SALINAN

BUPATI SITUBONDO
PROVINSI JAWA TIMUR

KEPUTUSAN
BUPATI SITUBONDO
NOMOR : 100.3.3.2/247/431.013/2025

TENTANG

PROSEDUR PENGENDALIAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN SITUBONDO

BUPATI SITUBONDO

Menimbang : bahwa guna pelaksanaan pengendalian keamanan informasi dalam penerapan sistem pemerintahan berbasis elektronik Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Situbondo dalam rangka mencegah, mendeteksi, dan menanggulangi risiko keamanan informasi serta menjaga kerahasiaan, keutuhan, dan ketersediaan data dan informasi pemerintah untuk mewujudkan tata kelola pemerintahan yang baik dan pelayanan publik yang berkualitas dan terpercaya, perlu menetapkan Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Situbondo, yang pelaksanaannya ditetapkan dengan Keputusan Bupati;

Mengingat :

1. 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 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaks1 Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1);
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 195);
3. 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);
4. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

5. Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. Peraturan Badan Siber dan Sandi Negara (BSSN) 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 Nomor 541 Tahun 2021);
7. Peraturan Bupati Situbondo Nomor 24 Tahun 2024 Tentang penyelenggaraan Sistem Pemerintahan Berbasis Elektronik;
8. Peraturan Bupati Situbondo Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo.

MEMUTUSKAN :

Menetapkan :

KESATU : Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Situbondo, sebagaimana tersebut dalam Lampiran keputusan ini.

KEDUA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Situbondo
Pada Tanggal 15 September 2025

BUPATI SITUBONDO,

ttd.

YUSUF RIO WAHYU PRAYOGA

SALINAN Keputusan ini disampaikan kepada Yth.:
1. Sdr. Inspektur Daerah Kabupaten Situbondo;
2. Sdr. Kepala Dinas Komunikasi dan Informasi Kabupaten Situbondo.

SALINAN sesuai dengan Aslinya,
Plt. KEPALA BAGIAN HUKUM

SALIMA SUNARTO PUTRA, S.H.
Pembina Tingkat I (III/d)
19850725 201503 1 001

LAMPIRAN Keputusan Bupati Situbondo
Tanggal :15 September 2025
Nomor : 100.3.3.2/247/431.013/2025

PROSEDUR PENGENDALIAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN SITUBONDO

A. PENDAHULUAN

Sebagai upaya mendukung penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) yang aman, andal, dan terintegrasi, diperlukan tata kelola keamanan data dan informasi yang efektif dan berkelanjutan. Keamanan data dan informasi menjadi salah satu elemen kunci dalam menjaga kepercayaan publik, mendukung pelayanan yang berkualitas, serta memastikan keberlangsungan operasional pemerintahan daerah. Dalam perwujdannya dibentuk komitmen Pemerintah Kabupaten Situbondo, melalui penetapan Standar Operasional Prosedur (SOP) Keamanan Data dan Informasi yang bertujuan untuk memberikan pedoman teknis bagi seluruh perangkat daerah dalam melaksanakan perlindungan terhadap aset informasi. SOP ini menjadi instrumen penting dalam mengawal keamanan penyelenggaraan SPBE, serta mendukung implementasi prinsip-prinsip keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) sehingga penerapan keamanan SPBE yang efektif, efisien dan berkesinambungan mampu mendukung layanan SPBE yang berkualitas.

B. RUANG LINGKUP

Pada penetapan penetapan Standar Operasional Prosedur (SOP) Keamanan Data dan Informasi mengacu pada ISO 27001:2022 sebagai standar international pada pelaksanaan pengamanan data dan informasi. Ruang lingkup kontrol pengamanan data dan informasi menurut ISO/IEC 27001:2022 mencakup berbagai aspek yang bertujuan untuk memastikan bahwa informasi dalam organisasi Tersedia saat dibutuhkan (*availability*), Akurat dan lengkap (integrity), Hanya dapat diakses oleh pihak yang berwenang (confidentiality). Beberapa kontrol dalam ISO 27001:2022 yang secara langsung terkait pengamanan data meliputi:

1. Annex 13.2 (Data Transfer Protection) – Memastikan keamanan data saat dikirim.
2. Annex 13.1 (Network Security Management) – Melindungi data dalam jaringan.
3. Annex12.3 (Backup) – Memastikan data dapat dipulihkan jika terjadi kehilangan.
4. A.9.4 (System & Application Access Control) – Membatasi akses hanya kepada yang berwenang.

Pada penerapannya penggunaan ISO 27001:2022 menyediakan kerangka komprehensif untuk mengamankan data dengan pendekatan berbasis risiko sehingga tujuan pembangunan standar operasional prosedur pengamanan data dan informasi ini bertujuan meminimalkan peluang terjadinya resiko dalam pemanfataan data.
Lingkup dan penanggung jawab standar teknis dan prosedur keamanan teknologi informasi adalah:

a. Pengembangan aplikasi web dan mobile dilakukan oleh unit yang melaksanakan pengembangan teknologi informasi dan perangkat lunak dan unit lain yang dibawah supervisinya;
b. Sistem Penghubung Layanan dilakukan oleh unit yang melaksanakan pengembangan teknologi informasi dan perangkat lunak; unit yang mengelola layanan jaringan dan perangkat keras dan unit lain yang dibawah supervisinya;
c. Keamanan Pusat Data Pemerintah Kabupaten Situbondo dilaksanakan oleh unit yang mengelola layanan jaringan dan perangkat keras; dan unit lain yang dibawah supervisinya;
d. Keamanan Jaringan Intra dilaksanakan oleh unit yang mengelola layanan jaringan dan perangkat keras; dan unit lain yang dibawahsupervisinya;
e. Pengelolaan dan pengawasan akun secara kredensial dalam pembangunan, penggunaan dan pemanfataan database.

C. KLASIFIKASI KEAMANAN TEKNOLOGI INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN SITUBONDO

Keamanan teknologi informasi di lingkungan Pemerintah Kabupaten Situbondo diklasifikasikan menjadi :

1. Keamanan data Informasi, yang sekurang-kurangnya memenuhi standar teknis keamanan data dan informasi terdiri dari :
   a. Kerahasiaan;
   b. Keaslian;
   c. Keutuhan;
   d. Kenirsangkalan; dan
   e. Ketersediaan.
2. Pengembangan aplikasi berbasis web, yang sekurang-kurangnya memenuhi Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:
   a. Autentikasi;
   b. Manajemen sesi;
   c. Persyaratan kontrol akses;
   d. Validasi input;
   e. Kriptografi pada verifikasi statis;
   f. Penanganan *error* dan pencatatan log;
   g. Proteksi data;
   h. Keamanan komunikasi;
   i. Pengendalian kode berbahaya;
   j. Logika bisnis;
   k. File;
   l. Keamanan api dan *web service*; dan
   m. Keamanan konfigurasi.

3. Pengembangan aplikasi berbasis mobile yang sekurang-kurangnya memenuhi Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi
   a. Penyimpanan data dan persyaratan privasi;
   b. Kriptografi;
   c. Autentikasi dan manajemen sesi;
   d. Komunikasi jaringan;
   e. Interaksi platform;
   f. Kualitas kode dan pengaturan *build*; dan
   g. Ketahanan.
4. Sistem Penghubung Layanan yang sekurang-kurangnya memenuhi Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhinya fungsi
   a. Keamanan interoperabilitas data dan informasi;
   b. Kontrol sistem integrasi;
   c. Kontrol perangkat integrator;
   d. Keamanan api dan *web service*; dan
   e. Keamanan migrasi data.
5. Keamanan Pusat Data Pemerintah Kabupaten Situbondo yang sekurang-kurangnya memenuhi Standar teknis keamanan Pusat Data Pemerintah Kabupaten Situbondo terdiri atas terpenuhinya
   a. Persyaratan keamanan fisik dan manajemen Pusat Data;
   b. Persyaratan koneksi perangkat ke Pusat Data.
6. Keamanan Jaringan Intra yang sekurang-kurangnya memenuhi Standar teknis keamanan Jaringan Intra yang diterapkan pada Jaringan Intra Pemerintah Kabupaten Situbondo terdiri atas terpenuhinya
   a. Aspek administrasi keamanan Jaringan Intra;
   b. Kontrol akses dan autentikasi;
   c. Persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
   d. Kontrol keamanan *gateway*;
   e. Kontrol keamanan access point pada jaringan nirkabel; dan
   f. Kontrol konfigurasi access point pada jaringan nirkabel.

D. STANDAR OPERASIONAL PROSEDUR (SOP) KEAMANAN DATA DAN INFORMASI

1. Standar Operasional Prosedur (SOP) Keamanan Data dan Informasi merupakan panduan tertulis yang mengatur tata cara pengelolaan, penyimpanan, pemrosesan, dan perlindungan data serta informasi dalam suatu organisasi. Pihak yang terlibat dalam SOP ini dimulai dari pemilik data dan informasi yang hendak digunakan, bertahap kepada pengembang yang mengelola data dan informasitersebut dengan otoritas dan atutentikasi dari pimpinan bidang yang berwenang dalam pengelolaan data dan informasi serta melibatkan verifikator yang memiliki kapasitas guna meastikan bahwa persyaratan dan prosedur yang dilakukan telah sesuai. Tujuan dari pembangunan SOP ini adalah memastikan bahwa seluruh aspek keamanan data diterapkan secara konsisten dan terukur, guna mencegah risiko kebocoran, penyalahgunaan, kerusakan, atau kehilangan informasi yang dapat berdampak pada operasional maupun reputasi organisasi.

SOP Keamanan Data dan Informasi harus memenuhi prinsip-prinsip dasar keamanan siber (*cybersecurity*), yang meliputi:

a. Kerahasiaan (Confidentiality) – prinsip yang memastikan bahwa data dan informasi hanya dapat diakses oleh pihak yang berwenang dan terhindar dari penyebaran atau pengungkapan yang tidak sah.
   Melalui pelaksanaan prosedur :
   1) Kontrol Akses Ketat: bentuk penerapan *role-based access control* (RBAC) sehingga hanya pengguna dengan hak tertentu yang dapat mengakses data sensitif dengan mengajukan permohonan akses informasi dan data dengan penerapan tingkatan hak akses yang dilakukan oleh pengelola data dan informasi.
   2) Enkripsi Data: Penggunaan algoritma enkripsi (seperti AES atau RSA) untuk data dalam penyimpanan (*storage*) maupun selama transmisi (*SSL/TLS*) dilakukan oleh pemilik dan pengelola data dan informasi.
   3) NDA (Non-Disclosure Agreement): Setiap pihak yang berinteraksi dengan data wajib menandatangani perjanjian kerahasiaan yang dilakukan antara pemilik data dan pengelola data sehingga memiliki batasan kewenangan sejauh mana data dapat dikelola.

b. Keaslian (Authenticity) – Menjamin bahwa sumber data atau informasi dapat diverifikasi kebenarannya, serta mencegah pemalsuan identitas dalam proses pertukaran data. Melalui :
   1) Autentikasi Multifaktor (MFA): Verifikasi identitas pengguna dengan kombinasi *password*, OTP, atau biometrik yang dilakukan pengelola data dan informasi dalam pemberian hak akses pada pengguna melalui aplikasi yang disediakan.
   2) *Digital Signature*: Tanda tangan digital untuk memvalidasi keaslian dokumen atau transaksi elektronik untuk melakukan validasi terhadap keabsahan data dan informasi.
   3) *Audit Log*: Pencatatan riwayat akses dan modifikasi data untuk pelacakan sumber yang dikembangkan oleh pengelolaan data guna menjadi catatan penelusuran terhadap akses data dan informasi.

c. Keutuhan (Integrity) – Memastikan data tetap akurat, lengkap, dan tidak mengalami perubahan yang tidak sah selama penyimpanan atau transmisi. SOP memastikan keutuhan data dengan menerapkan suatu prosedural terhadap proses pengolahan data yang dilakukan oleh pengelola data dengan penerapan:
   1) *Checksum* dan *Hash Function*: Memastikan data tidak diubah secara tidak sah (contoh: SHA-256).
   2) *Version Control*: Pelacakan perubahan dokumen dan *rollback* jika terjadi kesalahan.
   3) Proteksi dari *Malware*: Pemindaian rutin untuk mencegah korupsi data oleh virus atau *ransomware*.

d. Kenirsangkalan (Non-Repudiation) - Mencegah pihak yang terlibat dalam transaksi atau pertukaran data untuk menyangkal tindakan yang telah dilakukan, sehingga setiap aktivitas dapat dilacak dan dipertanggungjawabkan.
   1) *Digital Certificate*: Menggunakan sertifikat digital yang diterbitkan oleh otoritas terpercaya.
   2) *Timestamping*: Pencatatan waktu setiap transaksi untuk bukti hukum.
   3) *Log Aktivitas Terenkripsi*: Menyimpan bukti tindakan pengguna yang tidak dapat disangkal
e. Ketersediaan (Availability) – Memastikan data dan informasi dapat diakses oleh pihak yang berhak kapan pun dibutuhkan, termasuk perlindungan terhadap gangguan seperti serangan *ransomware* atau bencana sistem. Ketersediaan data dijamin oleh:
   1) *Redundancy System*: Cadangan data di *server* atau lokasi geografis berbeda.
   2) *Disaster Recovery Plan (DRP)*: Prosedur pemulihan data setelah insiden (seperti serangan siber atau bencana alam).
   3) *DDoS Protection*: Mitigasi serangan yang mengganggu akses layanan.

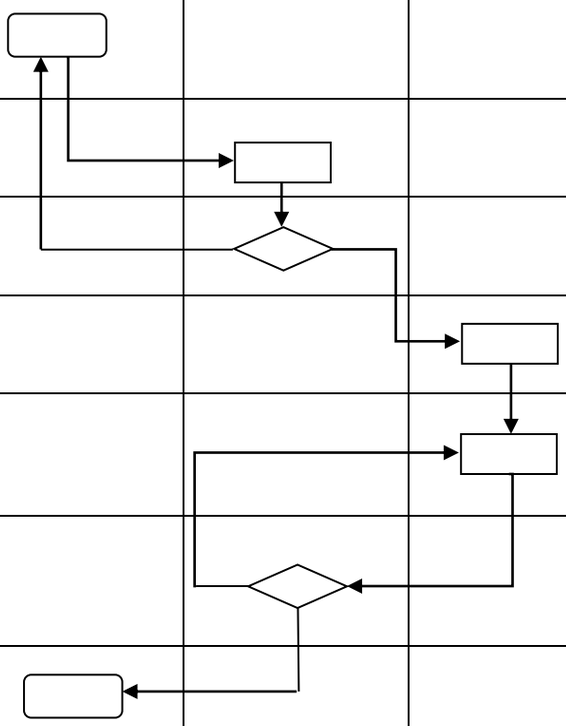
Pemenuhan terhadap kelima prinsip di atas, menghasilkan SOP Keamanan Data dan Informasi tidak hanya melindungi aset digital organisasi, tetapi juga mematuhi regulasi serta meningkatkan kepercayaan. Pelaksanaan implementasi SOP ini mencakup kebijakan *access control*, enkripsi data, audit berkala, *backup* rutin, dan pelatihan kesadaran keamanan bagi seluruh pegawai.

SOP PENGELOLAAN KEAMANAN DATA DAN INFORMASI

PEMERINTAH KABUPATEN SITUBONDO Jl. PB. Sudirman No. 1 SITUBONDO-68312	NOMOR SOP	: 047/SOP.4/431.313.4/2025
	TGL PEMBUATAN	: 01 September 2025
	TGL REVISI	04-Sep-25
	TGL EFEKTIF	05-Sep-25
	NAMA SOP	: Pengelolaan Keamanan Data Dan Informasi

DASAR HUKUM	KUALIFIKASI PELAKSANA
1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan perubahan kedua dengan Undang-Undang Nomor 1 Tahun 2024;	1.Memahami Bahasa Pemrograman 2. Menguasai analisa data 3. Memahami klausul dari standarisasi 4. Memahami proses Bisnis 5. Memahami alur proses 6. Mampu bekerjasama dalam tim 7. Memiliki kemampuan berkomunikasi dengan baik
2. Undang- Undang Nomor 27 Tahun 2022 tentang Pelindungan Data pribadi	
3. Peraturan Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik:	
4. 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:	
4. Peraturan Bupati Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo	
KETERKAITAN	PERALATAN/PERLENGKAPAN
1. ISO 27001:2022 2. Indeks KAMI versi 5.0 3. NIST SP 800-63B	1. Komputer / Laptop 2. Jaringan internet 3. Software untuk pemantauan
PERINGATAN	PENCATATAN DAN PENDATAAN
Agar mengikuti tata tertib yang berlaku guna pencegahan kebocoran data dengan melakukan antisipasi penggunaan password yang mengandung Huruf Besar, Angka dan Simbol	-Disimpan sebagai data elektronik dan manual menggunakan metode MFA - Memiliki catatan tiap perubahan - Penyimpanan yang bersifat independen
Agar mengikuti tata tertib yang berlaku guna pencegahan penyalahgunaan data dengan menekankan pada kontrol akses dan log terhadap data dan informasi	-Disimpan sebagai data elektronik dan manual menggunakan persandian - Memiliki catatan tiap akses - Penyimpanan yang bersifat independen dan terbackup

Diagram SOP Pengelolaan Keamanan Data Dan Informasi				
No.	Kegiatan	Pelaksana		
		Pengelola Data dan Informasi	Pengelolaa Keamanan Informasi	JF Persandian
1	Merumuskan Pembangunan Tata Kelola data Dan Infromasi			
2	Melakukan analisa data dan Informasi			
3	Memverifikasi data dan Informasi			
4	Menetapkan klasifikasi Data dan informasi			
6	Menyusun Teknis Pengelolaan data dan Informasi			
8	Melakukan Assesmenti Sistem Tata kelola Data Dan Informasi			
9	Melaksanakan pengelolaan data dan informasi			



Mutu Baku			Keterangan
Kelengkapan	Waktu	Output	
Data dan Infromasi yang hendak dikelola	1 Hari	Draft Rule pengelolaan	Standar yang digunakan dalam melakukan persiapan pengelolaan data
- Standarisasi Pengelolaan data dan Informasi '- Rule Pengelolaan Data	1 Hari	Analisa Tingkat kepentingan data dan informasi	Melakukan Analisa terhadap tingkat kepentingan data dan informasi
-Analisa Tingkat kepentingan data dan informasi	3 Jam	Verifikasi terhadap kesesuaian Standarisai data	melakukan verifikasi terhadap hasil analisa melalui pemadanan sesuai dengan standar yang ditentukan
Verifikasi terhadap kesesuaian Standarisai data	6 jam	Mengklasifikasikan data dan informasi	melakukan klasifikasi data dan infromasi
Kalsifikasi data dan informasi	1 Hari	Metode persandian data dan informasi	menetapkan metode persandian yang digunakan dalam pengelolaan data dan infromasi
- Metode persandian data dan informasi	6 jam	Analisa metode persandian terhadap kesesuaian kriteria pengelolaan data	melakukan analisa terhadap metode persandian dengan data dan informasi yang akan dikelola
Analisa metode persandian terhadap kesesuaian kriteria pengelolaan data	6 Jam	Melakukan pengelolaan data	melakukan pengelolaan data

E. STANDAR OPERASIONAL PROSEDUR (SOP) PENGEMBANGAN APLIKASI BERBASIS WEB

1. Standar Operasional Prosedur SOP Pengembangan Aplikasi Berbasis Web disusun sebagai wujud pelaksanaan prinsip *due diligence* terhadap kewajiban hukum yang diatur dalam berbagai regulasi nasional yang mengatur perlindungan data, keamanan siber, serta tata kelola sistem elektronik. SOP ini dirancang agar pengembangan aplikasi web di lingkungan instansi publik maupun swasta dilakukan secara aman, bertanggung jawab, dan sesuai standar.

   Penyusunan SOP ini mengacu pada pemenuhan aspek-aspek teknis yang relevan dengan norma hukum yang berlaku yaitu:

   a. Autentikasi
      Mengacu pada ketentuan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), yang mewajibkan adanya mekanisme untuk memastikan bahwa hanya pihak yang sah yang dapat mengakses sistem sehingga pihak pengelola data dan pemilik data wajib melakukan mekanisme dalam penjaminan autentenkasi, pengaturan menganai hal ini sesuai dengan regulasi dan standar:
      1) ISO/IEC 27001 (Kontrol A.9.4 – Manajemen Akses Pengguna)
      2) NIST SP 800-63B (Digital Identity Guidelines)
      3) PCI DSS Requirement 8 (Autentikasi Multi-Faktor untuk akses administratif)
      4) UU PDP (UU No. 27 Tahun 2022) – Perlindungan data pribadi

   b. Manajemen Sesi
      Penerapan penanganan sesi pengguna yang di bangun oleh pengelola data masuk dalam ruang lingkup pengamanan akses sebagaimana diatur dalam Peraturan BSSN Nomor 4 Tahun 2021 tentang Manajemen Risiko Keamanan Siber diatur dalam standar:
      1) NIST SP 800-53 (SI-11) – Manajemen sesi yang aman
      2) GDPR (Pasal 32) – Keamanan pemrosesan data

   c. Persyaratan Kontrol Akses
      Pengelola data dan informasi wajib membangun persyaratan kontrol akses bagi pengguna dan pemilik data yang merupakan pelaksanaan dari prinsip least privilege sebagaimana tercantum dalam standar keamanan nasional dan internasional, serta prinsip akses terbatas sesuai tanggung jawab pengguna sebagaimana diatur melalui:
      1) ISO/IEC 27001 (A.9.1 – Kebijakan Kontrol Akses)
      2) NIST SP 800-53 (AC-3, AC-6 – Least Privilege)

   d. Validasi Input
      Penerapan mengenai validasi input yang dilakukan oleh pemilik data melalui aplikasi yang kemudian mendapat otentikasi oleh pengelola data adalah diwajibkan dalam kerangka perlindungan integritas sistem elektronik, sebagaimana tertuang dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan perubahannya, untuk mencegah manipulasi data dan celah keamanan (vulnerabilities). Hal ini sesuai standarisasi:
      1) OWASP Top 10 (A1: Injection, A3: XSS)
      2) PCI DSS (Requirement 6.5) – Pencegahan code injection
      3) NIST SP 800-115 (Technical Guide to Information Security Testing)

e. Kriptografi pada Verifikasi Statis
Pihak dari pengelola data dan informasi diwajibkan melakukan kriptografi pada data dan informasi. Selaras dengan kewajiban penggunaan teknologi pengamanan data elektronik yang diatur dalam PP No. 71/2019 dan Peraturan BSSN No. 8 Tahun 2020 tentang Keamanan Informasi serta standar yang diacu yaitu ISO/IEC 27001 (A.10.1 – Kebijakan Kriptografi)

f. Penanganan Error dan Pencatatan Log
Dalam pemberian akses pada data dan informasi, perlu juga diterapkan pencatatan log terhadap data dan informasi serta penanganan error yang merupakan bagian dari sistem pencatatan. Hal ini wajib dilakukan oleh penyelenggara sistem elektronik (PSE) untuk tujuan forensik digital, sebagaimana diatur dalam Permenkominfo No. 4 Tahun 2016 serta mengacu pada standarisasi terkait t:
1) ISO/IEC 27001 (A.12.4 – Logging & Monitoring)
2) GDPR (Pasal 33 – Pelaporan Pelanggaran Data)
3) NIST SP 800-92 (Guide to Computer Security Log Management)

g. Proteksi Data
Merupakan pelaksanaan kewajiban pelindungan data pribadi sesuai dengan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengharuskan adanya pengamanan terhadap data pribadi pengguna dalam sistem elektronik, Regulasi Terkait:
1) GDPR (Pasal 5, 25 – Data Minimization & Privacy by Design)
2) UU PDP (Pasal 20 – Penyimpanan & Penghapusan Data Pribadi)
3) PCI DSS (Requirement 3 – Proteksi Data Pemegang Kartu)

h. Keamanan Komunikasi
Penggunaan enkripsi dan kanal komunikasi aman diatur dalam kerangka perlindungan informasi dalam sistem terbuka, sebagaimana tercantum dalam Peraturan BSSN dan ISO/IEC 27033 mengenai keamanan jaringan dan komunikasi.
Regulasi Terkait:
1) NIST SP 800-52 (Guidelines for TLS Implementation)
2) ISO/IEC 27001 (A.13.2 – Keamanan Jaringan)

i. Pengendalian Kode Berbahaya
Prosedur Penanganan terhadap potensi malware dan injeksi kode jahat termasuk dalam prinsip mitigasi risiko siber dan merupakan bagian dari tanggung jawab penyelenggara sistem elektronik sebagaimana diatur dalam PP 71/2019 sebagiamana Regulasi Terkait
1) ISO/IEC 27001 (A.12.2 – Malware Protection)
2) NIST SP 800-83 (Guide to Malware Incident Prevention)
3) OWASP Top 10 (A8: Insecure Deserialization, A9: Using Components with Known Vulnerabilities)

j. Logika Bisnis
Kesesuaian alur logika bisnis untuk mencegah fraud atau penyalahgunaan sistem merupakan bagian dari prinsip transparansi, akuntabilitas, dan pengendalian internal dalam pengelolaan aplikasi yang ditetapkan dalam standar SPBE dan Permen PANRB No. 59 Tahun 2020.

Regulasi Terkait:
1) ISO/IEC 27034 (Application Security Standards)
2) FFIEC (Federal Financial Institutions Examination Council) – Keamanan Aplikasi Perbankan

k. File
Pengaturan keamanan file (unggah dan unduh) merupakan aspek teknis dalam perlindungan sistem dari eksploitasi celah file berbahaya, diatur sebagai bagian dari kebijakan pengendalian akses dan input sistem elektronik.
Regulasi Terkait:
1) ISO/IEC 27001 (A.8.3 – Media Handling)
2) NIST SP 800-171 (Protection of Controlled Unclassified Information)
3) HIPAA (164.310(d) – Media Reuse & Disposal)

l. Keamanan API dan Web Service
Merupakan pelaksanaan dari tanggung jawab integrasi sistem antar layanan yang aman dan andal, sebagaimana tercantum dalam arsitektur SPBE nasional, dan standar interoperability dari Peraturan BSSN dan Permenkominfo.
Regulasi Terkait:
1) OWASP API Security Top 10
2) NIST SP 800-204 (Secure Microservices Architecture)

m. Keamanan Konfigurasi
Pengamanan konfigurasi sistem, termasuk penghapusan default setting dan hardening sistem, merupakan bagian dari kepatuhan terhadap kebijakan minimum security baseline dalam penyelenggaraan layanan publik berbasis digital.
Regulasi Terkait:
1) CIS Benchmarks (Center for Internet Security)
2) NIST SP 800-123 (Guide to Server Security)
3) ISO/IEC 27001 (A.12 – Operations Security)

Standar Operasional Prosedur (SOP) Pengembangan Aplikasi Berbasis Web harus mematuhi berbagai regulasi dan kerangka kerja (*framework*) keamanan siber yang berlaku secara nasional maupun internasional. SOP Pengembangan Aplikasi Berbasis Web yang mengatur ke-13 aspek teknis di atas merupakan manifestasi langsung dari pemenuhan kewajiban hukum dan regulasi nasional. Dengan demikian, SOP ini memiliki dasar normatif yang kuat dan mendukung kepatuhan hukum (compliance) terhadap regulasi keamanan dan perlindungan data yang berlaku di Indonesia. Regulasi ini menjadi landasan hukum dan teknis untuk memastikan bahwa aplikasi web memenuhi prinsip keamanan, privasi, dan integritas data.

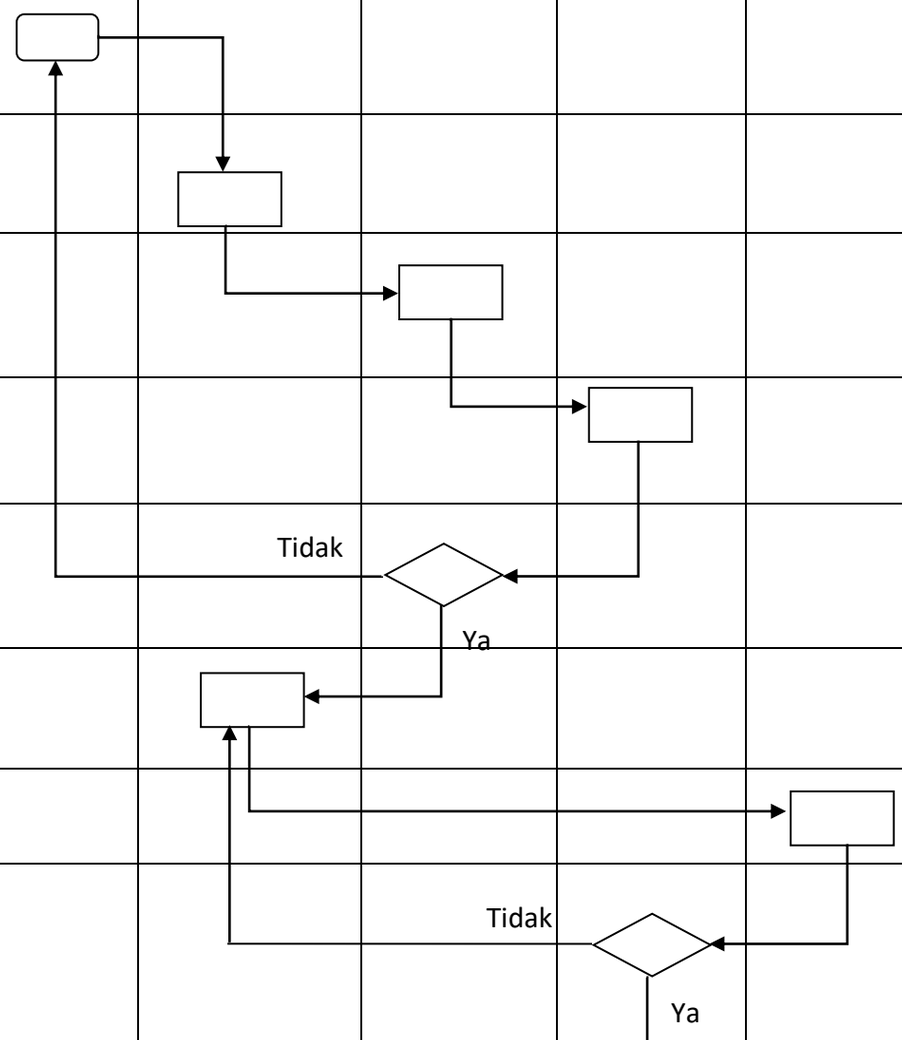
SOP PENGEMBANGAN APLIKASI BERBASIS WEB

PEMERINTAH KABUPATEN SITUBONDO Jl. PB. Sudirman No. 1 SITUBONDO-68312	NOMOR SOP	: 047/SOP.4/431.313.4/2025
	TGL PEMBUATAN	: 01 September 2025
	TGL REVISI	04-Sep-25
	TGL EFEKTIF	05-Sep-25
	NAMA SOP	: Pengembangan Aplikasi Berbasis Website

DASAR HUKUM	KUALIFIKASI PELAKSANA
1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan perubahan kedua dengan Undang-Undang Nomor 1 Tahun 2024;	1.Memahami Bahasa Pemrograman 2. Menguasai analisa data 3. Memahami klausul dari standarisasi 4. Memahami proses Bisnis 5. Memahami alur proses 6. Mampu bekerjasama dalam tim 7. Memiliki kemampuan berkomunikasi dengan baik
2. Peraturan Pemerintah Nomor 82 tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik	
2. Peraturan Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik:	
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:	
3. Peraturan Bupati Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo	

KETERKAITAN	PERALATAN/PERLENGKAPAN
1. ISO 27001:2022 2. Indeks KAMI versi 5.0 3. SOP Pengamanan Data Dan informasi	1. Komputer / Laptop 2. Jaringan internet 3. Software Pengembangan 4. Software Pemantauan
PERINGATAN	**PENCATATAN DAN PENDATAAN**
rancangan untuk diwujudkan pedoman pengembangan yang terperinci dan terstruktur guna pengembangan lebih lanjut	- Pencatatan terhadap setiap Aktivitas yang dilakukan dalam pengembangan berbasis website - Pendataan untuk tiap alur pemrogarman di susun dalam pedoman terperinci - Kontrol terhadap mekanisme pengembangan terkait dengan keamanan data dan informasi di lakukan pencatatan - Inspeksi terhadap pemenuhan standarisasi yang digunakan dalam pengembangan aplikasi dilakukan dengan seksama
pengembangan memiliki platform yang sesuai dan mengikuti perkembangan teknologi guna meminimalisir kerusakan dan kegagalan sistem yang berakibat pada kegagalan pengelolaan data	

Diagram SOP Pengembangan Aplikasi Berbasis Web						
No.	Kegiatan	Pelaksana				
		Pemohon Aplikasi	Tim Perancangan Aplikasi	JF Persandian	Tim Keamanan informasi	Pengembang Aplikasi
1	Menerima Permintaan Pembangunan Aplikasi					
2	Menganalisa data yang digunakan dalam aplikasi					
3	Menentukan metode pengelolaan data aplikasi					
4	merumuskan proses bisnis aplikasi					
5	Melukakan verifikasi kesesuaian standar					
6	Menerima desain Pembangunan Aplikasi					
7	Membangun aplikasi					
8	Melakukan verifikasi terhadap proses dalam aplikasi dengan standar					
9	Menyerahkan Pengelolaan aplikasi					
10	Menyerahkan Pengelolaan aplikasi					



Prosedur Pengembangan Aplikasi Berbasis Website			
Mutu Baku			Keterangan
Kelengkapan	Waktu	Output	
Draft pembangunan aplikasi berbasis website	1 Hari	data dan prosedur penggunaan aplikasi	Melakukan Penelitian terhadap tinkat kepentingan dari pembangunan aplikasi
data dan prosedur penggunaan aplikasi	3 Jam	-Analisa Tingkat kerentanan data dan informasi yang akan digunakan	melakukan analisa terhadap tingkat kerentana data dan informasi yang dilintakan dalam pembangunan aplikasi berbasis website
-Analisa Tingkat kerentanan data dan informasi yang akan digunakan	1 hari	Metode persandian data dan informasi	menetapkan metode persandian yang digunakan dalam pengelolaan data dan infromasi
- Metode persandian data dan informasi	6 Jam	Perumusan proses bisnis dari aplikasi yang akan dibanguna	melakukan analisa terhadap metode persandian dengan data dan informasi yang akan dikelola
Perumusan proses bisnis dari aplikasi yang akan dibangun	6 Jam	verifikasi proses bisnis dari aplikasi yang dibanguna dengan standarisasi yang digunakan	melakukan verifikasi terhadap proses bisnis sesuai dengan standarisasi
verifikasi proses bisnis dari aplikasi yang dibanguna dengan standarisasi yang digunakan	1 Hari	Rancangan Aplikasi	Melakukan perancangan aplikasi secara prosedural
Rancangan Aplikasi	4 hari	Pembangunan Aplikasi	melakukan pemabngunan tahapan tiap prosedur dalam aplikasi
Mengembangkan Aplikasi	1 hari	Verifikasi tiap proses pengembangan website dengan standar yang digunakan	melakukan Verifikasi tiap proses dalam aplikai dengan standar yang digunakan
Verifikasi tiap proses pengembangan website dengan standar yang digunakan	6 Jam	persetujuan penyerahan Aplikasi	melakukan Penyerahan Aplikasi
persetujuan penyerahan Aplikasi	6 Jam	Menerima Aplikasi	melakukan pengelolaan Aplikasi

F. STANDAR OPERASIONAL PROSEDUR (SOP) PENGEMBANGAN APLIKASI BERBASIS MOBILE

Standar Operasional Prosedur (SOP) Teknis Keamanan Aplikasi Berbasis Mobile sangat penting untuk memastikan bahwa aplikasi mobile tidak hanya berfungsi dengan baik, tetapi juga aman dari berbagai ancaman siber. SOP ini dirancang untuk memenuhi fungsi-fungsi kritis yang secara kolektif menjaga integritas, kerahasiaan, dan ketersediaan data serta fungsionalitas aplikasi. Pembangunan SOP ini ditujukan untuk pembanguna keamanan yang komprehensif, aplikasi rentan terhadap serangan yang dapat menyebabkan kebocoran data, kerugian finansial, hilangnya kepercayaan pengguna, dan kerusakan reputasi. kerangka kerja yang sistematis dihasilkan dalam alur SOP ini sebagai bagian untuk mengembangkan dan memelihara aplikasi yang aman. Hal ini dipastikan dengan terpenuhinya fungsi-fungsi SOP dalam perwujudan Keamanan Aplikasi Mobile sebagaimana penjelasan berikut ini :

a. Penyimpanan Data dan Persyaratan Privasi
   SOP ini memastikan bahwa data sensitif, baik yang disimpan di perangkat maupun di *backend*, dienkripsi dan dilindungi dari akses tidak sah. Titik penting fungsi ini adalah tindakan mencegah pencurian data pribadi, informasi keuangan, atau data sensitif lainnya. Kepatuhan terhadap regulasi privasi seperti GDPR (*General Data Protection Regulation*) atau undang-undang perlindungan data lokal juga sangat penting. Cakupan SOP adalah Menentukan praktik terbaik untuk enkripsi data saat istirahat (*data at rest*), pengelolaan kunci enkripsi, penghapusan data yang aman, dan penerapan kontrol akses yang ketat.

b. Kriptografi
   SOP yang dibangun mencakup pengaturan penggunaan algoritma kriptografi yang kuat dan praktik terbaik untuk implementasinya. Tujuan dari pemenuhan fungsi ini adalah melindungi data selama transmisi dan penyimpanan. Penggunaan kriptografi yang lemah atau salah implementasi dapat dengan mudah dipecahkan oleh penyerang. Hal-hal yang mencakup didalam SOP inin adalah menentukan algoritma enkripsi yang disetujui, metode pertukaran kunci yang aman, pengelolaan sertifikat digital, dan pencegahan penggunaan fungsi kriptografi yang usang atau tidak aman.

c. Autentikasi dan Manajemen Sesi
   Fungsi ini memastikan bahwa hanya pengguna yang sah yang dapat mengakses aplikasi dan bahwa sesi pengguna dikelola dengan aman untuk mencegah penyalahgunaan. Sehingga mampu mencegah akses tidak sah ke akun pengguna. Celah dalam autentikasi atau manajemen sesi dapat memungkinkan penyerang untuk menyamar sebagai pengguna lain atau melakukan tindakan tanpa izin. Dalam SOP ini bertujuan menentukan standar untuk autentikasi multifaktor (MFA), kebijakan kata sandi yang kuat, batas waktu sesi, penghapusan token sesi setelah logout, dan perlindungan terhadap serangan *brute force* atau *credential stuffing*.

d. Komunikasi Jaringan
Fungsi dari SOP ini memastikan bahwa komunikasi dalam status aman dan terlindungi dari penyadapan atau modifikasi mengingat aplikasi mobile sering berkomunikasi dengan *backend server* melalui jaringan. Sehingga mencegah serangan *man-in-the-middle* (MitM), kebocoran data selama transmisi, atau penyuntikan data berbahaya. Dimana titik utamanya adalah penggunaan HTTPS/TLS (Transport Layer Security) dengan konfigurasi yang tepat, *pinning* sertifikat, validasi sertifikat server, dan pencegahan penggunaan protokol komunikasi yang tidak aman.

e. e. Interaksi Platform
Aplikasi mobile berinteraksi dengan sistem operasi (OS) perangkat dan komponen platform lainnya. SOP bertujuan mengelola potensi kerentanan yang muncul dari interaksi ini. Mencegah eksploitasi celah keamanan pada OS atau komponen pihak ketiga yang dapat memengaruhi aplikasi. Menentukan praktik untuk penggunaan izin aplikasi yang minimal, validasi input dari OS, penanganan *intent* atau *deep link* yang aman, dan pembaruan rutin komponen platform.

f. Kualitas Kode dan Pengaturan Build
Kualitas kode yang buruk dapat menyebabkan kerentanan keamanan yang signifikan. SOP ini memastikan bahwa kode ditulis dengan aman dan proses *build* aplikasi juga aman. Mengurangi jumlah kerentanan dalam kode sumber, seperti *injection flaws*, *buffer overflows*, atau kesalahan logika. Mendorong praktik *secure coding*, penggunaan alat analisis kode statis dan dinamis (SAST/DAST), *code review*, dan konfigurasi *build* yang mengamankan aplikasi dari *reverse engineering* atau *tampering*.

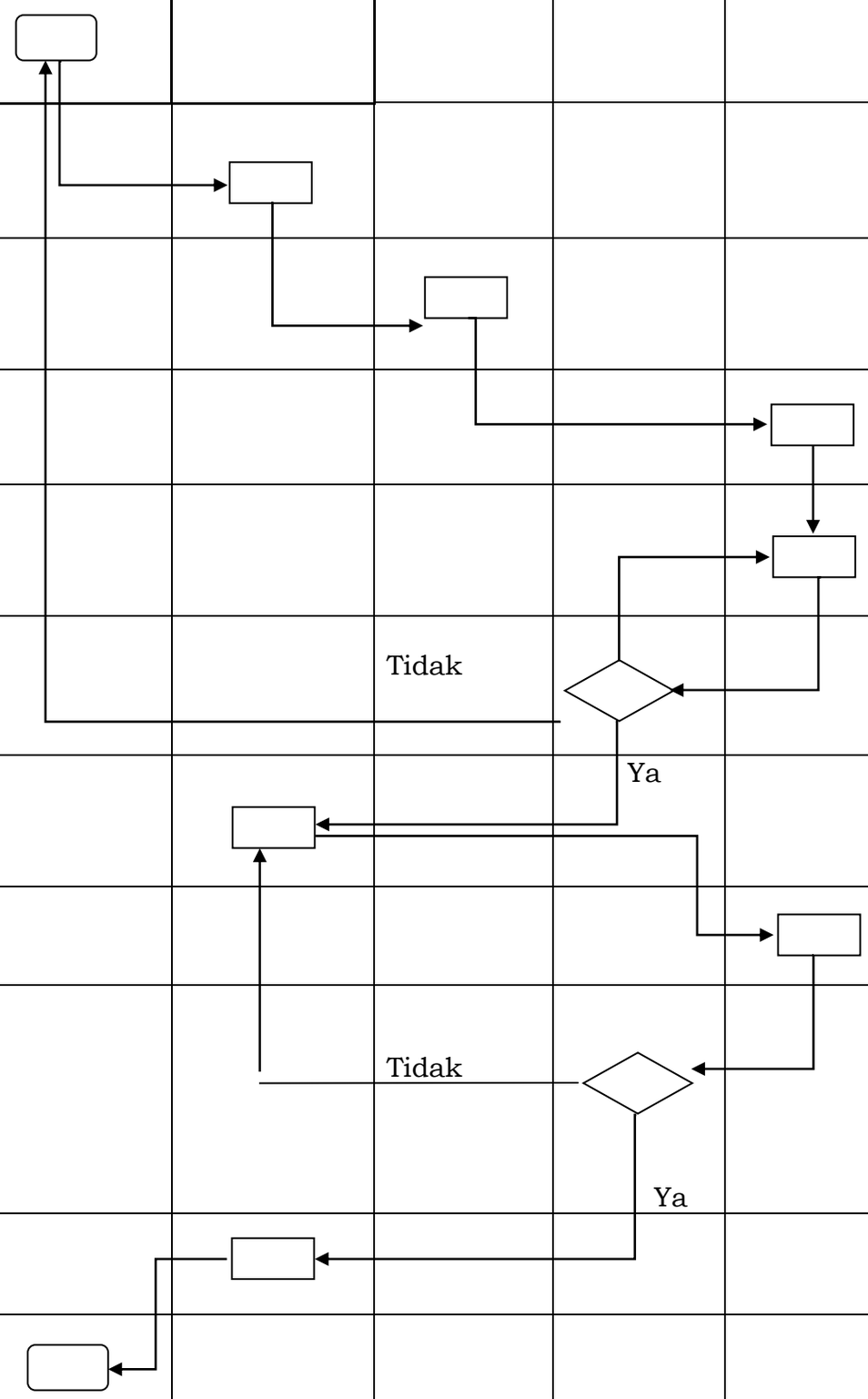
g. Ketahanan (Resilience)
Ketahanan merujuk pada kemampuan aplikasi untuk menahan serangan dan terus beroperasi meskipun ada upaya perusakan. Memastikan aplikasi dapat bertahan dari serangan seperti tampering, reverse engineering, atau upaya untuk menemukan kerentanan. Mencakup teknik seperti obfuscation kode, anti-tampering, root/jailbreak detection, dan implementasi mekanisme pertahanan diri untuk mempersulit penyerang menganalisis atau memodifikasi aplikasi.

Dengan memenuhi fungsi-fungsi ini, pembangunan SOP teknis keamanan aplikasi berbasis mobile akan menciptakan sebuah fondasi yang kuat untuk mengembangkan dan mengoperasikan aplikasi yang aman dan dapat dipercaya, melindungi pengguna dan data mereka dari berbagai ancaman siber.

SOP PENGEMBANGAN APLIKASI BERBASIS MOBILE

<table>
<tr><td colspan="2" rowspan="5">PEMERINTAH
KABUPATEN SITUBONDO
Jl. PB. Sudirman No. 1
SITUBONDO-68312</td><td>NOMOR SOP</td><td>: 047/SOP.4/431.313.4/2025</td></tr>
<tr><td>TGL PEMBUATAN</td><td>: 01 September 2025</td></tr>
<tr><td>TGL REVISI</td><td>04-Sep-25</td></tr>
<tr><td>TGL EFEKTIF</td><td>05-Sep-25</td></tr>
<tr><td>NAMA SOP</td><td>: Pengembangan Aplikasi Berbasis Mobile</td></tr>
<tr><td colspan="2">DASAR HUKUM</td><td colspan="2">KUALIFIKASI PELAKSANA</td></tr>
<tr><td colspan="2">1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan perubahan kedua dengan Undang-Undang Nomor 1 Tahun 2024;</td><td colspan="2" rowspan="4">1.Memahami Bahasa Pemrograman
2. Menguasai analisa data
3. Memahami klausul dari standarisasi
4. Memahami proses Bisnis
5. Memahami alur proses
6. Mampu bekerjasama dalam tim
7. Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td colspan="2">2. Peraturan Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik:</td></tr>
<tr><td colspan="2">3. 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:</td></tr>
<tr><td colspan="2">4. Peraturan Bupati Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo</td></tr>
<tr><td colspan="2">KETERKAITAN</td><td colspan="2">PERALATAN/PERLENGKAPAN</td></tr>
<tr><td colspan="2">1. ISO 27001:2022
2. Indeks KAMI versi 5.0
3. SOP Pengamanan data Dan informasi</td><td colspan="2">1. Komputer / Laptop
2. Jaringan internet
3. Software untuk pemantauan</td></tr>
<tr><td colspan="2">PERINGATAN</td><td colspan="2">PENCATATAN DAN PENDATAAN</td></tr>
<tr><td colspan="2">- rancangan harus menjadi pedoman pengembangan yang terperinci dan terstruktur guna pengembangan lebih lanjut
- Pembangunan aplikasi harus bersifat adaptif mengikuti perkembangan teknologi mobile</td><td colspan="2" rowspan="2">-Disimpan sebagai data elektronik dan manual
- Memiliki catatan tiap perubahan
- Penyimpanan yang bersifat independen</td></tr>
<tr><td colspan="2">pengembangan memiliki platform yang memiliki tingkat keamanan tinggi guna meminimalisir pencurian data dan kegagalan sistem</td></tr>
</table>

Diagram SOP Pengembangan Aplikasi Berbasis Mobile						
No.	Kegiatan	Pelaksana				
		Pemohon Aplikasi	Tim Perancangan Aplikasi	JF Persandian	Tim Keamanan informasi	Pengembang Aplikasi
1	Menerima Permintaan Pembangunan Aplikasi					
2	Menganalisa data yang digunakan dalam aplikasi					
3	Menentukan metode pengelolaan data aplikasi					
4	merumuskan proses bisnis aplikasi					
5	Menyesuaikan dengan Frame work yang digunakan					
6	Melukakan verifikasi kesesuaian standar			Tidak	Ya	
7	Menerima desain Pembangunan Aplikasi					
8	Membangun aplikasi					
9	Melakukan verifikasi terhadap proses dalam aplikasi dengan standara			Tidak	Ya	
10	Menyerahkan Pengelolaan aplikasi					
11	Menyerahkan Pengelolaan aplikasi					



Mutu Baku			Keterangan
Kelengkapan	Waktu	Output	
Draft pembangunan aplikasi berbasis website	1 Hari	data dan prosedur penggunaan aplikasi	Melakukan Penelitian terhadap tinkat kepentingan dari pembangunan aplikasi
data dan prosedur penggunaan aplikasi	3 Jam	-Analisa Tingkat kerentanan data dan informasi yang akan digunakan	melakukan analisa terhadap tingkat kerentana data dan informasi yang dilintakan dalam pembangunan aplikasi berbasis Mobile
-Analisa Tingkat kerentanan data dan informasi yang akan digunakan	1 Hari	Metode persandian data dan informasi	menetapkan metode persandian yang digunakan dalam pengelolaan data dan infromasi
- Metode persandian data dan informasi	6 jam	Perumusan proses bisnis dari aplikasi yang akan dibanguna	melakukan analisa terhadap metode persandian dengan data dan informasi yang akan dikelola
Perumusan proses bisnis dari aplikasi yang akan dibanguna	6 jam	- framework pengembangan yang digunakan	melakukan analisa mengenai kesesuaian framework dan ruang lingkup dari pengembangan aplikasi yang berbasis mobile
- framework pengembangan yang digunakan	6 Jam	verifikasi proses bisnis dari aplikasi yang dibanguna dengan standarisasi yang digunakan	melakukan verifikasi terhadap proses bisnis sesuai dengan standarisasi
verifikasi proses bisnis dari aplikasi yang dibanguna dengan standarisasi yang digunakan	1 Hari	Rancangan Aplikasi	Melakukan perancangan aplikasi secara prosedural
Rancangan Aplikasi	4 hari	Pembangunan Aplikasi	melakukan pemabngunan tahapan tiap prosedur dalam aplikasi
Mengembangkan Aplikasi	1 hari	Verifikasi tiap proses pengembangan website dengan standar yang digunakan	melakukan Verifikasi tiap proses dalam aplikai dengan standar yang digunakan
Verifikasi tiap proses pengembangan website dengan standar yang digunakan	6 Jam	persetujuan penyerahan Aplikasi	melakukan Penyerahan Aplikasi
persetujuan penyerahan Aplikasi	6 Jam	Menerima Aplikasi	melakukan pengelolaan Aplikasi

G. STANDAR OPERASIONAL PROSEDUR (SOP) SISTEM PENGHUBUNG LAYANAN

Penyusunan Standar Operasional Prosedur (SOP) Teknis Keamanan Sistem Penghubung Layanan diwajibkan memebuhi fungsi krusial untuk menjaga integritas, kerahasiaan, dan ketersediaan data serta layanan. kelima fungsi tersebut adalah :

a. Keamanan Interoperabilitas Data dan Informasi
batasan dalam SOP ini merinci bagaimana data dan informasi yang dipertukarkan antara sistem yang berbeda akan diamankan sebagaimana berikut:
1) Enkripsi Data: Prosedur untuk mengenkripsi data baik saat transit (in-transit) maupun saat disimpan (at-rest) untuk mencegah akses tidak sah.
2) Integritas Data: Mekanisme untuk memverifikasi bahwa data tidak diubah selama transmisi atau penyimpanan, seperti penggunaan *hashing* atau tanda tangan digital.
3) Otentikasi dan Otorisasi: Proses untuk memastikan hanya sistem dan pengguna yang berwenang yang dapat mengakses dan memproses data tertentu. Ini bisa melibatkan penggunaan token, sertifikat digital, atau protokol otentikasi kuat lainnya.
4) Manajemen Kunci: Prosedur aman untuk pembuatan, distribusi, penyimpanan, dan pencabutan kunci enkripsi.
5) Format Data Aman: Panduan untuk menggunakan format data yang aman dan terstandarisasi untuk mengurangi kerentanan.

b. Kontrol Sistem Integrasi
Fungsi ini berfokus pada kontrol keamanan terhadap seluruh sistem integrasi yang menghubungkan berbagai layanan. SOP harus mencakup:
1) Manajemen Konfigurasi Aman: Prosedur untuk mengkonfigurasi sistem integrasi agar sesuai dengan best practices keamanan, termasuk penonaktifan layanan yang tidak perlu, hardening sistem operasi, dan patch management rutin.
2) Segmentasi Jaringan: Aturan untuk mengisolasi sistem integrasi dari jaringan internal atau eksternal yang tidak relevan untuk membatasi dampak serangan.
3) Pemantauan dan Pencatatan (Logging): Prosedur untuk memantau aktivitas sistem integrasi secara terus-menerus dan mencatat semua peristiwa relevan untuk deteksi anomali dan forensik keamanan.
4) Manajemen Akses: Kontrol ketat terhadap siapa yang dapat mengakses sistem integrasi dan dengan hak akses apa, mengikuti prinsip least privilege.
5) Backup dan Pemulihan Bencana: Prosedur untuk membuat cadangan sistem dan data secara teratur, serta rencana pemulihan bencana jika terjadi insiden keamanan besar.

c. Kontrol Perangkat Integrator
Pengaturan terhadap keamanan perangkat keras dan lunak yang berfungsi sebagai integrator atau penghubung antar sistem. Ini mencakup:
1) Penyusunan tingkat keamanan yang bertujuan menentukan kriteria keamanan dalam pemilihan serta pengadaan perangkat keras dan perangkat lunak sebagai integrator.
2) Penguatan Perangkat (Device Hardening): Prosedur untuk mengamankan perangkat integrator dengan menonaktifkan port yang tidak digunakan, mengubah kata sandi default, dan menerapkan konfigurasi aman.

3) Manajemen Vulnerabilitas: Proses untuk secara rutin memindai dan menambal kerentanan keamanan pada perangkat integrator.
4) Kendali Akses Fisik: Prosedur untuk membatasi akses fisik ke perangkat integrator hanya kepada personel yang berwenang.
5) Penghapusan Data Aman: Prosedur untuk menghapus data secara aman dari perangkat integrator sebelum dibuang atau digunakan kembali.

d. Keamanan API dan Web Service

API (Application Programming Interface) dan *web service* sering menjadi titik masuk utama untuk integrasi data yang menjadi bagian pengembangan aplikasi dan penguatan pada keamanan data dan informasi. SOP ini menguraikan langkah-langkah keamanan spesifik untuk mereka:

1) Otentikasi dan Otorisasi API: Mekanisme untuk memverifikasi identitas klien yang mengakses API dan menentukan operasi apa yang diizinkan untuk mereka (misalnya, melalui token OAuth2, kunci API, atau sertifikat).
2) Validasi Input: Prosedur untuk memvalidasi semua input yang diterima oleh API untuk mencegah serangan seperti injeksi SQL atau Cross-Site Scripting (XSS).
3) Pembatasan Tingkat (Rate Limiting): Kebijakan untuk membatasi jumlah permintaan API dalam periode waktu tertentu untuk mencegah Denial of Service (DoS).
4) Manajemen Sesi Aman: Prosedur untuk memastikan sesi API aman, termasuk penggunaan token yang berumur pendek dan pencegahan pembajakan sesi.
5) Penanganan Kesalahan Aman: Panduan untuk memastikan bahwa pesan kesalahan API tidak mengungkapkan informasi sensitif yang dapat dieksploitasi oleh penyerang.
6) Keamanan Transport Layer: Penggunaan HTTPS/SSL/TLS untuk mengamankan komunikasi antara klien dan web service.

e. Keamanan Migrasi Data

Migrasi data adalah proses yang sangat rentan terhadap insiden keamanan jika tidak ditangani dengan hati-hati. SOP ini harus mencakup:

1) Perencanaan Keamanan Migrasi: Assessment risiko sebelum migrasi, identifikasi data sensitif, dan penentuan metode migrasi paling aman.
2) Enkripsi Data Selama Migrasi: Prosedur untuk mengenkripsi data saat dipindahkan dari sistem sumber ke sistem target.
3) Integritas Data Migrasi: Mekanisme untuk memverifikasi bahwa data tidak rusak atau diubah selama proses migrasi.
4) Validasi Data Pasca-Migrasi: Prosedur untuk memverifikasi integritas dan kelengkapan data setelah migrasi selesai.
5) Penghapusan Data Sumber Aman: Panduan untuk menghapus data dari sistem sumber secara aman setelah migrasi berhasil dan divalidasi.
6) Manajemen Akses Selama Migrasi: Kontrol ketat terhadap siapa yang memiliki akses ke data dan sistem selama proses migrasi.

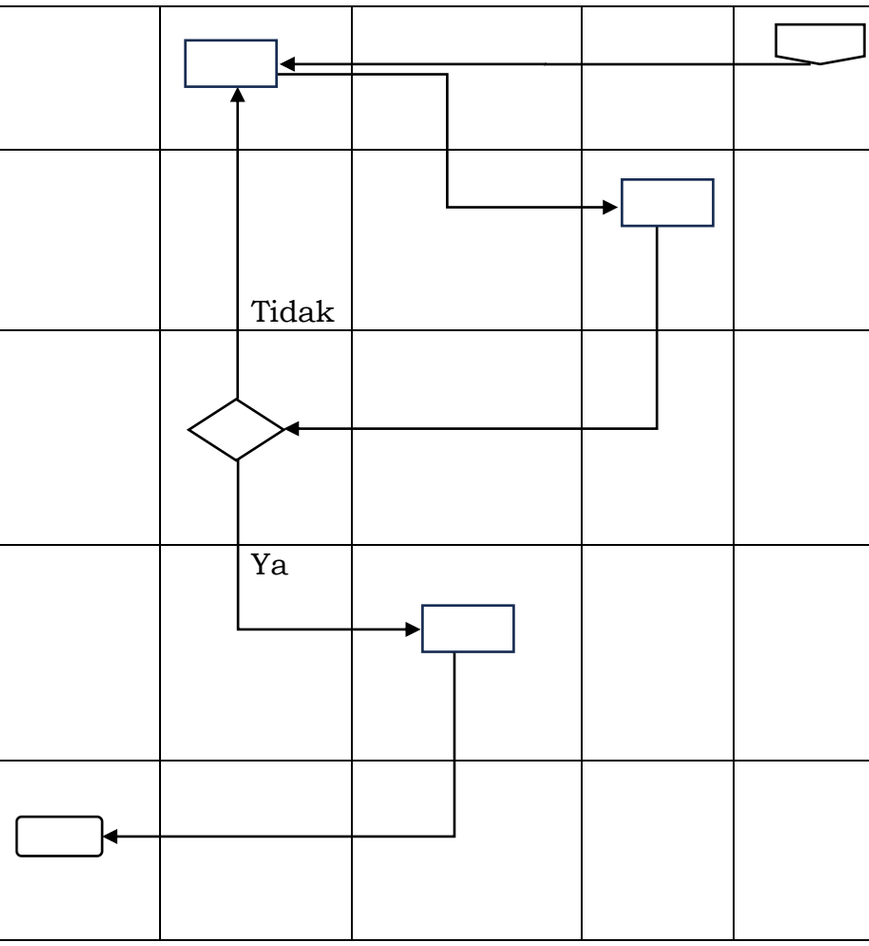
Dengan mencakup kelima aspek ini secara komprehensif, SOP Teknis Keamanan Sistem Penghubung Layanan dapat secara efektif mengurangi risiko keamanan dan memastikan operasional yang aman dan andal.

SOP PROSEDUR SISTEM PENGHUBUNG LAYANAN

<table>
<tr><td colspan="2" rowspan="5">PEMERINTAH
KABUPATEN SITUBONDO
Jl. PB. Sudirman No. 1
SITUBONDO-68312</td><td>NOMOR SOP</td><td>047/SOP.4/431.313.4/2025</td></tr>
<tr><td>TGL PEMBUATAN</td><td>01 September 2025</td></tr>
<tr><td>TGL REVISI</td><td>04-Sep-25</td></tr>
<tr><td>TGL EFEKTIF</td><td>05-Sep-25</td></tr>
<tr><td>NAMA SOP</td><td>Prosedur Sistem Penghubung Layanan</td></tr>
<tr><td colspan="2">DASAR HUKUM</td><td colspan="2">KUALIFIKASI PELAKSANA</td></tr>
<tr><td colspan="2">1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan perubahan Kedua Undang-Undang Nomor 1 Tahun 2024;</td><td colspan="2" rowspan="7">1.Memahami Bahasa Pemrograman
2. Menguasai analisa data
3. Memahami klausul dari standarisasi
4. Memahami proses Bisnis
5. Memahami alur proses
6. Mampu bekerjasama dalam tim
7. Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td colspan="2">2. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik</td></tr>
<tr><td colspan="2">3. Instruksi Presiden Nomor 6 Tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia</td></tr>
<tr><td colspan="2">4. Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan e-Government</td></tr>
<tr><td colspan="2">5. Peraturan Menteri Kominfo Nomor 1 Tahun 2023 tentang Interoperabilitas Data dalam Penyelenggaraan SPBE dan SDI</td></tr>
<tr><td colspan="2">6. Peraturan Bupati Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo</td></tr>
<tr><td colspan="2">KETERKAITAN</td><td colspan="2">PERALATAN/PERLENGKAPAN</td></tr>
<tr><td colspan="2">1. ISO 27001:2022
2. Indeks KAMI versi 5.0
3. SOP Keamanan data dan Informasi</td><td colspan="2">1. Komputer / Laptop
2. Jaringan internet
3. Software untuk pemantauan</td></tr>
<tr><td colspan="2">PERINGATAN</td><td colspan="2">PENCATATAN DAN PENDATAAN</td></tr>
<tr><td colspan="2">Penyediaan Sistem Penghubung Layanan pemerintah mensyaratkan adanya standar interoperabilitas, standar keamanan, dan akses melalui Jaringan Intra pemerintah</td><td colspan="2" rowspan="2">-Pendokumentasian tiap Progress penggunaan SPL
- Memiliki catatan tiap perubahan yang dilakukan dengan integrasi SPL
- Penyimpanan yang bersifat independen</td></tr>
<tr><td colspan="2">Penyediaan Sistem Penghubung Layanan pemerintah ditujukan untuk meningkatkan efisiensi dalam pembangunan dan pengembangan Layanan SPBE dan melakukan integrasi Layanan SPBE.</td></tr>
</table>

Diagram SOP Prosedur Sistem Penghubung Layanan						
No.	Kegiatan	Pelaksana				
		Administrator sistem	Tim Keamanan Informasi	Tim Infrastruktur	Tim Migrasi Data	Pengembang Aplikasi
1	Melakukan Perencanaan Keamanan Migrasi					
2	Melakukan Definisi Kebutuhan keamanan					
3	Menyiapkan Manajemen Kunci					
4	Menerapkan Kriteria Keamanan dalam pengadaan perangkat.					
5	menerapkan Manajemen Konfigurasi Aman (hardening, patch management rutin).					
6	Menerapkan Keamanan Selama Migrasi Data					
7	Menerapkan Keamanan API & Web Service		Tidak			
8	Melakukan Otentikasi & Otorisasi Interoperabilitas					
9	Membanguna manajemen Sesi Aman API		Ya			

10	Melakukan Pemantauan dan Pencatatan					
11	Menjalankan proses Backup dan Pemulihan Bencana		Tidak			
12	melakukan validasi melalui Penghapusan Data Pasca-Migrasi					
13	Memberi Kendali Akses Fisik & Penghapusan Data Aman Perangkat		Ya			
14	Menngelola Sistem penghubung layanan terintegrasi					



Prosedur Sistem Penghubung Layanan			
Mutu Baku			
Kelengkapan	Waktu	Output	Keterangan
Draft Pemanfataan Sistem Penguhubung Layanan	1 Hari	- Assessment Risiko migrasi - Identifikasi Data Sensitif, - penentuan metode migrasi yang paling aman.	Melakukan Pembelajaran mengenai kebutuhan keamanan dalam pemanfaatan sistem penghubung layanan yang di ajukan
- Assessment Risiko migrasi - Identifikasi Data Sensitif, - penentuan metode migrasi yang paling aman.	1 hari	- protokol Enkripsi Data (in-transit dan at-rest) - mekanisme Integritas Data (hashing/tanda tangan digital) -standar Format Data Aman.	Melakukan Penilaian penggunaan Sistem Penghubung Layanan
- protokol Enkripsi Data (in-transit dan at-rest) - mekanisme Integritas Data (hashing/tanda tangan digital) -standar Format Data Aman.	1 Hari	- Prosedur aman untuk pembuatan distribusi, penyimpanan, dan pencabutan kunci enkripsi	menyusun prosedur dalam pemanfaatan sistem penghubung layanan
- Prosedur aman untuk pembuatan distribusi, penyimpanan, dan pencabutan kunci enkripsi	6 jam	Melakukan Device Hardening: nonaktifkan port/layanan tak terpakai, ubah sandi default, terapkan konfigurasi aman.	melakukan identifikasi dan persiapan perangkat dan untuk sistem penghubung layanan
Melakukan Device Hardening: nonaktifkan port/layanan tak terpakai, ubah sandi default, terapkan konfigurasi aman.	6 Jam	- Segmentasi Jaringan untuk mengisolasi sistem. - Manajemen Akses ketat (least privilege)	Melakukan pembangunan segmentasi jaringan dan manajemen akses ketat
- Segmentasi Jaringan untuk mengisolasi sistem. - Manajemen Akses ketat (least privilege)	1 Hari	Prosedur Enkripsi Data Selama Migrasi dan Manajemen Akses Selama Migrasi (kontrol ketat terhadap data/sistem)	menyiapkan enkripsi data untuk imigrasi dan manajemen akses untuk migrasi data

Prosedur Sistem Penghubung Layanan			
Mutu Baku			
Kelengkapan	Waktu	Output	Keterangan
Prosedur Enkripsi Data Selama Migrasi dan Manajemen Akses Selama Migrasi (kontrol ketat terhadap data/sistem)	3 Jam	Terapkan Otentikasi dan Otorisasi API (token, sertifikat). Terapkan Validasi Input dan Pembatasan Tingkat (Rate Limiting). Pastikan Keamanan Transport Layer (HTTPS/TLS) dan Penanganan Kesalahan Aman.	melakukan prosedur penerapan otentikasi dan otorisasi pengunaan sistem penghubung layanan
Terapkan Otentikasi dan Otorisasi API (token, sertifikat). Terapkan Validasi Input dan Pembatasan Tingkat (Rate Limiting). Pastikan Keamanan Transport Layer (HTTPS/TLS) dan Penanganan Kesalahan Aman.	6 jam	Proses untuk memastikan hanya sistem dan pengguna yang berwenang yang dapat mengakses data (token, sertifikat, protokol otentikasi kuat).	menjalankan prosedur verifikasi dalam penerapan otentikasi dan otorisasi pengunaan sistem penghubung layanan
Proses untuk memastikan hanya sistem dan pengguna yang berwenang yang dapat mengakses data (token, sertifikat, protokol otentikasi kuat).	6 Jam	Prosedur untuk sesi aman, penggunaan token berumur pendek, dan pencegahan pembajakan sesi.	menjalankan prosedur token dan pencegahan pembajakan sesi pada penggunaan sistem penghubung layanan
Prosedur untuk sesi aman, penggunaan token berumur pendek, dan pencegahan pembajakan sesi.	1 hari	Prosedur Pemantauan aktivitas sistem integrasi secara terus-menerus dan Pencatatan (Logging) semua peristiwa relevan untuk deteksi anomali.	melakukan pemantauan aktivitas sistem penghubung layanan yang integrasi secara kontinu
Prosedur Pemantauan aktivitas sistem integrasi secara terus-menerus dan Pencatatan (Logging) semua peristiwa relevan untuk deteksi anomali.	1 hari	Prosedur membuat cadangan sistem dan data secara teratur, serta rencana pemulihan bencana jika terjadi insiden keamanan besar.	Melakukan penyusunan prosedur mitigasi
Prosedur membuat cadangan sistem dan data secara teratur, serta rencana pemulihan bencana jika terjadi insiden	3 jam	Validasi Data Pasca-Migrasi (integritas dan kelengkapan). Penghapusan Data Sumber Aman setelah migrasi berhasil dan divalidasi.	menggunakan standar dalam melakukan validasi data

Prosedur Sistem Penghubung Layanan			
Mutu Baku			
Kelengkapan	Waktu	Output	Keterangan
keamanan besar.			
Validasi Data Pasca-Migrasi (integritas dan kelengkapan). Penghapusan Data Sumber Aman setelah migrasi berhasil dan divalidasi.	1 hari	Batasi akses fisik ke perangkat integrator. Prosedur Penghapusan Data Aman dari perangkat integrator sebelum dibuang/digunakan kembali.	membatasi akses fisik
Batasi akses fisik ke perangkat integrator. Prosedur Penghapusan Data Aman dari perangkat integrator sebelum dibuang/digunakan kembali.	6 Jam	persetujuan penyerahan Aplikasi	penyerahan akses aplikasi

H. STANDAR OPERASIONAL PROSEDUR (SOP) KEAMANAN PUSAT DATA PEMERINTAH KABUPATEN SITUBONDO

Penyusunan Standar Operasional Prosedur (SOP) Teknis Keamanan Pusat Data merupakan langkah kritis dalam menjamin keamanan, keandalan, dan keberlanjutan layanan Pusat Data Pemerintah Kabupaten Situbondo. SOP ini menjadi pedoman resmi dalam mengelola risiko keamanan siber dan operasional, serta memastikan bahwa seluruh aktivitas terkait Pusat Data dilaksanakan secara konsisten, terukur, dan sesuai dengan regulasi yang berlaku.

Tujuan Penyusunan SOP Teknis Keamanan Pusat Data adalah:

1. Melindungi Aset Digital Pemerintah
   a. Pusat Data menyimpan informasi sensitif milik pemerintah dan masyarakat, sehingga memerlukan pengamanan fisik dan siber yang ketat untuk mencegah kebocoran, kerusakan, atau akses ilegal.
   b. SOP menjamin bahwa seluruh aspek keamanan telah dipertimbangkan, termasuk pengendalian akses fisik, mitigasi bencana, dan pemulihan data.
2. Memenuhi Regulasi dan Standar Nasional
   a. Pemerintah Indonesia mewajibkan instansi pemerintah untuk menerapkan keamanan TI sesuai Peraturan Menteri Kominfo, Perpres No. 95/2018 tentang SPBE, dan standar ISO 27001 (Manajemen Keamanan Informasi).
   b. SOP membantu Kabupaten Situbondo memenuhi kewajiban hukum dan menghindari sanksi akibat ketidakpatuhan.
3. Mencegah Gangguan Keamanan Siber
   a. Dengan maraknya serangan siber (seperti ransomware, data breach, atau DDoS), SOP menjadi panduan dalam mengantisipasi dan merespons ancaman secara cepat dan terstruktur.
   b. Prosedur yang jelas mengurangi risiko human error dan celah keamanan.
4. Memastikan Ketersediaan Layanan (Availability)
   a. Pusat Data harus beroperasi 24/7 untuk mendukung layanan publik. SOP memuat langkah-langkah pemeliharaan, backup data, dan disaster recovery agar downtime diminimalkan.

Terdapat dua persyaratan utama yang melingkupi penyusunan SOP Teknis Keamanan Pusat Data yaitu:

1. Persyaratan Keamanan Fisik dan Manajemen Pusat Data
   a. Pengamanan Fisik
      1) Kontrol akses ke ruang server (penggunaan kartu akses, biometrik, CCTV, dan logbook).
      2) Proteksi terhadap bencana alam (sistem pemadam kebakaran, pendingin ruangan, dan proteksi anti-gempa).
      3) Pembatasan area kritikal (hanya personel berwenang yang boleh masuk).
   b. Manajemen Pusat Data
      1) Prosedur pemantauan (monitoring) suhu, kelembaban, dan daya listrik.
      2) Kebijakan pemeliharaan rutin (maintenance schedule) untuk server, jaringan, dan perangkat pendukung.
      3) Pelatihan SDM terkait kesadaran keamanan (security awareness) dan tanggap darurat.

2. Persyaratan Koneksi Perangkat ke Pusat Data
   a. Keamanan Jaringan
      1) Enkripsi data (menggunakan VPN, SSL/TLS) untuk transmisi informasi.
      2) Autentikasi kuat (multi-factor authentication) bagi perangkat yang terhubung.
      3) Segmentasi jaringan (misalnya VLAN terpisah untuk layanan internal dan eksternal).
   b. Kontrol Akses Perangkat
      1) Whitelisting perangkat yang diizinkan terkoneksi (MAC address filtering).
      2) Pembaruan berkala (patch management) untuk mencegah eksploitasi kerentanan.
      3) Logging dan audit aktivitas koneksi untuk deteksi anomali.

   Dengan memiliki SOP Teknis Keamanan yang komprehensif, Pemerintah Kabupaten Situbondo dapat Meningkatkan kepercayaan publik terhadap layanan digital pemerintah. Meminimalkan risiko gangguan operasional dan kerugian finansial. Memastikan compliance dengan regulasi dan standar keamanan TI nasional.
   Oleh karena itu, penyusunan SOP ini harus melibatkan tim IT, pihak hukum, dan stakeholder terkait untuk menjamin implementasi yang efektif dan berkelanjutan

SOP PENGELOLAAN KEAMANAN DATA DAN INFORMASI

<table>
<tr><td rowspan="4">PEMERINTAH
KABUPATEN SITUBONDO
Jl. PB. Sudirman No. 1
SITUBONDO-68312</td><td>NOMOR SOP</td><td>: 047/SOP.4/431.313.4/2025</td></tr>
<tr><td>TGL PEMBUATAN</td><td>: 01 September 2025</td></tr>
<tr><td>TGL REVISI</td><td>04-Sep-25</td></tr>
<tr><td>TGL EFEKTIF</td><td>05-Sep-25</td></tr>
<tr><td colspan="2">NAMA SOP</td><td>Pengelolaan Keamanan Data Dan Informasi</td></tr>
<tr><td>DASAR HUKUM</td><td colspan="2">KUALIFIKASI PELAKSANA</td></tr>
<tr><td>1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan perubahan kedua dengan Undang-Undang Nomor 1 Tahun 2024;
2. Undang- Undang Nomor 27 Tahun 2022 tentang Pelindungan Data pribadi;
3. Peraturan Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik:
4. Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 35 Tahun 2012 Tentang pedoman Penyusuan SOP Administrasi Pemerintahan.
5. 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:
6. Peraturan Bupati Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo</td><td colspan="2">1.Memahami Bahasa Pemrograman
2. Menguasai analisa data
3. Memahami klausul dari standarisasi
4. Memahami proses Bisnis
5. Memahami alur proses
6. Mampu bekerjasama dalam tim
7. Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td>KETERKAITAN</td><td colspan="2">PERALATAN/PERLENGKAPAN</td></tr>
<tr><td>1. ISO 27001:2022
2. Indeks KAMI versi 5.0</td><td colspan="2">1. Komputer / Laptop
2. Jaringan internet
3. Software untuk pemantauan</td></tr>
<tr><td>PERINGATAN</td><td colspan="2">PENCATATAN DAN PENDATAAN</td></tr>
<tr><td>Agar dilaksanakan sebagaiman prosedur yang ditetapkan guna menjamin keamanan fisik dan aplikasi yang tercakup di dalam pusat data</td><td colspan="2">- Memiliki catatan tiap Permohonan Akses
- Memiliki catatan tiap aktivitas yang terjadi di dalam pusat data</td></tr>
<tr><td>persyaratan yang diikuti harus sesuai dengan standar yang diikuti guna meminimalisir kemungkinan terjadinya gagal sistem</td><td colspan="2">- Penyimpanan yang bersifat independen dan terbackup</td></tr>
</table>

Diagram SOP pengelolaan keamanan data dan informasi						
No.	Kegiatan	Pelaksana				
		Administrator sistem	Tim Keamanan Informasi	Tim Mitigasi	Tim Infratruktur	Tim Persandian
1	Melakukan Pengendalian Akses					
2	Mengaktifkan Perlindungan					
3	Menyiapkan Manajemen Kunci					
4	Melakukan Monitoring					
5	Menyiapkan protokol Mitigasi Insiden					
6	Melakukan Check setiap prosedur keamanan					
7	Memeverifikasi Kesiapan Protokol Keamanan		Tidak			
8	Melakukan pembukaan akses Pusat Data			Ya		
9	Menerima Akses Pusat Data					

Prosedur Keamanan Pusat Data			
Mutu Baku			Keterangan
Kelengkapan	Waktu	Output	
Permintaan Akses Pusat Data	10 menit	Verifikasi Identitas Pencatatan Akses Biometrik/Kartu	Melakukan penelahaan terhadap kepentingan permintaan Akses
Verifikasi Identitas Pencatatan Akses Biometrik/Kartu	10 menit	- protokol Enkripsi Data (in-transit dan at-rest) - mekanisme Integritas Data (hashing/tanda tangan digital) -standar Format Data Aman.	melakukan pengaktifan prosedur Pengamanan Pusat Data
- protokol Enkripsi Data (in-transit dan at-rest) - mekanisme Integritas Data (hashing/tanda tangan digital) -standar Format Data Aman.	15 menit	- Prosedur aman untuk pembuatan distribusi, penyimpanan, dan pencabutan kunci enkripsi	Menerapkan Manajemen kunci pengamanan pusat data
- Prosedur aman untuk pembuatan distribusi, penyimpanan, dan pencabutan kunci enkripsi	20 menit	catatan log ini, akses fisik,terapkan konfigurasi aman.	Melakukan Pencatatan Aktifitas Akses Pusat Data
catatan log ini, akses fisik,terapkan konfigurasi aman.	10 menit	- Sistem Backup diaktifkan. - Device Backup	Mengaktifkan Sistem Backup, Menyiapkan Perangkat pengamanan
- Sistem Backup diaktifkan. - Device Backup	15 menit	Check List Prosedur terhadap data/sistem	melakukan pemantauan prosedur pengamanan pusat data
Check List Prosedur terhadap data/sistem	15 menit	Persetujuan Pemberian akes	memberikan persetujuan akses pusat data
Persetujuan Pemberian akes	10 menit	token, sertifikat, protokol otentikasi kuat.	menerbitkan kunci token, sertifikat, protokol
token, sertifikat, protokol otentikasi kuat.	5 menit	persetujuanAkses Pusat Data	Memberikan Akses Pusat data

I. STANDAR OPERASIONAL PROSEDUR (SOP) KEAMANAN JARINGAN INTRA

Penyusunan Standar Operasional Prosedur (SOP) Keamanan Jaringan Intra untuk Pemerintah Kabupaten Situbondo adalah hal krusial. Lampiran regulasi ini memastikan bahwa Jaringan Intra terlindungi dari berbagai ancaman, baik dari internal maupun eksternal. SOP ini mencakup beberapa aspek penting untuk menciptakan ekosistem jaringan yang aman dan andal.

Aspek Administrasi Keamanan Jaringan Intra. Aspek ini adalah fondasi dari seluruh kebijakan keamanan jaringan. Lampiran regulasi akan mengatur hal-hal berikut:

1. Kebijakan Keamanan: Menentukan aturan main yang jelas tentang bagaimana keamanan Jaringan Intra harus dikelola, termasuk tanggung jawab personel, prosedur penanganan insiden, dan penegakan kebijakan. Ini menjadi payung hukum dan etika bagi semua pengguna dan administrator.
2. Manajemen Risiko: Mengidentifikasi potensi ancaman dan kerentanan pada Jaringan Intra, serta merumuskan strategi mitigasi untuk mengurangi risiko tersebut. Ini melibatkan penilaian rutin untuk mengidentifikasi celah keamanan baru.
3. Pelatihan dan Kesadaran Keamanan: Mewajibkan pelatihan rutin bagi seluruh pegawai mengenai praktik keamanan siber terbaik, seperti pentingnya kata sandi yang kuat, identifikasi phishing, dan cara melaporkan insiden keamanan. Kesadaran pengguna adalah garis pertahanan pertama yang vital.
4. Audit dan Pemantauan: Menetapkan jadwal dan metode untuk melakukan audit keamanan secara berkala, serta sistem pemantauan untuk mendeteksi aktivitas mencurigakan atau pelanggaran kebijakan. Ini memastikan kepatuhan dan efektivitas langkah-langkah keamanan.

Kontrol Akses dan Autentikasi Ini adalah inti dari perlindungan data dan sistem. Lampiran regulasi akan memastikan:

1. Identifikasi dan Otentikasi Pengguna: Mengharuskan penggunaan username dan password yang kuat, serta mendorong implementasi otentikasi multi-faktor (MFA) untuk semua akses ke Jaringan Intra. Ini mencegah akses tidak sah bahkan jika kata sandi bocor.
2. Otorisasi Berbasis Peran: Mengatur hak akses pengguna berdasarkan peran dan kebutuhan kerja mereka (prinsip least privilege). Misalnya, staf administrasi hanya dapat mengakses data administrasi, bukan data keuangan. Ini membatasi kerusakan jika sebuah akun disusupi.
3. Manajemen Akun: Prosedur untuk pembuatan, modifikasi, penonaktifan, dan penghapusan akun pengguna harus jelas dan teratur. Akun yang tidak aktif harus segera dinonaktifkan untuk mencegah penyalahgunaan.
4. Kontrol Akses Jaringan: Menerapkan segmentasi jaringan (network segmentation) untuk memisahkan berbagai departemen atau fungsi, sehingga membatasi penyebaran ancaman jika satu segmen dikompromikan.

Persyaratan Perangkat dan Aplikasi Keamanan Jaringan Intra
Bagian ini berfokus pada alat-alat teknis yang melindungi jaringan. Lampiran regulasi akan mencakup:

1. Firewall: Mewajibkan penggunaan firewall yang dikonfigurasi dengan baik untuk mengontrol lalu lintas masuk dan keluar dari Jaringan Intra, memblokir akses yang tidak sah dan serangan siber.
2. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS): Menginstal dan memelihara sistem yang dapat mendeteksi dan secara otomatis memblokir aktivitas mencurigakan atau serangan yang sedang berlangsung di jaringan.
3. Anti-Malware dan Antivirus: Mengharuskan instalasi dan pembaruan rutin perangkat lunak anti-malware pada semua perangkat yang terhubung ke Jaringan Intra untuk melindungi dari virus, ransomware, dan jenis malware lainnya.
4. Enkripsi Data: Mewajibkan penggunaan enkripsi untuk melindungi data sensitif saat transit maupun saat disimpan dalam jaringan.
5. Manajemen Patch dan Pembaruan: Prosedur untuk memastikan semua perangkat keras dan perangkat lunak di Jaringan Intra selalu diperbarui dengan patch keamanan terbaru untuk menutup kerentanan yang diketahui.

Kontrol Keamanan Gateway
Gateway adalah pintu gerbang utama ke Jaringan Intra, sehingga pengamanannya sangat penting. Lampiran regulasi akan mengatur:

1. Filter Konten: Menerapkan filter web dan email di gateway untuk memblokir akses ke situs web berbahaya, phishing, dan spam yang dapat menjadi sumber serangan.
2. VPN (Virtual Private Network): Mengatur penggunaan VPN untuk akses jarak jauh yang aman ke Jaringan Intra, memastikan bahwa koneksi terenkripsi dan terotentikasi.
3. Load Balancing dan Redundansi: Mengatur konfigurasi gateway agar memiliki redundansi dan load balancing untuk memastikan ketersediaan layanan yang tinggi dan ketahanan terhadap serangan DDoS (Distributed Denial of Service).

Kontrol Keamanan Access Point pada Jaringan Nirkabel
Jaringan nirkabel (Wi-Fi) seringkali menjadi titik masuk yang rentan. Lampiran regulasi akan menekankan:

1. Pemisahan Jaringan (VLAN): Mengharuskan penggunaan Virtual Local Area Network (VLAN) untuk memisahkan jaringan nirkabel publik dari jaringan internal yang sensitif.
2. WPA3 Encryption: Mewajibkan penggunaan standar enkripsi terbaru seperti WPA3 untuk mengamankan koneksi nirkabel dan mencegah eavesdropping atau penyadapan data.
3. Strong Password for Wi-Fi: Mengatur kebijakan kata sandi yang kuat untuk jaringan nirkabel, yang sulit ditebak dan sering diubah.
4. Guest Network Isolation: Menyediakan jaringan tamu yang terpisah dan terisolasi dari Jaringan Intra utama untuk pengunjung, membatasi akses mereka hanya ke internet.

Kontrol Konfigurasi Access Point pada Jaringan Nirkabel

Konfigurasi yang tepat adalah kunci untuk keamanan access point. Lampiran regulasi akan mencakup:

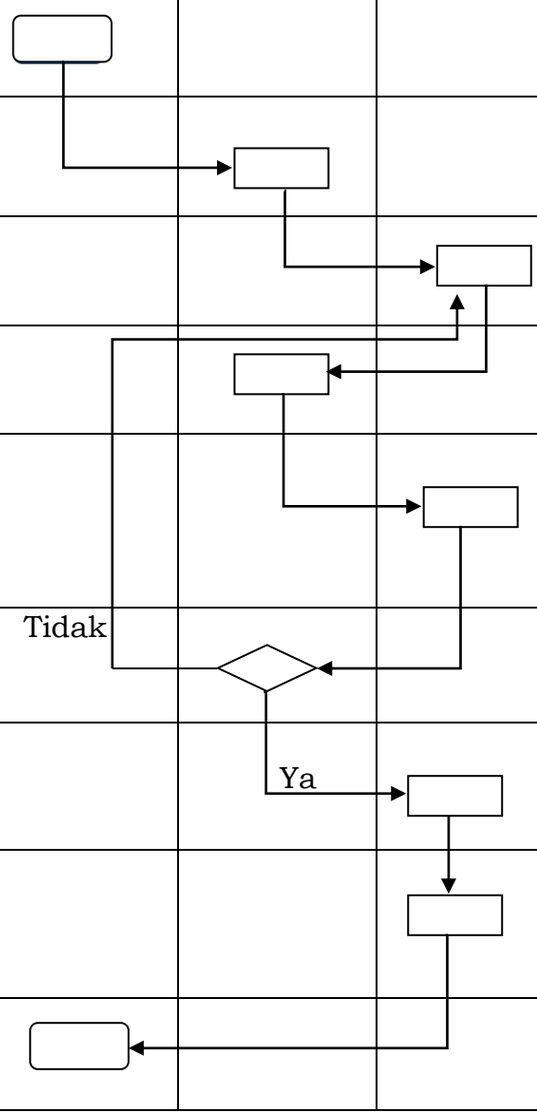
- Penonaktifan SSID Broadcast: Menganjurkan untuk menonaktifkan penyiaran SSID (*Service Set Identifier*) agar nama jaringan tidak terlihat secara publik, meskipun ini bukan satu-satunya lapisan keamanan.
- Penggunaan MAC Filtering: Menerapkan *MAC filtering* untuk membatasi perangkat yang dapat terhubung ke *access point* berdasarkan alamat MAC mereka, meskipun ini dapat diakali.
- Perubahan Kata Sandi Default: Mewajibkan perubahan kata sandi *default* pada semua *access point* segera setelah instalasi untuk mencegah akses tidak sah oleh pihak ketiga.
- Pemantauan dan Logging: Mengatur pemantauan log aktivitas *access point* secara berkala untuk mendeteksi anomali atau upaya intrusi.

Dengan terpenuhinya semua aspek di atas, Standar Operasional Prosedur Keamanan Jaringan Intra akan menjadi pedoman komprehensif yang melindungi Jaringan Intra Pemerintah Kabupaten Situbondo dari berbagai ancaman siber dan memastikan operasional yang aman dan efisien

SOP PENGELOLAAN KEAMANAN JARINGAN INTRA

<table>
<tr><td colspan="2" rowspan="4">PEMERINTAH
KABUPATEN SITUBONDO
Jl. PB. Sudirman No. 1
SITUBONDO-68312</td><td>NOMOR SOP</td><td>: 047/SOP.4/431.313.4/2025</td></tr>
<tr><td>TGL PEMBUATAN</td><td>: 01 September 2025</td></tr>
<tr><td>TGL REVISI</td><td>04-Sep-25</td></tr>
<tr><td>TGL EFEKTIF</td><td>05-Sep-25</td></tr>
<tr><td colspan="2">NAMA SOP</td><td>Pengelolaan Keamanan Jaringan Intra</td></tr>
<tr><td colspan="2">DASAR HUKUM</td><td>KUALIFIKASI PELAKSANA</td></tr>
<tr><td colspan="2">1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan perubahan kedua dengan Undang-Undang Nomor 1 Tahun 2024;</td><td rowspan="4">1. Menguasai analisa data
2. Memahami klausul dari standarisasi
3. Memahami proses Bisnis
4. Memahami alur proses
5. Mampu bekerjasama dalam tim
6. Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td colspan="2">2. Peraturan Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik:</td></tr>
<tr><td colspan="2">3. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi</td></tr>
<tr><td colspan="2">4. 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:</td></tr>
<tr><td colspan="2">5. Peraturan Bupati Nomor 18 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Situbondo</td><td></td></tr>
<tr><td colspan="2">KETERKAITAN</td><td>PERALATAN/PERLENGKAPAN</td></tr>
<tr><td colspan="2">1. ISO 27001:2022
2. Indeks KAMI versi 5.0
3. SOP Pengamanan data dan Informasi</td><td>1. Komputer / Laptop
2. Jaringan internet
3. Software untuk pemantauan</td></tr>
<tr><td colspan="2">PERINGATAN</td><td>PENCATATAN DAN PENDATAAN</td></tr>
<tr><td colspan="2">Wajib Mengikuti prosedur yang ditetapkan guna menjamin keamanan jaringan intra antar OPD</td><td>- Memiliki catatan secara berkala guna memantau perubahan
- memiliki catatan kondisi awal pengaktifan jaringan intar</td></tr>
<tr><td colspan="2">Perlu dilakukan pemantauan secara berkala untuk mendapatkan data guna menganlisa kemungkinan terjadinya anomali maupun penyusupan dan percobaan penyerangan yang berpotensi membuat jaringan terputus</td><td>- Memiliki catatan tiap pengguna jaringan intar
- Memiliki catatan mengenai trafik penggunaan jaringan intra</td></tr>
</table>

Diagram SOP Pengelolaan Keamanan Jaringan Intra				
No.	Kegiatan	Pelaksana		
		Administrator sistem	Tim Keamanan Informasi	Tim Infrastruktur
1	Melakukan perumusan prosedur keamanan Jaringan Intra			
2	Melakukan Definisi Kebutuhan keamanan			
3	Mengidentifikasi aset jaringan			
4	Menetapkan Kriteria Keamanan dalam pengadaan perangkat.			
5	menerapkan Manajemen Konfigurasi Aman (hardening, patch management rutin).			
6	Melakukan Otentikasi & Otorisasi	Tidak		
7	Melakukan Pemantauan dan Pencatatan		Ya	
8	Memberi Kendali Akses Fisik & Penghapusan Data Aman Perangkat			
9	Menngelola Sistem penghubung layanan terintegrasi			



Prosedur Keamanan Jaringan Intra			
Mutu Baku			Keterangan
Kelengkapan	Waktu	Output	
Draft Pemanfataan Sistem Penguhubung Layanan	1 Hari	- Assessment Risiko migrasi - Identifikasi Data Sensitif, - penentuan metode migrasi yang paling aman.	Melakukan Perumusan prosedur keamanan jaringan denga identifikasi kebutuhan, sifat data yang berjalan diatasnya, pemetaan terhadap posisi jaringan intra
- Assessment Risiko migrasi - Identifikasi Data Sensitif, - penentuan metode migrasi yang paling aman.	1 hari	- protokol Enkripsi Data (in-transit dan at-rest) - mekanisme Integritas Data (hashing/tanda tangan digital) -standar Format Data Aman.	Melakukan Asesmen Risiko migrasi guna menangani kegagalan jaringan, mengidentifikasi tiap paket data yang berjalan
- protokol Enkripsi Data (in-transit dan at-rest) - mekanisme Integritas Data (hashing/tanda tangan digital) -standar Format Data Aman.	1 Hari	- Prosedur aman untuk pembuatan distribusi, penyimpanan, dan pencabutan kunci enkripsi	melakukan penyiapan protokol untuk enkripsi data dan mengaktifkan mekanisme integritas data
- Prosedur aman untuk pembuatan distribusi, penyimpanan, dan pencabutan kunci enkripsi	6 jam	Melakukan Device Hardening: nonaktifkan port/layanan tak terpakai, ubah sandi default, terapkan konfigurasi aman.	menetukan prosedur aman guna memetakan distribusi, penyimpanan data dan pencabutan kunci enkripsi data
Melakukan Device Hardening: nonaktifkan port/layanan tak terpakai, ubah sandi default, terapkan konfigurasi aman.	6 Jam	- Segmentasi Jaringan untuk mengisolasi sistem. - Manajemen Akses ketat (least privilege)	melakukan skema pencegaran dengan melakukan nonkatifkan port yang tidak digunakan, memastikan perubahan sandi default dan menerapkan knfigurasi jaringan dengan tingkat keamanan tinggi
Terapkan Otentikasi dan Otorisasi API (token, sertifikat). Terapkan Validasi Input dan Pembatasan Tingkat (Rate Limiting). Pastikan Keamanan Transport Layer (HTTPS/TLS) dan Penanganan Kesalahan Aman.	6 jam	Proses untuk memastikan hanya sistem dan pengguna yang berwenang yang dapat mengakses data (token, sertifikat, protokol otentikasi kuat).	melakukan otentikasi dan otorisai pengguna jaringan intra dan pembatasan besaran data yang berjalan

Prosedur Keamanan Jaringan Intra			
Mutu Baku			Keterangan
Kelengkapan	Waktu	Output	
Prosedur untuk sesi aman, penggunaan token berumur pendek, dan pencegahan pembajakan sesi.	1 hari	Prosedur Pemantauan aktivitas sistem integrasi secara terus-menerus dan Pencatatan (Logging) semua peristiwa relevan untuk deteksi anomali.	menggunak prosedur untuk sesi aman dengan menggunakan token yang berjangka waktu pendek dan mencegah adanya pembajakn sesi melalui pemantauan durasi sesi
Validasi Data Pasca-Migrasi (integritas dan kelengkapan). Penghapusan Data Sumber Aman setelah migrasi berhasil dan divalidasi.	1 hari	Batasi akses fisik ke perangkat integrator. Prosedur Penghapusan Data Aman dari perangkat integrator sebelum dibuang/digunakan kembali.	Melakukan pembatasan akses fisik kepada perangkat yang terintegrasi dan melakukan pengahpusan data keamanan dari perangkat integrator secara berkala
Batasi akses fisik ke perangkat integrator. Prosedur Penghapusan Data Aman dari perangkat integrator sebelum dibuang/digunakan kembali.	6 Jam	persetujuan pemanfaaatan jaringan intra	akses untuk menggunakan jaringan Intra

BUPATI SITUBONDO,

ttd.

YUSUF RIO WAHYU PRAYOGO