BUPATI TOJO UNA-UNA
PROVINSI SULAWESI TENGAH

PERATURAN BUPATI TOJO UNA-UNA
NOMOR 14 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAH BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI TOJO UNA-UNA,

Menimbang :

a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa untuk melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik;

c. bahwa sesuai dengan ketentuan Pasal 2 Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, manajemen keamanan inormasi sistem pemerintahan berbasis elektronik dilaksanakan oleh perangkat daerah berdasarkan pedoman manajemen keamanan informasi;

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. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 32 Tahun 2003 tentang Pembentukan Kabupaten Tojo Una-Una di Provinsi Sulawesi Tengah (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 147, Tambahan Lembaran Negara Republik Indonesia Nomor 4342);
3. 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 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 2022 Nomor 238, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

MEMUTUSKAN:

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

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
2. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.

3. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang 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.
4. Keamanan SPBE mencakup penjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
5. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (confidentiality) atas informasi dan komunikasi secara Elektronik.
6. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
7. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
8. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinamungan, serta mendukung layanan SPBE yang berkualitas.
9. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
10. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunkasi data, pengolahan dan penyimpanan data, perangkat integrase/penghubung, dan perangkat Elektronik lainnya.
11. Daerah adalah Kabupaten Tojo Una-Una.
12. Bupati adalah Bupati Tojo Una-Una.
13. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Tojo Una-Una.
14. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.

(2) Kebijakan internal menajemen keamanan informasi SPBE sebagaimana dimaksud pada 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 menajemen 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 sebagaiman 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 ketentuan 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) Pelaksana teknis Keamanan SPBE sebagaimana 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 dari seluruh pimpinan Perangkat Daerah lainnya 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. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan Peraturan perUndang- Undangan;
d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
f. 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 business continuity dan *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 minimal 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 Keempat
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 meningkatkan kapasitas terhadap:
   a. sumber daya manusia Keamanan SPBE;
   b. teknologi keamanan SPBE; dan
   c. anggaran keamanan SPBE.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 10

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a minimal 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/atau

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 SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah yang terdiri atas:

a. pelaporan insiden;
b. menjaga kerahasiaan;
c. kekayaan intelektual; dan
d. tata tertib penggunaan dan pengamanan aset maupun layanan TIK.

(5) Anggaran 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 di lingkungan Pemerintah Daerah.

(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 sedikit 1 (satu) kali dalam 1 (satu) tahun.

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

Bagian Kesatu

Manajemen Resiko

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 (risk register) dengan ketentuan substansi 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 mengacu 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 di lingkungan Pemerintah Daerah 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. persayaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat *IT Security*;
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 (*business continuity*);
t. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
u. audit internal keamanan SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk Keputusan Bupati.

Pasal 15

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (3).
(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 Infrastruktur 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 kerjasama 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

KETENTUAN PENUTUP

Pasal 17

Peraturan Bupati ini mulai berlaku pada tanggal diundagkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Tojo Una-Una.

Ditetapkan di Ampana
pada tanggal 8 Juli 2024

BUPATI TOJO UNA-UNA,

MOHAMMAD LAHAY