disampaikan oleh Bupati kepada Presiden melalui Menteri Dalam Negeri dan tembusan kepada Kepala Badan Siber dan Sandi Negara.
(2) Laporan hasil evaluasi sebagaimana dimaksud pada ayat (1) memuat capaian kinerja Urusan Pemerintahan Bidang Persandian.
(3) Dalam hal tertentu yang dianggap penting terkait teknis Persandian, Bupati dapat menyampaikan laporan langsung kepada Kepala Badan Siber dan Sandi Negara.

BAB XII
PENDANAAN

Pasal 75

Pembiayaan penyelenggaraan Persandian untuk pengamanan Informasi di Pemerintah Kabupaten bersumber dari anggaran, pendapatan dan belanja daerah Kabupaten

BAB XIII
KETENTUAN PENUTUP

Pasal 76

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

Ditetapkan di Muara Teweh
pada tanggal 10 Agustus 2020

BUPATI BARITO UTARA,

ttd

NADALSYAH

Diundangkan di Muara Teweh
pada tanggal 10 Agustus 2020

SEKRETARIAT DAERAH
KABUPATEN BARITO UTARA,

ttd

JAINAL ABIDIN

BERITA DAERAH KABUPATEN BARITO UTARA TAHUN 2020 NOMOR 26

Salinan Sesuai Dengan Aslinya
KEPALA BAGIAN HUKUM,

SETDA

SUGENG HALUYO
NIP. 19670413 [illegible]

LAMPIRAN :
PERATURAN BUPATI BARITO UTARA
NOMOR 26 TAHUN 2020
TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

A. Format Label Informasi Terbatas

TERBATAS

PEMERINTAH KABUPATEN BARITO UTARA
DINAS KOMUNIKASI,INFORMATIKA DAN PERSANDIAN
Jl. Pramuka No. 21 Telepon (0519) 22432 Faximile (0519) 22432
Muara Teweh Provinsi Kalimantan Tengah - 73811

Nomor : .....
Klasifikasi : Terbatas
Lampiran : .....
Perihal : .....

Muara Teweh,.....

Kepada
Yth. .....
.....
.....
Di –
.....

.....
.....
.....
.....
.....
.....

KEPALA DINAS KOMINIKASI,
INFORMATIKA DAN PERSANDIAN

Ttd

.....

B. Format Label Informasi Rahasia

RAHASIA

PEMERINTAH KABUPATEN BARITO UTARA
DINAS KOMUNIKASI,INFORMATIKA DAN PERSANDIAN
Jl. Pramuka No. 21 Telepon (0519) 22432 Faximile (0519) 22432
Muara Teweh Provinsi Kalimantan Tengah - 73811

Nomor : .....
Klasifikasi : Rahasia
Lampiran : .....
Perihal : .....

Muara Teweh,.....

Kepada
Yth. .....
.....
.....
Di –
.....

.....
.....
.....
.....
.....
.....

SEKRETARIS DAERAH
KABUPATEN BARITO UTARA,

Ttd

.....

C. Format Label Informasi Sangat Rahasia

SANGAT RAHASIA

PEMERINTAH KABUPATEN BARITO UTARA
DINAS KOMUNIKASI,INFORMATIKA DAN PERSANDIAN
Jl. Pramuka No. 21 Telepon (0519) 22432 Faximile (0519) 22432
Muara Teweh Provinsi Kalimantan Tengah - 73811

Nomor : .....
Klasifikasi : Sangat Rahasia
Lampiran : .....
Perihal : .....

Muara Teweh,.....

Kepada
Yth. .....
.....
.....
Di –
.....

.....
.....
.....
.....
.....
.....

BUPATI BARITO UTARA,

Ttd

.....

BUPATI BARITO UTARA,

ttd

NADALSYAH