SALINAN

BUPATI KENDAL

PROVINSI JAWA TENGAH
PERATURAN BUPATI KENDAL
NOMOR 57 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KENDAL,

Menimbang : a. bahwa perkembangan teknologi informasi yang pesat sangat berpengaruh terhadap aspek keamanan informasi atau data elektronik bagi Pemerintah Daerah sebagai Penyelenggara Sistem Elektronik maupun masyarakat atau pihak lainnya sebagai Pengguna Sistem Elektronik;

b. bahwa dalam rangka penyelenggaraan Sistem Pemerintahan Berbasis Elektronik yang aman di lingkungan Pemerintah Kabupaten Kendal, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap Sistem Pemerintahan Berbasis Elektronik dari berbagai ancaman keamanan informasi;

c. bahwa berdasarkan ketentuan Pasal 28 ayat (3) Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal terkait pentingnya kebijakan keamanan informasi, perlu mengatur Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal;

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 di Lingkungan Pemerintah Kabupaten Kendal;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana

telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan mengubah Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 52, Tambahan Lembaran Negara Republik Indonesia Nomor 2757);

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. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
6. Peraturan Pemerintah Nomor 32 Tahun 1950 tentang Penetapan Mulai Berlakunya Undang-Undang 1950 Nomor 12, 13, 14, dan 15 dari Hal Pembentukan Daerah-Daerah Kabupaten di Jawa Timur/Tengah/Barat dan Daerah Istimewa Yogyakarta;
7. Peraturan Pemerintah Nomor 16 Tahun 1976 tentang Perluasan Kotamadya Daerah Tingkat II Semarang (Lembaran Negara Republik Indonesia Tahun 1976 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 3079);

8. 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 Nomor 6400);
9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
10. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
11. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);
12. Peraturan Daerah Kabupaten Kendal Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kendal (Lembaran Daerah Kabupaten Kendal Tahun 2016 Nomor 8 Seri D No. 1, Tambahan Lembaran Daerah Kabupaten Kendal Nomor 159) sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Daerah Kabupaten Kendal Nomor 13 Tahun 2021 tentang Perubahan Kedua atas Peraturan Daerah Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kendal (Lembaran Daerah Kabupaten Kendal Tahun 2021 Nomor 13, Tambahan Lembaran Daerah Kabupaten Kendal Nomor 219);
13. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
14. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
15. 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);
16. 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 (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
17. Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di

Lingkungan Pemerintah Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2021 Nomor 35);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati Kendal ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Kendal.
2. Bupati adalah Bupati Kendal.
3. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Kendal.
4. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
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 adalah pengendalian keamanan yang terpadu dalam SPBE, yang 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 Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan informasi 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 sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.

Pasal 2

(1) Peraturan Bupati Kendal ini dimaksudkan sebagai kebijakan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kabupaten Kendal.
(2) Kebijakan Manajemen Keamanan Informasi SPBE sebagaimana dimaksud ayat (1) meliputi :
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan terhadap Keamanan Informasi.
(3) Ketentuan lain untuk mendukung kebijakan 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 MANAJEMEN KEAMANAN INFORMASI SPBE
Pasal 3

(1) Penetapan ruang lingkup Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a meliputi:
    a. data dan informasi SPBE;
    b. Aplikasi SPBE;

c. Infrastruktur SPBE; dan
d. kebijakan keamanan informasi SPBE yang telah dimiliki.

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Kabupaten Kendal yang harus diamankan dalam penyelenggaraan SPBE.

Pasal 4

(1) Penetapan penanggung jawab Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Bupati.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah Kabupaten Kendal.
(3) Sekretaris Daerah Kabupaten Kendal 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 Keamanan Informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan pelaksana teknis Keamanan Informasi SPBE dan prosedur pengendalian Keamanan Informasi SPBE.
(2) Pelaksana teknis Keamanan Informasi 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 Kabupaten Kendal.

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 Kabupaten Kendal yang meliputi:

a. memastikan penerapan standar teknis dan prosedur pengendalian Keamanan Informasi SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
b. mengevaluasi penerapan standar teknis dan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Pemerintah Kabupaten Kendal;
c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi SPBE;
d. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *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 standar teknis dan prosedur pengendalian Keamanan Informasi SPBE pada Perangkat Daerah masing-masing;
b. memastikan penerapan keamanan aplikasi dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur pengendalian Keamanan Informasi SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
c. membantu Ketua Tim merancang dan merumuskan langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans* sesuai sistem elektronik yang dikelola pada Perangkat Daerah masing-masing;
d. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
e. berkoordinasi dengan Ketua Tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 7

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

Pasal 8

(1) Program kerja Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a paling sedikit meliputi:
   a. edukasi kesadaran keamanan Informasi SPBE;
   b. penilaian kerentanan Keamanan Informasi SPBE;
   c. peningkatan Keamanan Informasi SPBE;
   d. penanganan insiden Keamanan Informasi SPBE; dan
   e. audit keamanan SPBE.
(2) Target realisasi program kerja Keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

Edukasi kesadaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf a dilaksanakan paling sedikit melalui kegiatan:
a. sosialisasi; dan
b. pelatihan.

Pasal 10

Penilaian kerentanan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf b dilaksanakan paling sedikit melalui:
a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
c. mengukur tingkat risiko Keamanan Informasi SPBE.

Pasal 11

(1) Peningkatan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 10.
(2) Peningkatan Keamanan Informasi SPBE dilaksanakan paling sedikit melalui:
   a. menerapkan standar teknis dan prosedur pengendalian Keamanan Informasi SPBE; dan
   b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 12

Penanganan insiden Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf d dilaksanakan paling sedikit melalui:

a. mengidentifikasi sumber serangan;
b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. mendokumentasi bukti insiden yang terjadi; dan
e. memitigasi atau mengurangi dampak risiko Keamanan Informasi SPBE.

Pasal 13

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf e harus dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan mencakup :

a. audit keamanan Infrastruktur SPBE; dan
b. audit keamanan aplikasi khusus.

Pasal 14

(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 Informasi SPBE;
    b. teknologi Keamanan Informasi SPBE; dan
    c. anggaran Keamanan Informasi SPBE.
(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan Manajemen Keamanan Informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 15

(1) Sumber daya manusia Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a paling sedikit harus memiliki kompetensi:
    a. keamanan infrastruktur TIK; dan
    b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), setidak-tidaknya diselenggarakan dukungan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur TIK dan keamanan aplikasi; dan

b. bimbingan teknis mengenai standar teknis dan prosedur pengendalian Keamanan Informasi SPBE.

(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan Informasi SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan Informasi SPBE.

(4) Teknologi Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(5) Anggaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 16

(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 Kabupaten Kendal.

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
   a. menganalisis efektifitas pelaksanaan Keamanan Informasi SPBE; dan
   b. mendukung dan merealisasikan program audit Keamanan Informasi SPBE.

(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 17

(1) Perbaikan berkelanjutan terhadap Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh pelaksana teknis Keamanan Informasi SPBE.

(2) Perbaikan berkelanjutan terhadap Keamanan Informasi sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

(3) Perbaikan berkelanjutan terhadap Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan dengan:
   a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi SPBE;
   b. memperbaiki pelaksanaan Keamanan Informasi SPBE secara periodik; dan

c. tindak lanjut hasil audit Keamanan Informasi SPBE.

BAB III
PENGENDALIAN TEKNIS KEAMANAN
Pasal 18

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dilakukan oleh setiap Perangkat Daerah.
(2) Setiap Perangkat Daerah harus menyusun dokumen manajemen risiko atau daftar risiko (*risk register*) dengan substansi meliputi:
   a. inventarisasi aset SPBE;
   b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
   c. penilaian risiko keamanan terhadap aset SPBE;
   d. penentuan risiko yang menjadi prioritas;
   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 pada ketentuan peraturan perundang-undangan.

Pasal 19

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b digunakan untuk mengimplementasikan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kabupaten Kendal dengan cakupan aspek dapat meliputi:
   a. manajemen risiko;
   b. kelangsungan bisnis atau layanan TIK (*business continuity*);
   c. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
   d. audit internal Keamanan Informasi SPBE;
   e. pengendalian Keamanan Informasi SPBE terhadap pihak ketiga;
   f. pengelolaan aset;
   g. perlindungan data pribadi;
   h. keamanan perangkat teknologi informasi komunikasi;
   i. keamanan jaringan;
   j. keamanan pusat data;
   k. keamanan perangkat *end point*;
   l. keamanan penyimpanan elektronik;
   m. keamanan fisik dan lingkungan;
   n. keamanan *remote working*;
   o. pengelolaan akses kontrol;

p. persyaratan keamanan pembangunan dan pengembangan Aplikasi SPBE;
q. keamanan migrasi data;
r. konfigurasi perangkat *IT Security*;
s. keamanan komunikasi;
t. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
u. penerapan kriptografi;
v. penanganan insiden Keamanan Informasi SPBE; dan/atau
w. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.

(2) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) selanjutnya ditetapkan Sekretaris Daerah.

Pasal 20

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 19 ayat (2).
(2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

Pasal 21

(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 prosedur pengendalian Keamanan Informasi 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 dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
KETENTUAN PENUTUP

Pasal 22

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

Ditetapkan di Kendal
pada tanggal 18 Desember 2023

BUPATI KENDAL,

cap ttd

DICO M GANINDUTO

Diundangkan di Kendal
pada tanggal 18 Desember 2023

SEKRETARIS DAERAH
KABUPATEN KENDAL,

cap ttd

SUGIONO

BERITA DAERAH KABUPATEN KENDAL TAHUN 2023 NOMOR 57

Salinan sesuai dengan aslinya,
KEPALA BAGIAN HUKUM
SETDA KABUPATEN KENDAL,

NUR FUAD, S.H., M.H.
Pembina Tk I
NIP. 19700215 199003 1 006