BUPATI BONE

PROVINSI SULAWESI SELATAN

PERATURAN BUPATI BONE
NOMOR 106 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BONE

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kabupaten Bone, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap Sistem Pemerintahan Berbasis Elektronik dari berbagai ancaman keamanan informasi;

b. bahwa berdasarkan ketentuan dalam Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik jo 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 Informasi Sistem Pemerintahan Berbasis Elektronik, Pemerintah Daerah harus menerapkan keamanan Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati Bone tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Undang-Undang Republik Indonesia Nomor 29 Tahun 1959 tentang Pembentukan Daerah Tingkat II di Sulawesi (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 74, Tambahan Lembaran Negara Republik Indonesia Nomor 1822);

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. 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);

6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
8. 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);
9. 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);
10. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 16 Tahun 2022 Tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi Dan Komunikasi (Berita Negara Republik Indonesia Tahun 2022 Nomor 1374 ;
11. 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);
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. Peraturan Daerah Kabupaten Bone Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Bone Tahun 2016 Nomor 8, Tambahan Lembaran Daerah Kabupaten Bone Nomor 6);
14. Peraturan Bupati Bone Nomor 13 Tahun

2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Bone (Berita Daerah Kabupaten Bone Tahun 2021 Nomor 13);

15. Peraturan Bupati Bone Nomor 31 Tahun 2023 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi, Informatika dan Persandian (Berita Daerah Kabupaten Bone Tahun 2023 Nomor 31);
16. Peraturan Bupati Bone Nomor 64 Tahun 2023 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Bone Tahun 2023 Nomor 64).

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. Daerah adalah Kabupaten Bone.
2. Pemerintah Daerah adalah Bupati Bone dan Perangkat Daerah sebagai unsur penyelenggara pemerintahan daerah.
3. Bupati adalah Bupati Bone.
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 mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*non repudiation*) 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. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
13. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan 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 integrase/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

(1) Maksud pembentukan Peraturan Bupati ini sebagai pedoman kebijakan internal dalam melaksanakan serangkaian proses Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

(2) Kebijakan internal 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 internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi :

g. manajemen risiko;
h. penetapan prosedur pengendalian keamanan informasi SPBE; dan
i. pengelolaan pihak ketiga

BAB II

KEBIJAKAN INTERNAL

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; 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) Penetapan penanggung jawab sebagaimana dimaksud dalam pasal 2 ayat (2) huruf b dilaksanakan oleh Bupati.

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.

(3) Sekretaris Daerah 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 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) terdiri atas:

a. pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi; dan

b. pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan keamanan informasi dan persandian.

Pasal 6

(1) Pejabat pimpinan tinggi pratama sebagaimana

dimaksud dalam pasal 5 ayat (2) huruf a bertugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah yang meliputi :

a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan
c. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE Pemerintah Daerah.

(2) Pejabat pimpinan tinggi atau pejabat administrator sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b bertugas :

a. menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;
b. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
c. memastikan keberlangsungan proses bisnis SPBE;
d. berkoordinasi dengan pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada Instansi Pusat dan Pemerintah Daerah masing-masing terkait perumusan program kerja dan anggaran Keamanan SPBE.

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c ditetapkan oleh 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 pada pasal 7 ayat (2) huruf a 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.

(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

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; dan

b. anggaran keamanan SPBE.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan Manajemen Keamanan Informasi SPBE diberikan alokasi sumber daya yang sesuai

dengan perundang-undangan.

Pasal 10

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada pasal 9 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
   a. keamanan TIK; dan
   b. keamanan aplikasi SPBE.

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

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada pasal 9 ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

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. 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; dan
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.

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 dalam Pasal 2 ayat (2) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.

(4) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

(5) 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 KEAMANAN

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

Pasal 14

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada Pasal 2 ayat (3) huruf b ditetapkan oleh 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 Pemerintah Daerah 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. 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 (*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 atau surat edaran sekretaris daerah atau kebijakan teknis lainnya.

Pasal 15

(1) Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada 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.

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

PEMBIAYAAN

Pasal 17

Pembiayaan yang diperlukan untuk penyelenggaraan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dibebankan pada :

a. Anggaran Pendapatan Belanja Daerah; dan
b. Sumber lainnya yang sah dan tidak mengikat.

BAB V

KETENTUAN PENUTUP

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Watamponee
Pada Tanggal

Pj. BUPATI BONE,

ANDI ISLAMUDDIN

SUDAH DITELITI OLEH TIM HARMONISASI DAN SINKRONISASI PERUNDANG-UNDANGAN	
1. Drs. H.A.MUH.YAMIN AT., M.Si	
2. ANWAR, S.H., M.Si., M.H.	
3. A.IRSAL MAHMUD, S.Hut,M.Si	
4. RAMLI, S.H.	
5. ANDI GUNAWAN, S.H., M.H.	

Diundangkan di Watamponee
Pada Tanggal

Pj. SEKRETARIS DAERAH,

ANDI MUHAMMAD GUNTUR

BERITA DAERAH KABUPATEN BONE TAHUN 2023 NOMOR