Salinan

BUPATI NIAS BARAT
PROVINSI SUMATERA UTARA

PERATURAN BUPATI NIAS BARAT
NOMOR 12 TAHUN 2022

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH KABUPATEN NIAS BARAT

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI NIAS BARAT,

Menimbang :

a. bahwa berdasarkan Pasal 4 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk mengamankan informasi di Pemerintah Daerah, Bupati bertanggung jawab terhadap pelaksanaan persandian untuk pengamanan informasi;
b. bahwa berdasarkan huruf a di atas, perlu mengatur Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Kabupaten Nias Barat melalui Peraturan Bupati;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b di atas, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Kabupaten Nias Barat;

Mengingat :

1. 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 Indonsia Nomor 5952);
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
3. Undang-Undang Nomor 46 Tahun 2008 tentang Pembentukan Daerah Kabupaten Nias Barat di Provinsi Sumatera Utara (Lembaran Negara Republik Indonesia

Tahun 2008 Nomor 183 Tambahan Lembaran Negara Republik Indonesia Nomor 4930);

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 Repubiik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
5. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
6. Peraturan Presiden 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Tahun 2019 Nomor 1054);
8. Peraturan Daerah Kabupaten Nias Barat Nomor 4 Tahun 2016 tentang Pembentukan Perangkat Daerah Kabupaten Nias Barat (Lembaran Daerah Kabupaten Nias Barat Tahun 2016 Nomor 4).
9. Peraturan Bupati Nias Barat Nomor 38 Tahun 2016 tentang Rincian Tugas, Fungsi dan Penjabaran Tata Kerja Organisasi Perangkat Daerah Kabupaten Nias Barat (Berita Daerah Kabupaten Nias Barat Tahun 2016 Nomor 38 sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Bupati Nias Barat Nomor 6 Tahun 2020 tentang Perubahan Kedua Atas Peraturan Bupati Nias Barat Nomor 38 Tahun 2016 tentang Rincian Tugas, Fungsi dan Penjabaran Tata Kerja Organisasi Perangkat Daerah Kabupaten Nias Barat (Berita Daerah Kabupaten Nias Barat Tahun 2020 Nomor 6).

MEMUTUSKAN

Menetapkan : PERATURAN BUPATI TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN NIAS BARAT.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Nias Barat.

2. Pemerintah Daerah adalah Bupati dan Perangkat Daerah sebagai unsur penyelenggara pemerintahan daerah Kabupaten Nias Barat.
3. Bupati adalah Bupati Nias Barat
4. Perangkat Daerah adalah perangkat daerah di lingkungan Pemerintah Kabupaten Nias Barat.
5. Dinas Komunikasi dan Informatika Kabupaten Nias Barat yang selanjutnya disebut Dinas adalah perangkat daerah yang menyelenggarakan urusan di bidang komunikasi dan informatika, statistik dan persandian.
6. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
8. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
9. Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan, Informasi.
10. Jaring Komunikasi Sandi adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
11. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
12. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
13. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara sertifikat elektronik.
14. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
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 ataupun nonelektronik.

16. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
17. 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, 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.
18. 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 autentifikasi.

Pasal 2

Penyelenggaraan persandian untuk pengamanan informasi di pemerintah Kabupaten Nias Barat bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan persandian untuk pengamanan informasi diantara Pemerintah Daerah dan Pemerintah Pusat;
b. meningkatkan komitmen, efektivitas, dan kinerja Pemerintah Kabupaten Nias Barat dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan persandian untuk pengamanan informasi; dan
c. Memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah;

Pasal 3

Penyelenggaraan persandian untuk pengamanan informasi di pemerintah daerah sebagaimana dimaksud dalam Pasal 2 meliputi :

a. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Kabupaten Nias Barat; dan
b. Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

Bagian Kesatu

Umum
Pasal 4

(1) Penyelenggaraan persandian untuk pengamanan informasi

Pemerintah Daerah sebagaimana dimaksud dalam Pasal 3 huruf a dilaksanakan melalui :

a. penyusunan kebijakan pengamanan informasi;
b. pengelolaan sumber daya keamanan informasi;
c. pengamanan sistem elektronik dan pengamanan informasi nonelektronik; dan
d. penyediaan layanan keamanan informasi.

(2) Bupati sesuai kewenangannya bertanggungjawab terhadap penyelenggaraan persandian sebagaimana dimaksud pada ayat (1).

(3) Penyelenggaraan Persandian yang dilaksanakan Bupati sesuai dengan kewenangannya sebagaimana dimaksud pada ayat (2) dibantu oleh Dinas sesuai dengan tugas dan fungsinya di bidang persandian.

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 5

Penyusunan kebijakan pengamanan informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a dilakukan dengan:

a. menyusun Rencana Strategis Pengamanan Informasi;
b. menetapkan Arsitektur Keamanan Informasi; dan
c. Tata Kelola Keamanan Informasi.

Pasal 6

(1) Bupati melalui Dinas menyusun Rencana Strategis Pengamanan Informasi sebagaimana dimaksud pada Pasal 5 huruf a.

(2) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas :

a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
b. peta rencana penyelenggaraan pengamanan informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.

(3) Rencana strategis pengamanan informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.

(4) Dalam melakukan penyusunan Rencana strategis pengamanan informasi sebagaimana dimaksud pada ayat (1) Bupati melalui Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 7

(1) Bupati melalui Dinas menyusun dan menetapkan Arsitektur Keamanan Informasi sebagaimana dimaksud pada Pasal 5 huruf b.
(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) Bupati melalui Dinas 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) Bupati melakukan evaluasi terhadap Arsitektur Keamanan Informasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Bagian Ketiga

Tata Kelola Keamanan Informasi

Pasal 8

Tata kelola Keamanan Informasi Daerah dimaksudkan untuk:
a. pedoman bagi Dinas dan Perangkat Daerah dalam memanfaatkan teknologi;
b. menjamin terselenggaranya e-Government pada Pemerintah Daerah.
c. menjamin terwujudnya Sistem Pemerintahan Berbasis Elektronik yang aman.

Pasal 9

Ruang lingkup Tata kelola Keamanan Informasi Daerah yaitu:
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

Pasal 10

(1) Keamanan sumber daya teknologi informasi sebagaimana dimaksud pada pasal 9 huruf a meliputi :
    a. aspek keamanan dan keberlangsungan sistem; dan
    b. mekanisme dasar.
(2) Aspek keamanan dan keberlangsungan sistem sebagaimana dimaksud pada ayat (1) harus memenuhi:
    a. Confidentiality, akses terhadap data/informasi dibatasi hanya bagi mereka yang punya otoritas;
    b. Integrity, data tidak boleh diubah tanpa ijin dari yang berhak
    c. Authentication, untuk meyakinkan identitas pengguna sistem; dan
    d. Availability: terkait dengan ketersediaan layanan, termasuk up-time dari sistem dan teknologi informasi;
    e. Non-repudiation, terkait penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.
(3) Mekanisme dasar sebagaimana dimaksud pada ayat (1) huruf b untuk memastikan tercapainya aspek-aspek keamanan dan keberlangsungan sistem yang harus terpenuhi meliputi :
    a. pengamanan dari sisi software aplikasi; dan
    b. pengamanan dari sisi infrastruktur teknologi.

Pasal 11

Keamanan akses kontrol sebagaimana dimaksud pada pasal 9 huruf b meliputi:
a. persyaratan organisasi untuk kendali akses;
b. manajemen akses pengguna;
c. tanggung jawab pengguna; dan
d. kendali akses sistem dan aplikasi.

Pasal 12

Keamanan data dan informasi sebagaimana dimaksud pada pasal 9 huruf c dilaksanakan melalui perlindungan informasi berklasifikasi, mencakup:
a. perlindungan fisik, 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;
b. perlindungan administrasi, dilakukan untuk mencegah kelalaian dan tindakan indisipliner; dan
c. perlindungan logik, dilakukan dengan menggunakan perlindungan logik menggunakan teknik Kriptografi dan steganografi untuk memenuhi aspek kerahasiaan, keutuhan, otentikasi, dan kenirsangkalan.

Pasal 13

Keamanan sumber daya manusia sebagaimana dimaksud pada pasal 9 huruf d mencakup :

a. sumber daya manusia sebelum dipekerjakan;
b. sumber daya manusia selama bekerja; dan
c. sumber daya manusia saat penghentian dan perubahan kepegawaian.

Pasal 14

(1) Keamanan jaringan sebagaimana dimaksud pada Pasal 9 huruf e dilaksanakan untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi.
(2) Keamanan jaringan sebagaimana dimaksud pada ayat (1) dilaksanakan melalui:
    a. kendali jaringan, bahwa jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi;
    b. kemanan layanan jaringan, bahwa mekanisme jaringan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan; dan
    c. pemisahan dalam jaringan, bahwa kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.

Pasal 15

Keamanan surat elektronik sebagaimana dimaksud pada Pasal 9 huruf f dilaksanakan melalui pemanfaatan layanan sertifikat elektronik.

Pasal 16

(1) Keamanan pusat data sebagaimana dimaksud pada Pasal 9 huruf g meliputi kontrol akses dan keamanan fisik dan *logical.*
(2) Kontrol akses dan keamanan fisik dan *logical* pusat data sebagaimana dimaksud pada ayat (1) wajib memenuhi persyaratan sebagai berikut:
    a. memiliki pengaman fisik di setiap jendela yang memungkinkan akses langsung ke pusat data;
    b. memastikan setiap sumber daya manusia di pusat data memiliki pengetahuan dan kesadaran yang cukup terhadap keamanan fisik pusat data;
    c. melakukan pengamanan pusat data selama 24 (dua puluh empat) jam dengan jumlah petugas paling sedikit 2 (dua) orang per *shift*;
    d. memasang perangkat sistem pemantau visual yang berfungsi untuk memantau dan merekam setiap aktivitas pada ruang komputer, ruang mekanik dan

kelistrikan, ruang telekomunikasi dan kawasan kantor;

e. menggunakan sistem akses elektronik dan sistem pengawasan (*surveillance*) yang dikendalikan dengan mekanisme otentikasi yang berfungsi untuk mencegah dan menanggulangi akses fisik tanpa izin terhadap fasilitas, peralatan dan sumber daya dalam ruang komputer;
f. memastikan setiap tamu/pengunjung memiliki izin dan dilengkapi dengan tanda masuk serta tanda pengenal untuk dapat masuk ke ruang komputer, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kantor; dan
g. melengkapi Pusat Data dengan sistem *audit trail* untuk pencatatan akses fisik dan akses *logical* yang terjadi.

Pasal 17

(1) Keamanan komunikasi sebagaimana dimaksud pada Pasal 9 huruf h mencakup keamanan perpindahan informasi.
(2) Perpindahan informasi sebagaimana dimaksud pada ayat (1) dilaksanakan untuk memelihara keamanan informasi yang dipindahkan antar Perangkat Daerah ataupun pihak luar.
(3) Perpindahan informasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui:
    a. prosedur dan kebijakan perpindahan informasi, bahwa kebijakan, prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan informasi melalui penggunaan semua jenis fasilitas komunikasi;
    b. perjanjian perpindahan informasi, bahwa perjanjian harus mengatur perpindahan informasi yang aman antara Perangkat Daerah dan pihak luar ;
    c. pesan elektronik, bahwa informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat; dan
    d. perjanjian kerahasiaan atau menjaga rahasia (nondisclosure agreement), bahwa persyaratan untuk perjanjian kerahasiaan atau menjaga rahasia mencerminkan kebutuhan Pemerintah Daerah untuk perlindungan informasi harus diidentifikasi, direviu secara teratur dan didokumentasikan.

Pasal 18

Ketentuan lebih lanjut terkait Tata Kelola Keamanan Informasi ditetapkan melalui Keputusan Kepala Dinas.

Bagian Keempat

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 19

(1) Dinas melaksanakan pengelolaan sumber daya keamanan informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b.
(2) Pengelolaan sumber daya keamanan informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
    b. pengelolaan sumber daya manusia; dan
    c. manajemen pengetahuan.

Pasal 20

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
(2) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden keamanan informasi dalam sistem elektronik.

Pasal 21

Ketentuan lebih lanjut terkait teknis pengelolaan aset keamanan teknologi informasi dan komunikasi yang meliputi perencanaan, pengadaan, pemanfaatan, dan penghapusan di lingkungan Pemerintah Daerah diatur dan ditetapkan oleh Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 22

(1) Dinas melakukan pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf b.
(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
    a. pengembangan kompetensi;
    b. pembinaan karir;
    c. pendayagunaan; dan
    d. pemberian tunjangan pengamanan persandian

Pasal 23

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 22 ayat (2) 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;
b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau pemerintah daerah; dan
c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf b dilaksanakan dengan ketentuan:
a. pembinaan jabatan fungsional di bidang 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 22 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di Dinas yang menangani urusan keamanan informasi dan persandian sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

(4) Pemberian tunjangan pengamanan persandian sebagaimana dimaksudkan dalam Pasal 22 ayat (2) huruf d meliputi Tunjangan Pengamanan Persandian dan Tunjangan Jabatan Fungsional Sandiman sesuai dengan ketentuan Peraturan Perundang-undangan.

(5) Pemberian Tunjangan sebagaimana dimaksud pada ayat (4) disesuaikan dengan kemampuan keuangan daerah.

Pasal 24

(1) Dinas melakukan manajemen pengetahuan sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf c.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas layanan keamanan informasi dan mendukung proses pengambilan keputusan terkait keamanan informasi.

(3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan keamanan informasi Pemerintah Daerah.

(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan keamanan informasi Pemerintah Daerah.

(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

(6) Ketentuan lebih lanjut mengenai pedoman manajemen pengetahuan keamanan informasi Pemerintah Daerah diatur dengan Peraturan BSSN.

Bagian Kelima

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 25

Dinas melaksanakan pengamanan sistem elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 26

Pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 25 terdiri atas :

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 27

(1) Dalam melaksanakan pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 25, Dinas melakukan:
    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 28

(1) Dalam melaksanakan pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 25, Pemerintah Daerah 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 29

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam pasal 28 ayat (1) Dinas 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.
(3) Pedoman teknis penyelenggaraan pusat operasi pengamanan informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah diatur dan ditetapkan oleh Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 30

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 25 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
(2) Ketentuan lebih lanjut terkait teknis pengamanan informasi nonelektronik sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah diatur dan ditetapkan oleh Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 31

(1) Dinas melaksanakan audit keamanan informasi di lingkup Pemerintah Daerah.
(2) Audit keamanan informasi meliputi audit keamanan sistem elektronik dan audit pelaksanaan sistem manajemen.

(3) Ketentuan lebih lanjut terkait teknis pelaksanaan audit keamanan informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah diatur dan ditetapkan oleh Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Keenam

Penyediaan Layanan Keamanan Informasi

Pasal 32

(1) Dinas melaksanakan penyediaan layanan keamanan informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d.
(2) Layanan keamanan informasi sebagaimana dimaksud pada ayat (1) disediakan untuk pengguna layanan yang terdiri atas :
    a. bupati dan Wakil;
    b. perangkat Daerah; dan
    c. pegawai atau aparatur sipil negara pada Pemerintah Daerah.

Pasal 33

Jenis layanan keamanan informasi sebagaimana dimaksud dalam Pasal 32 ayat (1) 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 persandian dan keamanan informasi;
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.

Pasal 34

(1) Dalam menyediakan layanan keamanan informasi sebagaimana dimaksud dalam Pasal 33 Dinas melaksanakan manajemen layanan keamanan informasi.
(2) Manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas layanan keamanan informasi kepada pengguna layanan.
(3) Manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan layanan keamanan informasi dari pengguna layanan.
(4) Ketentuan lebih lanjut terkait teknis pelaksanaan manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (3) di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan Peraturan Perundang-Undangan.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 35

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 3 huruf b ditetapkan oleh Bupati melalui Keputusan Bupati.
(2) Penetapan hubungan pola komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.
(3) Jaring komunikasi sandi internal pemerintah daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
    a. jaring komunikasi sandi antar Perangkat Daerah;
    b. jaring komunikasi sandi internal Perangkat Daerah; dan
    c. jaring komunikasi sandi pimpinan daerah.
(4) Jaring komunikasi sandi antar perangkat daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
(5) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b

menghubungkan antar pengguna layanan di lingkup internal perangkat daerah.

(6) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Bupati, Wakil Bupati, dan Kepala Perangkat Daerah.

Pasal 36

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 35 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 perangkat daerah dan internal Perangkat Daerah;
   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) Bupati menetapkan hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) sebagai pola hubungan komunikasi sandi antar Perangkat Daerah, dengan Keputusan Bupati.

(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 kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB IV

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 37

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan persandian untuk keamanan informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah.
(2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.
(3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 38

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan persandian untuk pengamanan informasi Daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah di lingkungan Pemerintah Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V

PEMBINAAN DAN PENGAWASAN

Pasal 39

(1) Bupati melakukan pembinaan dan pengawasan terhadap penyelenggaran persandian untuk pengamanan informasi di wilayah Pemerintah Daerah.
(2) Dalam hal Pembinaan dan Pengawasan secara teknis terhadap penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilaksanakan oleh BSSN dan Gubernur sebagai wakil Pemerintah Pusat sesuai dengan kewenanganya.
(3) Ketentuan lebih lanjut terkait pelaksanaan pembinaan dan pengawasan secara teknis terhadap Perangkat Daerah sebagaimana dimaksud dalam ayat (2) dilaksanakan sesuai ketentuan peraturan perundang-undangan.

BAB VI

PENDANAAN

Pasal 40

Pendanaan pelaksanaan penyelenggaraan persandian untuk pengamanan informasi pemerintah daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah; dan/atau
b. Sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII

PENUTUP

Pasal 41

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Lahomi
pada tanggal 7 Maret 2022

BUPATI NIAS BARAT,

ttd.

KHENOKI WARUWU

Diundangkan di Lahomi
pada tanggal 7 Maret 2022

SEKRETARIS DAERAH KABUPATEN NIAS BARAT,

ttd.

FAKHILI GULO

BERITA DAERAH KABUPATEN NIAS BARAT TAHUN 2022 NOMOR 12.

Salinan sesuai dengan aslinya
Plt. KEPALA BAGIAN HUKUM,

HEDWIG SAMITRO GULO, SH., MM
PENATA
NIP. 19900512 201403 1 001