SALINAN

BUPATI MOROWALI UTARA

PROVINSI SULAWESI TENGAH

PERATURAN BUPATI MOROWALI UTARA

NOMOR 16 TAHUN 2026

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MOROWALI UTARA,

Menimbang :

a. bahwa dalam rangka melindungi kerahasiaan keutuhan dan ketersediaan aset Informasi di lingkungan Pemerintah Kabupaten Morowali Utara dari berbagai ancaman keamanan Informasi baik dari dalam maupun luar, perlu adanya Manajemen 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 lingkungan Pemerintah Daerah dari segala jenis gangguan sebagai akibat Informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Pasal 17 ayat (1) 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, setiap instansi pusat dan Pemerintah Daerah harus menerapkan Keamanan Sistem Pemerintahan Berbasis Elektronik;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati Morowali Utara 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 12 Tahun 2013 tentang Pembentukan Kabupaten Morowali Utara di Provinsi Sulawesi Tengah (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 83, Tambahan Lembaran Negara Republik Indonesia Nomor 5414);
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 beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana (Lembaran Negara Republik Indonesia Tahun 2026 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 7153);

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. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara Elektronik.
2. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan Pemerintahan yang memanfaatkan teknologi Informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.

3. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah bagian dari Sistem Manajemen secara keseluruhan berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan, dan memelihara keamanan informasi.
4. Teknologi Informasi dan Komunikasi yang selanjutnya disebut TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan Informasi antar media.
5. Sistem adalah kumpulan komponen atau elemen-elemen yang saling berhubungan satu sama lain untuk mencapai suatu tujuan tertentu.
6. 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.
7. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
8. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
9. Pusat Data adalah fasilitas yang digunakan untuk penempatan Sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
10. Kerahasiaan adalah sesuai dengan konsep hukum tentang Kerahasiaan *(confidentiality)* atas Informasi dan komunikasi secara elektronik.
11. Keutuhan adalah sesuai dengan konsep hukum tentang Keutuhan *(integrity)* atas Informasi elektronik.
12. Ketersediaan adalah sesuai dengan konsep hukum tentang Ketersediaan *(avialibity)* atas Informasi elektronik.
13. Aplikasi SPBE adalah suatu 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.

15. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengirimkan dan/atau menyebarkan Informasi Elektronik.
16. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data *interchange*, surat elektronik, telegram, teleks, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
17. Daerah adalah Kabupaten Morowali Utara.
18. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah otonom.
19. Bupati adalah Bupati Morowali Utara.
20. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Morowali Utara.
21. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
22. Inspektorat adalah Inspektorat Daerah Kabupaten Morowali Utara.
23. Dinas Komunikasi dan Informatika Daerah yang selanjutnya disebut Diskominfo adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi, informatika, persandian dan statistik.
24. Kepala Dinas adalah kepala dinas komunikasi dan informatika Daerah.

Pasal 2

Ruang lingkup pengaturan dalam Peraturan Bupati ini meliputi:

a. penetapan ruang lingkup;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. standar dan prosedur pengendalian;
f. manajemen risiko;
g. pengelolaan pihak ketiga;
h. evaluasi kinerja; dan
i. perbaikan berkelanjutan.

BAB II

PENETAPAN RUANG LINGKUP

Pasal 3

(1) Penetapan ruang lingkup Manajemen Keamanan Informasi SPBE 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 Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Data dan Informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf a merupakan data dan Informasi dalam bentuk elektronik meliputi satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, pertukaran data elektronik, surat elektronik, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
(2) Aplikasi SPBE dan Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dan huruf c yang saling terintegrasi merupakan Sistem Elektronik.

BAB III

PENETAPAN PENANGGUNG JAWAB

Pasal 5

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 huruf b ditetapkan oleh Bupati.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi, Sekretaris Daerah disebut sebagai koordinator SPBE.

Pasal 6

(1) Dalam melaksanakan tugas sebagai koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) bertanggung jawab terhadap pelaksanaan SMKI SPBE.

(2) Pelaksanaan SMKI SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan oleh tim yang terdiri atas:
   a. ketua tim; dan
   b. anggota tim.
(3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh kepala Dinas.
(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan Perangkat Daerah lainnya pada Pemerintah Daerah.
(5) Tim Pelaksana SMKI SPBE sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Bupati.

Pasal 7

(1) Ketua tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE dilingkungan Pemerintah Daerah yang meliputi:
   a. menetapkan standar operasional prosedur pengendalian Keamanan Informasi Pemerintah Daerah;
   b. memastikan penerapan standar teknis dan prosedur pengendalian Keamanan Informasi di lingkungan Pemerintah Daerah;
   c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   d. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen keberlangsungan bisnis dan perencanaan pengelolaan bencana;
   e. melaporkan pelaksanaan Manajemen Keamanan Informasi dan penerapan standar teknis dan prosedur pengendalian Kemanan Informasi pada koordinator SPBE; dan
   f. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Kabupaten Morowali Utara.
(2) Anggota tim sebagaiman dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas:
   a. mengoordinasikan dan/atau memastikan dan prosedur pengendalian keamanan setiap Daerah;
   b. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan perencanaan pengelolaan bencana;
   c. berkoordinasi dengan ketua tim terkait standar teknis dan prosedur pengendalian Keamanan Informasi dan standar teknis dan prosedur Kemanan SPBE; dan

d. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

Pasal 8

(1) Dalam melaksanakan pengawasan internal dilakukan oleh Inspektorat.
(2) Inspektorat sebagaimana dimaksud pada ayat (1) berperan melaksanakan audit internal Keamanan Informasi di Daerah.
(3) Inspektorat sebagaimana dimaksud pada ayat (1) bertanggung jawab untuk:
    a. menyusun pedoman audit internal keamanan informasi;
    b. menyusun perencanaan audit internal keamanan informasi;
    c. melaksanakan kegiatan audit internal keamanan informasi;
    d. memberikan rekomendasi perbaikan atas hasil temuan audit internal Keamanan Informasi;
    e. menyusun laporan audit internal keamanan informasi; dan
    f. menyampaikan laporan audit internal Keamanan Informasi kepada Sekretaris Daerah.

BAB IV
PERENCANAAN
Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 huruf c ditetapkan oleh pelaksana teknis Kemanan 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 10

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a minimal meliputi:
    a. edukasi kesadaran Kemanan 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 9 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

BAB V
DUKUNGAN PENGOPERASIAN
Pasal 11

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 huruf d dilakukan oleh koordinator SPBE.
(2) Koordinator SPBE memastikan pelaksanaan pengamanan Informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program Keamanan Informasi.
(3) 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.

Pasal 12

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf a harus memiliki kompetensi:
a. keamanan infrastruktur teknologi, Informasi dan komunikasi; dan
b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), minimal di dukung dengan kegiatan:
a. pelatihan dan atau sertifikasi kompetensi keamanan infrastruktur teknologi, Informasi dan komunikasi dan keamanan aplikasi; dan
b. bimbingan teknis mengenai standar 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 pengamanan Informasi.

Pasal 13

Teknologi Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

Pasal 14

Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI

STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 15

(1) Standar dan prosedur pengendalian Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 huruf e ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
(2) Standar dan prosedur pengendalian Keamanan SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan SMKI di lingkungan Pemerintah Daerah dengan persyaratan aspek meliputi:
    a. keamanan perangkat teknologi Informasi;
    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. penerapan kriptografi;
    o. keamanan fisik dan lingkungan;
    p. keamanan operasional;
    q. keamanan komunikasi;

r. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan Sistem Informasi;
s. pengendalian keamanan Informasi terhadap pihak ketiga;
t. penanganan insiden keamanan Informasi;
u. kebijakan terhadap pihak ketiga;
v. kelangsungan bisnis atau layanan TIK;
w. perencanaan pemulihan bencana terhadap layanan TIK;
x. audit internal Kemanan SPBE;
y. aspek prosedur pengendalian keamanan Informasi SPBE lainnya; dan/atau
z. Kepatuhan Keamanan SPBE.

(3) Standar dan prosedur pengendalian keamanan SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dengan Keputusan Bupati.

Pasal 16

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan standar dan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 15 ayat (2).
(2) Setiap Perangkat Daerah bertanggungjawab dalam memastikan kegiatan operasional teknologi Informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

BAB VII
MANAJEMEN RISIKO
Pasal 17

(1) Majemen risiko sebagaimana dimaksud dalam pasal 2 huruf f dilakukan oleh setiap Perangkat Daerah untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE.
(2) Setiap Perangkat Daerah harus menerapkan prosedur pelaksanaan manajemen risiko meliputi:
a. komunikasi dan konsultasi;
b. penetapan konteks dan risiko SPBE:
1. invetarisasi informasi umum;
2. identifikasi sasaran SPBE;
3. penentuan struktur pelaksanan Manajemen Risiko SPBE;

4. identifikasi pemangku kepentingan;
5. identifikasi peraturan perundang-undangan;
6. penetapan kategori risiko SPBE;
7. penetapan area dampak risiko SPBE;
8. penetapan kriteria risiko SPBE;
9. matriks analisis risiko SPBE dan level risiko SPBE; dan
10. selera risiko SPBE.

c. Penilaian risiko SPBE:
   1. identifikasi risiko SPBE;
   2. analisis risiko SPBE; dan
   3. evaluasi risiko SPBE.

d. Penanganan risiko SPBE:
   1. prioritas risiko;
   2. rencana penanganan risiko SPBE; dan
   3. risiko residual.

e. Pemantauan dan reviu;

f. Pencatatan dan pelaporan;

g. Dokumen manajemen risiko SPBE:
   1. pakta integritas manajemen risiko SPBE;
   2. dokumen proses risiko SPBE; dan
   3. dokumen proses pengendalian risiko SPBE.

(3) Perangkat Daerah dalam menerapkan prosedur manajemen risiko di setiap lingkungan kerja dapat berkoordinasi dengan pelaksanaan teknis Keamanan Informasi.

BAB VIII
PENGELOLAAN PIHAK KETIGA
Pasal 18

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 huruf g 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 dan aspek keamanan yang diisyaratkan dalam perjanjian kontrak dengan pihak ketiga.
(6) Perangkat Daerah dalam melaksanakan pengelolaan pihak ketiga di setiap lingkungan kerja dapat berkoordinasi kepada pelaksana teknik Keamanan Informasi.

BAB IX
EVALUASI KINERJA
Pasal 19

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 huruh f dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Keamanan SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
    b. menetapkan indikator kinerja pada setiap area proses;
    c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
    d. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
    e. 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.

BAB X
PERBAIKAN BERKELANJUTAN
Pasal 20

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 huruf i dilakukan oleh pelaksana teknis Keamanan SPBE.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari 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 sesuai dengan ketentuan peraturan perundang-undangan.

BAB XI

KETENTUAN PENUTUP

Pasal 21

Pada saat Peraturan Bupati ini diundangkan, ketentuan Pasal 40 Peraturan Bupati Nomor 28 Tahun 2024 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah dihapus.

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 Morowali Utara.

Ditetapkan di Kolonodale
pada tanggal 31 Juli 2026

BUPATI MOROWALI UTARA,

T T D.

DELIS JULKARSON HEHI

Diundangkan di Kolonodale
pada tanggal 31 Juli 2026

SEKRETARIS DAERAH
KABUPATEN MOROWALI UTARA,

T T D.

MUSDA GUNTUR

BERITA DAERAH KABUPATEN MOROWALI UTARA TAHUN 2026 NOMOR 16

Salinan sesuai dengan aslinya :
Kepala Bagian Hukum,

BETSI A. POMBALAWO, SH
NIP. 197801212006042027