BUPATI NGANJUK
PROVINSI JAWA TIMUR

KEPUTUSAN BUPATI NGANJUK
NOMOR 188/873/K/411.013/2024
TENTANG
PEDOMAN MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH
KABUPATEN NGANJUK

BUPATI NGANJUK,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 27 ayat (2) Peraturan Bupati Nganjuk Nomor 11 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik sebagaimana telah diubah dengan Peraturan Bupati Nganjuk Nomor 41 Tahun 2023, terkait pentingnya tersusunnya kebijakan manajemen keamanan informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Bupati tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Nganjuk;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2024;

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;

3. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 13 Tahun 2022;

4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah beberapa kali 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;

5. Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan Antara Pemerintah Pusat dan Pemerintahan Daerah;

6. Peraturan Pemerintah Nomor 12 Tahun 2019 tentang Pengelolaan Keuangan Daerah;

7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital;
10. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018;
11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik;
12. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
13. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
14. Peraturan Menteri Dalam Negeri Nomor 77 Tahun 2020 tentang Pedoman Teknis Pengelolaan Keuangan Daerah;
15. 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;
16. Peraturan Badan Riset dan Inovasi Nasional Nomor 2 Tahun 2024 tentang Pedoman Manajemen Pengetahuan Sistem Pemerintahan Berbasis Elektronik;
17. Peraturan Daerah Kabupaten Nganjuk Nomor 1 Tahun 2023 tentang Pengelolaan Keuangan Daerah;
18. Peraturan Bupati Nganjuk Nomor 11 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik sebagaimana telah diubah dengan Peraturan Bupati Nganjuk Nomor 41 Tahun 2023;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN BUPATI TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN NGANJUK.

KESATU : Menetapkan Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Nganjuk sebagaimana tercantum dalam Lampiran Keputusan Bupati ini.

KEDUA : Pedoman sebagaimana dimaksud dalam Diktum KESATU bertujuan untuk memberikan pedoman dalam implementasi keamanan dan informasi serta sebagai petunjuk tentang langkah-langkah yang akan diambil untuk membangun, mengelola serta mempertahankan keamanan informasi serta efektif di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

KETIGA : Segala biaya yang timbul akibat ditetapkannya Keputusan Bupati ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah Kabupaten Nganjuk.

KEEMPAT : Keputusan Bupati ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Nganjuk
pada tanggal 2 Agustus 2024

Pj. BUPATI NGANJUK,

ttd.

SRI HANDOKO TARUNA

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

SUTRISNO, S.H., M.Si.
Pembina Tingkat I
NIP. 19680501 199202 1 001

LAMPIRAN
KEPUTUSAN BUPATI NGANJUK
NOMOR 188/873/K/411.013/2024
TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN NGANJUK

BAB I
PENDAHULUAN

A. Latar Belakang

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE telah mendorong transformasi layanan pemerintahan dari semula dilakukan secara manual menjadi berbasis digital. Transformasi layanan berbasis digital menawarkan berbagai keuntungan antara lain efisiensi, efektifitas, dan akuntabilitas yang tinggi. Namun demikian, transformasi layanan berbasis digital juga menimbulkan risiko baru yaitu munculnya kerentanan dan potensi ancaman terhadap kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan informasi yang dikelola yang diakibatkan oleh berbagai gangguan terhadap sistem yang dimiliki termasuk serangan dan insiden siber.

Keamanan informasi merupakan hal penting yang harus diperhatikan dalam membangun dan menjalankan layanan berbasis digital. Dengan semakin meningkatnya risiko dan insiden siber dalam penyelenggaraan SPBE, maka upaya pengamanan terhadap SPBE harus dilakukan. Data pribadi, infrastruktur, dan aset lainnya yang dimiliki oleh Pemerintah Kabupaten Nganjuk harus dapat dikelola dengan baik. Dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan informasi di lingkungan Pemerintah Kabupaten Nganjuk, diperlukan Sistem Manajemen Keamanan Informasi.

Kebijakan Sistem Manajemen Keamanan Informasi disusun sebagai pedoman bagi setiap personel yang terlibat dalam pengelolaan informasi untuk memastikan terjaganya keamanan informasi. Pedoman ini mengatur proses pengelolaan pengamanan informasi maupun kendali yang diperlukan dalam melakukan pengamanan informasi. Pedoman ini menjadi acuan dalam penyusunan prosedur, petunjuk teknis maupun aturan yang lainnya dalam rangka pengamanan informasi di Pemerintah Kabupaten Nganjuk.

B. Tujuan

Kebijakan Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Pemerintah Lkabupaten Nganjuk dari berbagai bentuk ancaman baik internal maupun eksternal, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), dan kenirsangkalan (*non-repudiation*) aset informasi selalu terjaga dan terpelihara dengan baik.

C. Ruang Lingkup

Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi di lingkungan Pemerintah Kabupaten Nganjuk yang dilaksanakan oleh setiap unit kerja yang terlibat baik sebagai pengguna atau pengelola, instansi pemerintah terkait, mitra kerja, dan pihak ketiga di lingkungan Pemerintah Kabupaten Nganjuk.

Cakupan aset informasi meliputi:

1. data dan informasi;
2. aplikasi;
3. infrastruktur; dan
4. sumber daya manusia.

D. Ketentuan Umum

1. Daerah adalah Kabupaten Nganjuk.
2. Bupati adalah Bupati Nganjuk.
3. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Nganjuk.
4. Satuan Kerja Perangkat Daerah yang selanjutnya disingkat SKPD adalah Satuan Kerja Perangkat Daerah Kabupaten Nganjuk yang terdiri dari Sekretariat Daerah, Sekretariat DPRD, Badan Perencanaan Pembangunan Daerah, Inspektorat, Satuan Polisi Pamong Praja, Dinas Daerah, Lembaga Teknis Daerah dan Lembaga Lain.
5. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
7. 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.
8. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
9. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (confidentiality) atas informasi dan komunikasi secara Elektronik.
10. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (integrity) atas Informasi Elektronik.
11. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (availability) atas Informasi Elektronik.
12. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
13. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.

14. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan system, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrase/penghubung, dan perangkat Elektronik lainnya.
15. Kebijakan internal manajemen keamanan informasi SPBE sebagaimana meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan terhadap keamanan informasi.
16. Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE 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

1. Penetapan Ruang Lingkup

   Penetapan ruang lingkup manajemen keamanan informasi SPBE meliputi:
   a. data dan informasi SPBE;
   b. Aplikasi SPBE; dan
   c. Infrastruktur SPBE.

   Penetapan ruang lingkup diatas merupakan aset Pemerintah Kabupaten Nganjuk yang harus diamankan dalam SPBE.

2. Penetapan Penanggung Jawab
   a. Penetapan penanggung jawab dilaksanakan oleh Bupati.
   b. Penanggung jawab dijabat oleh sekretaris daerah Pemerintah Kabupaten Nganjuk.
   c. Sekretaris daerah Pemerintah Kabupaten Nganjuk sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang- undangan.

3. Pelaksana Teknis

   Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE menetapkan pelaksana teknis Keamanan SPBE. Pelaksana teknis Keamanan SPBE terdiri atas:
   a. Ketua Tim

      Ketua Tim dapat dijabat oleh pimpinan perangkat daerah yang membidangi urusan komunikasi dan informatika.

b. Anggota Tim

Anggota Tim terdiri dari seluruh pimpinan perangkat daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Kabupaten Nganjuk

4. Tugas Pelaksana Teknis

Ketua tim mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kabupaten Nganjuk yang meliputi:

a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Kabupaten Nganjuk;
b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Kabupaten Nganjuk;
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.

Anggota tim 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 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.

5. Perencanaan

Perencanaan ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE. Perencanaan dilakukan dengan merumuskan:

a. program kerja Keamanan SPBE; dan
b. target realisasi program kerja Keamanan SPBE.

6. Program Kerja Keamanan SPBE

Program kerja Keamanan SPBE 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.

Target realisasi program kerja Keamanan ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

7. Dukungan Pengoperasian

Dukungan pengoperasian dilakukan oleh koordinator SPBE dan dilakukan dengan meningkatkan kapasitas terhadap:

a. sumber daya manusia Keamanan SPBE;
b. teknologi keamanan SPBE; dan
c. anggaran keamanan SPBE.
d. Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

8. Sumber Daya Manusia Keamanan SBPE

Sumber daya manusia Keamanan paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:

a. keamanan TIK; dan
b. keamanan aplikasi.

Untuk memenuhi kompetensi SDM Keamanan SPBE), 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.
c. Pemenuhan kompetensi sebagaimana dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.
d. Teknologi keamanan informasi harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.
e. Anggaran Keamanan SPBE disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

9. Evaluasi Kinerja

Evaluasi kinerja dilakukan oleh koordinator SPBE terhadap pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kabupaten Nganjuk dan dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun. Evaluasi kinerja dilaksanakan dengan:

a. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
b. mendukung dan merealisasikan program audit Keamanan SPBE.

10. Perbaikan Berkelanjutan

Perbaikan berkelanjutan dilakukan oleh pelaksana teknis Keamanan SPBE merupakan tindak lanjut dari hasil evaluasi kinerja. Perbaikan berkelanjutan 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

1. Manajemen Risiko

Manajemen risiko dilakukan oleh setiap perangkat daerah dengan menyusun daftar risiko (risk register) 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.

Prosedur pelaksanaan manajemen risiko mengacu sesuai dengan ketentuan peraturan perundang-undangan.

2. Penetapan Prosedur Pengendalian Keamanan Informasi SPBE

Penetapan prosedur pengendalian keamanan informasi SPBE ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE. Penetapan prosedur pengendalian keamanan informasi SPBE digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kabupaten Nganjuk dengan cangkupan 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.

Penetapan prosedur pengendalian keamanan informasi SPBE selanjutnya ditetapkan dalam bentuk keputusan Bupati atau surat edaran sekretaris daerah atau kebijakan teknis lainnya.
Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE. Setiap perangkat daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

3. Pengelolaan Pihak Ketiga
   a. Pengelolaan pihak ketiga dilakukan oleh setiap perangkat daerah. 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.
   b. Perangkat daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
   c. Perangkat daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.
   d. Perangkat daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

SUTRISNO, S.H., M.Si.
Pembina Tingkat I
NIP. 19680501 199202 1 001

Pj. BUPATI NGANJUK,

ttd.

SRI HANDOKO TARUNA