BUPATI TANA TIDUNG
PROVINSI KALIMANTAN UTARA

PERATURAN BUPATI TANA TIDUNG
NOMOR .42 TAHUN .2023

TENTANG
MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI TANA TIDUNG,

Menimbang :

a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di Daerah, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap SPBE dari berbagai ancaman keamanan informasi;
b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di Daerah dari segala jenis gangguan sebagai akibat informasi elektronik dan transkasi elektronik, perlu pengaturan mengenai manajemen keamanan informasi SPBE;
c. bahwa pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu untuk memastikan terjaganya kerahasiaan, keutuhan dan ketersediaan,
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Undang-Undang Nomor 34 Tahun 2007 tentang Pembentukan Kabupaten Tana Tidung di Provinsi Kalimantan Timur (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 100, Tambahan Lembaran Negara Republik Indonesia Nomor 4750);
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 2016 Nomor 251,

Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia 6400);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Indonesia Tahun 2018 Nomor 182);
7. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Indonesia Tahun 2022 Nomor 129);
8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elekronik;
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
10. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
11. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Tana Tidung.
2. Bupati adalah Bupati Tana Tidung.
3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Tana Tidung.
5. Perangkat Daerah Kabupaten Tana Tidung yang selanjutnya disebut Perangkat Daerah adalah unsur pembantu Bupati dan dewan perwakilan rakyat Daerah dalam penyelenggaraan unsur pemerintahan yang menjadi kewenangan Daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. Keamanan Informasi adalah suatu kondisi untuk melindungi aset dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
9. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
10. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
11. Pengembangan Aplikasi adalah proses pembuatan, pengujian, pemeliharaan dan peningkatan aplikasi perangkat lunak yang dirancang untuk menjalankan tugas tertentu atau memberikan layanan kepada pengguna.
12. Aplikasi SPBE adalah satu sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
13. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrase/penghubung, dan perangkat Elekronik lainnya.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal Manajemen Keamanan Informasi SPBE di Daerah.
(2) Kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud ayat (1) meliputi:
    a. ruang lingkup;
    b. penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan terhadap Keamanan Informasi.

(3) Ketentuan lain untuk mendukung kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi:
   a. manajemen risiko;
   b. penetapan prosedur pengendalian Keamanan Informasi SPBE; dan
   c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Ruang Lingkup

Pasal 3

(1) Ruang lingkup Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a meliputi:
   a. data dan informasi SPBE;
   b. Aplikasi SPBE; dan
   c. Infrastruktur SPBE.
(2) Ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Daerah yang harus diamankan dalam SPBE.

Bagian Kedua
Penanggung Jawab

Pasal 4

(1) Penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dijabat oleh Sekretaris Daerah.
(2) Sekretaris Daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (2) menetapkan pelaksana teknis Keamanan SPBE.
(2) Pelaksanaan teknis Keamanan SPBE sebagai dimaksud pada ayat (1) terdiri atas :
   a. Ketua tim; dan
   b. Anggota tim.
(3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dapat dijabat oleh pimpinan Perangkat Daerah yang membidangi urusan komunikasi dan informatika.
(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri atas seluruh pimpinan Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.

Pasal 6

(1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:
   a. menetapkan prosedur pengendalian Keamanan Informasi SPBE;

b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE;
c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
d. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen bisnis berkelanjutan (*business continuity*) dan rencana pemulihan bencana (*disaster recovery plans*); dan
e. melaporkan pelaksanaan Manajemen Keamanan Informasi SPBE pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas:
a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian Keamanan Informasi SPBE pada Perangkat Daerah masing-masing;
b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen bisnis berkelanjutan (*business continuity*) dan rencana pemulihan bencana (*disaster recovery plans*): dan
d. berkoordinasi dengan ketua tim terkait penerapan Keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Bagian Ketiga
Perencanaan

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
a. program kerja Keamanan SPBE; dan
b. target realisasi program kerja Keamanan SPBE.

Pasal 8

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a paling sedikit meliputi:
a. edukasi kesadaran Keamanan SPBE;
b. penilaian kerentanan Keamanan SPBE;
c. peningkatan Keamanan SPBE;
d. penanganan insiden Keamanan SPBE; dan
e. audit Keamanan SPBE.

(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b ditetapkan berdasarkan Indeks Keamanan Informasi dan Tingkat Maturitas Penanganan Insiden setiap tahunnya.

Bagian Kempat
Dukungan Pengoperasian

Pasal 9

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan oleh koordinator SPBE.
(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatan kapasitas terhadap:

a. sumber daya manusia Keamanan SPBE;
b. teknologi Keamanan SPBE; dan
c. anggaran Keamanan SPBE.

Pasal 10

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
a. keamanan TIK; dan
b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan
b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.
(4) Teknologi Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b harus tersedia sesuai dengan kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah yang terdiri atas:
a. pelaporan insiden;
b. menjaga kerahasiaan;
c. hak atas kekayaan intelektual; dan
d. tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
(5) Anggaraan Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Evaluasi Kinerja

Pasal 11

(1) Evaluasi Kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh koordinator SPBE.
(2) Evaluasi Kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Manajemen Keamanan Informasi SPBE.
(3) Evaluasi Kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
a. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
b. mendukung dan merealisasikan program audit Keamanan SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling lama bulan maret pada tahun berikutnya.

Bagian Keenam
Perbaikan Berkelanjutan Terhadap Keamanan Informasi

Pasal 12

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;
b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
c. tindak lanjut hasil audit Keamanan SPBE.

BAB III
PENGENDALIAN TEKNIS KEAMANAN

Bagian Kesatu
Manajemen Risiko

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dilakukan oleh setiap Perangkat Daerah.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko dengan ketentuan subtansi meliputi:
a. inventarisasi aset SPBE;
b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
c. penilaian risiko keamanan terhadap aset SPBE;
d. penentuan prioritas risiko;
e. analisa dampak jika terjadi risiko;
f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
g. rekomendasi kontrol keamanan.
(3) Prosedur pelaksanaan manajemen risiko sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kedua
Penetapan prosedur

Pasal 14

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
(2) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan Manajemen Keamanan Informasi SPBE dengan cakupan aspek dapat meliputi:
a. keamanan perangkat teknologi informasi komunikasi;
b. keamanan jaringan;
c. keamanan pusat data;
d. keamanan perangkat *end point*;
e. keamanan *remote working*;
f. keamanan penyimpanan elektronik;
g. pengelolaan akses kontrol;
h. pengendalian keamanan dari ancaman *virus* dan *malware*;
i. persyaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat keamanan teknologi informasi;
m. perlindungan data pribadi;
n. keamanan komunikasi;

o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
p. pengendalian Keamanan Informasi terhadap pihak ketiga;
q. penerapan kriptografi;
r. penanganan insiden Keamanan Informasi;
s. kelangsungan bisnis atau layanan TIK;
t. perencanaan pemulihan bencana terhadap layanan TIK;
u. audit internal Keamanan SPBE; dan/atau
v. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.

(3) Standar Operasional Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan oleh Kepala Perangkat Daerah yang membidangi komunikasi dan informatika.

Pasal 15

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE.
(2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

Bagian Ketiga
Pengelolaan Pihak Ketiga

Pasal 16

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh setiap Perangkat Daerah.
(2) Perangkat Daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastuktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
(3) Perangkat Daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
(4) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerja sama dengan pihak ketiga.
(5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
PEMBIAYAAN

Pasal 17

Segala biaya yang timbul dalam pelaksanaan Peraturan Bupati ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah.

BAB V
KETENTUAN PENUTUP

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Tideng Pale
pada tanggal 02 November 2023

BUPATI TANA TIDUNG,

IBRAHIM ALI

Diundangkan di Tideng Pale
pada tanggal 02 November 2023

SEKRETARIS DAERAH KABUPATEN TANA TIDUNG,

SAID AGIL

BERITA DAERAH KABUPATEN TANA TIDUNG TAHUN 2023 NOMOR 42