



SALINAN

GUBERNUR PAPUA TENGAH
PERATURAN GUBERNUR PAPUA TENGAH
NOMOR 40 TAHUN 2024
TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN
BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH
PROVINSI PAPUA TENGAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR PAPUA TENGAH,

- Menimbang :
- a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Provinsi Papua Tengah, 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 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 Sistem Pemerintahan Berbasis Elektronik, Pemerintah Daerah mempunyai tanggung jawab untuk melaksanakan manajemen keamanan informasi;
 - c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Gubernur tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Provinsi Papua Tengah;
- Mengingat :
1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
 2. Undang-Undang Nomor 21 Tahun 2001 Tentang Otonomi Khusus Bagi Provinsi Papua (Lembaran Negara Republik Indonesia Tahun 2001 Nomor 135, Tambahan Lembaran Negara Republik Indonesia Nomor 4151), sebagaimana telah beberapa kali diubah terakhir dengan Undang-undang Nomor 2 Tahun 2021 tentang Perubahan Kedua Atas Undang-undang Nomor 21 Tahun 2001 tentang Otonomi Khusus Bagi Provinsi Papua Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 155, Tambahan Lembaran Negara Republik Indonesia Nomor 6697);

3. Undang-Undang...../2

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 Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 251, 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 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);
6. 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);
7. 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);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 189);
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 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
13. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
14. Peraturan Gubernur Nomor 1 Tahun 2022 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Papua Tengah (Berita Daerah Provinsi Papua Tengah Tahun 2022 Nomor 1);
15. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 157);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI PAPUA TENGAH.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini, yang dimaksud dengan:

1. Daerah adalah Provinsi Papua Tengah.
2. Pemerintah Daerah adalah Gubernur. sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonomi.
3. Gubernur adalah Gubernur Papua Tengah.
4. Perangkat Daerah adalah unsur pembantu kepala daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.

5. Sistem Pemerintah...../4

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 kerahasiaan atas informasi dan komunikasi secara Elektronik.
10. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan atas Informasi Elektronik.
11. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan 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 integrasi/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

- (1) Maksud pembentukan Peraturan Gubernur ini sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Provinsi Papua Tengah.
- (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:

- a. manajemen risiko;
- b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
- c. 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 PBE.
- (2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah Provinsi Papua Tengah yang harus diamankan dalam SPBE.
- (3) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) ditetapkan oleh Gubernur.

Pasal 4

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Gubernur.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah Provinsi Papua Tengah.
- (3) Sekretaris daerah Provinsi Papua Tengah 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 sebagai dimaksud pada ayat (1) terdiri atas:
 - a. Pejabat pimpinan tinggi pratama yang membidangi urusan komunikasi dan informatika; dan
 - b. Pejabat pimpinan tinggi atau administrator yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Provinsi Papua Tengah.

Pasal 6

- (1) Pejabat pimpinan tinggi pratama yang menyelenggarakan urusan pemerintahan dibidang komunikasi dan informatika sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas :

a. memastikan...../6

- a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
 - b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
 - c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE Instansi Pusat atau koordinator SPBE Pemerintah Daerah; dan
 - d. tugas lainnya dalam melaksanakan keamanan SPBE.
- (2) Pejabat pimpinan tinggi atau pejabat administrator yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Provinsi Papua Tengah sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas:
- 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; dan
 - e. tugas lainnya dalam melaksanakan keamanan SPBE.

Pasal 7

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c dilakukan 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 dalam Pasal 7 ayat (2) huruf a paling sedikit meliputi:
 - a. edukasi kesadaran Keamanan SPBE;
 - b. penilaian kerentanan Keamanan SPBE;
 - c. peningkatan Keamanan SPBE; dan
 - d. penanganan insiden Keamanan SPBE; dan
 - e. audit Keamanan SPBE.
- (2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.
- (3) Edukasi kesadaran keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan paling sedikit melalui kegiatan:
 - a. sosialisasi; dan
 - b. pelatihan.

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 diberikan alokasi sumber daya yang sesuai.

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:
 - a. keamanan TIK; dan
 - b. keamanan aplikasi.
- (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) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.
- (5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c 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 Provinsi Papua Tengah
- (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...../8

- 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 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 II

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 substansi 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 dalam Pasal 2 ayat (3) huruf b ditetapkan oleh pelaksana teknis Keamanan SPBE.
- (2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Provinsi Papua Tengah dengan cakupan aspek dapat meliputi:
 - a. keamanan perangkat teknologi informasi komunikasi;
 - b. keamanan jaringan;

c. keamanan pusat...../9

- 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 Gubernur 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 dalam 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...../10

- (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 VIII
KETENTUAN PENUTUP

Pasal 17

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Papua Tengah.

Ditetapkan di Nabire
pada tanggal 24 September 2024

Pj. GUBERNUR PAPUA TENGAH
CAP/TTD
RIBKA HALUK

Diundangkan di Nabire
pada tanggal 24 September 2024

Pj. SEKRETARIS DAERAH PAPUA TENGAH,
CAP/TTD

ANWAR HARUN DAMANIK

BERITA DAERAH PROVINSI PAPUA TENGAH TAHUN 2024 NOMOR 40

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM,


YULIUS MANURUNG, SH., M.H.
NIP 197606082002121002