BUPATI BIREUEN
PROVINSI ACEH

PERATURAN BUPATI BIREUEN
NOMOR 42 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PADA PEMERINTAH KABUPATEN BIREUEN

DENGAN RAHMAT ALLAH YANG MAHA KUASA

BUPATI BIREUEN,

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di Lingkungan Pemerintah Kabupaten Bireuen, perlu adanya pedoman manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi, infrastruktur dan keberlangsungan sistem pemerintahan berbasis elektronik pada Pemerintah Kabupaten Bireuen dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik serta untuk meminimalkan dampak resiko keamanan informasi perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu Menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik pada Pemerintah Kabupaten Bireuen;

Mengingat : 1. Undang-Undang Nomor 48 Tahun 1999 tentang Pembentukan Kabupaten Bireuen dan Kabupaten Simeulue (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 176, Tambahan Lembaran Negara Republik Indonesia Nomor 3897) sebagaimana telah diubah dengan Undang-Undang Nomor 8 Tahun 2000 tentang Perubahan atas Undang-Undang Nomor 48 Tahun 1999 tentang Pembentukan Kabupaten Bireuen dan Kabupaten Simeulue (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 75, Tambahan Lembaran Negara Republik Indonesia Nomor 3963);

2. Undang-Undang Nomor 11 Tahun 2006 tentang Pemerintahan Aceh (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 62, Tambahan Lembaran Negara Republik Indonesia Nomor 4633);

3. 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 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
4. 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);
5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 224, 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);
6. 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);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 182);
8. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
9. 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);
10. 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);
11. 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);

12. 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);
13. Qanun Kabupaten Bireuen Nomor 3 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Bireuen (Lembaran Kabupaten Bireuen Tahun 2016 Nomor 67, Tambahan Lembaran Kabupaten Bireuen Nomor 107) sebagaimana telah di ubah untuk kedua kalinya dengan Qanun Kabupaten Bireuen Nomor 3 Tahun 2024 (Lembaran Kabupaten Bireuen Tahun 2024 Nomor 114);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PADA PEMERINTAH KABUPATEN BIREUEN.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Bireuen.
2. Pemerintah Daerah Kabupaten yang selanjutnya disebut Pemerintah kabupaten adalah Bupati sebagai unsur penyelenggara Pemerintah daerah yang memimpin pelaksanaan urusan pemerintah yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Bireuen.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Bireuen.
5. Satuan Kerja Perangkat Kabupaten yang selanjutnya disingkat SKPK adalah unsur perangkat Kabupaten Bireuen yang melaksanakan urusan pemerintahan Kabupaten Bireuen.
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. Koordinator SPBE adalah Sekretaris Daerah Kabupaten Bireuen.
8. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.

9. 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.
10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
11. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (*confidentiality*) atas informasi dan komunikasi secara elektronik.
12. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
13. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
14. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
15. Pengendalian teknis keamanan adalah mekanisme yang diterapkan untuk melindungi informasi dari dampak risiko yang mungkin terjadi pada perangkat lunak dan perangkat keras sistem elektronik.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
17. 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 elektronik lainnya.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE pada Pemerintah Kabupaten Bireuen.
(2) Kebijakan internal manajemen keamanan informasi SPBE 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 internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi:
    a. manajemen risiko;
    b. penetapan prosedur pengendalian pengamanan informasi SPBE; dan

c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Penetapan Ruang Lingkup

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; dan
   c. Infrastruktur SPBE.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Kabupaten Bireuen yang harus diamankan dalam SPBE.

Bagian Kedua
Penetapan Tanggung Jawab

Pasal 4

(1) Penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b ditetapkan oleh Bupati.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah Kabupaten Bireuen.
(3) Sekretaris Daerah Kabupaten Bireuen 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 (3) menetapkan pelaksana teknis Keamanan SPBE.
(2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) paling sedikit terdiri dari:
   a. Ketua tim;
   b. Sekretaris tim; dan
   c. Anggota tim.
(3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh pimpinan SKPK yang membidangi urusan komunikasi dan informatika.
(4) Sekretaris tim sebagaimana dimaksud pada ayat (2) huruf b dijabat oleh kepala bidang yang membidangi persandian/Keamanan Informasi pada SKPK yang membidangi urusan persandian dan Statistik.

(5) Anggota tim sebagaimana dimaksud pada ayat (2) huruf c terdiri dari seluruh pimpinan SKPK yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan data dan informasi SPBE, Aplikasi SPBE dan/atau Infrastruktur SPBE pada Pemerintah Kabupaten.

Pasal 6

(1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a bertugas memastikan pelaksanaan manajemen Keamanan Informasi SPBE 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 ketentuan peraturan perundang-undangan;
   d. merumuskan, mengkoordinasikan dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   e. memutuskan dan merancang layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
   f. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE kepada Koordinator SPBE.

(2) Sekretaris tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b bertugas membantu ketua tim dalam memastikan pelaksanaan manajemen Keamanan Informasi SPBE.

(3) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c bertugas:
   a. mengoordinasikan dan memastikan penerapan prosedur pengendalian Keamanan Informasi SPBE pada SKPK 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 keberlangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
   d. berkoordinasi dengan ketua tim terkait penerapan keamanan data dan informasi SPBE, 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 memuat:
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 pada Pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas 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 mendapatkan alokasi sumber daya yang sesuai dengan ketentuan peraturan perundang-undangan.

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 di bidang:
a. keamanan TIK; dan
b. keamanan aplikasi.
(2) Untuk meningkatkan kompetensi sebagaimana dimaksud pada ayat (1), Pemerintah Kabupaten Bireuen harus melaksanakan kegiatan:
a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
(3) Peningkatan 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 SKPK.
(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada 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 Kabupaten.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan/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 atau sewaktu-waktu jika diperlukan.

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. menindaklanjuti 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 SKPK.

(2) Pelaksanaan manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (risk register) yang 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
   g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan manajemen risiko dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kedua
Penetapan Prosedur Pengendalian
Keamanan Informasi SPBE

Pasal 14

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada 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 yang 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 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 atau *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 Surat Keputusan Bupati atau Surat Edaran Sekretaris Daerah atau kebijakan teknis lainnya.

Pasal 15

(1) Setiap SKPK harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (3).

(2) Setiap kepala SKPK bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Bagian Ketiga
Manajemen Risiko

Pasal 16

(1) Pengelolaan Manajemen Keamanan SPBE pada SKPK dapat dikelola pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c sesuai dengan ketentuan peraturan perundang-undangan.

(2) Setiap SKPK 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) Setiap SKPK harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

(4) Setiap SKPK harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.

(5) Setiap SKPK harus membuat laporan secara berkala kepada penanggungjawab SPBE mengenai pencapaian sasaran tingkat layanan atau *SERVICE LEVEL AGREEMENT (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 diundangkan.

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

Ditetapkan di Bireuen
pada tanggal 31 Desember 2025

BUPATI BIREUEN,

MUKHLIS

Diundangkan di Bireuen
pada tanggal 31 Desember 2025

Pj. SEKRETARIS DAERAH
KABUPATEN BIREUEN,

HANAFIAH

BERITA DAERAH KABUPATEN BIREUEN TAHUN 2025 NOMOR 873