WALI KOTA PARIAMAN
PROVINSI SUMATERA BARAT

KEPUTUSAN WALI KOTA PARIAMAN
NOMOR 241 / 500.12/2025
TENTANG
PEDOMAN PEMBANGUNAN/PENGEMBANGAN/PEMELIHARAAN APLIKASI DAN SISTEM INFORMASI

WALI KOTA PARIAMAN,

Menimbang : a. bahwa dalam rangka meningkatkan kualitas pelayanan publik melalui pemanfaatan teknologi informasi dan komunikasi, diperlukan pembangunan, pengembangan, dan pemeliharaan aplikasi dan sistem informasi yang andal, efisien, berkelanjutan, dan untuk mendukung implementasi Sistem Pemerintahan Berbasis Elektronik yang optimal, perlu disusun pedoman pembangunan, pengembangan, dan pemeliharaan aplikasi dan sistem informasi di lingkungan Pemerintah Kota Pariaman;

b. bahwa berdasarkan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, setiap instansi pemerintah wajib menerapkan teknologi informasi secara terpadu dan terstandar;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan b, perlu menetapkan Keputusan Wali Kota tentang Pedoman Pembangunan/Pengembangan/ Pemeliharaan Aplikasi dan Sistem Informasi;

Mengingat : a. Undang-Undang Nomor 12 Tahun 2002 tentang Pembentukan Kota Pariaman di Provinsi Sumatera Barat (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 418);

b. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 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);

c. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

d. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan

Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

e. Peraturan Wali Kota Pariaman Nomor 23 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik.

MEMUTUSKAN:

Menetapkan : KEPUTUSAN WALI KOTA PARIAMAN TENTANG PEDOMAN PEMBANGUNAN/ PENGEMBANGAN/ PEMELIHARAAN APLIKASI DAN SISTEM INFORMASI.

KESATU : Pedoman Pembangunan/Pengembangan/Pemeliharaan Aplikasi dan Sistem Informasi tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Pedoman Pembangunan/Pengembangan/Pemeliharaan Aplikasi dan Sistem Informasi sebagai acuan dalam penyelenggaraan tata kelola teknologi informasi dan komunikasi di lingkungan Pemerintah Kota Pariaman.

KETIGA : Pedoman ini digunakan sebagai acuan bagi seluruh perangkat daerah di lingkungan Pemerintah Kota Pariaman dalam merencanakan, membangun, mengembangkan, dan memelihara aplikasi dan sistem informasi secara efektif, efisien, terintegrasi, dan aman.

KEEMPAT : Dalam pelaksanaannya, seluruh perangkat daerah wajib mematuhi standar teknis, prosedur, dan tahapan sebagaimana diatur dalam pedoman ini guna menjamin kualitas dan keamanan aplikasi/sistem informasi.

KELIMA : Penanggung jawab pelaksanaan pembangunan, pengembangan, dan pemeliharaan aplikasi dan sistem informasi berada pada masing-masing Perangkat Daerah, dan dikoordinasikan oleh Dinas Komunikasi dan Informatika Kota Pariaman.

KEENAM : Pendanaan atas pelaksanaan Keputusan ini bersumber dari Anggaran Pendapatan dan Belanja Daerah Pemerintah Kota Pariaman sesuai ketentuan peraturan perundang-undangan.

KETUJUH : Keputusan Wali Kota ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Pariaman
pada tanggal 7 Agustus 2025

WALI KOTA PARIAMAN,

YOTA BALAD

PARAF KOORDINASI

SEKRETARIS DAERAH	
KEPALA DINAS KOMUNIKASI DAN INFORMATIKA	
KEPALA BADAN KESATUAN BANGSA DAN POLITIK	
KEPALA BAGIAN HUKUM	
KEPALA BAGIAN PERATURAN PERUNDANG UNDANGAN	

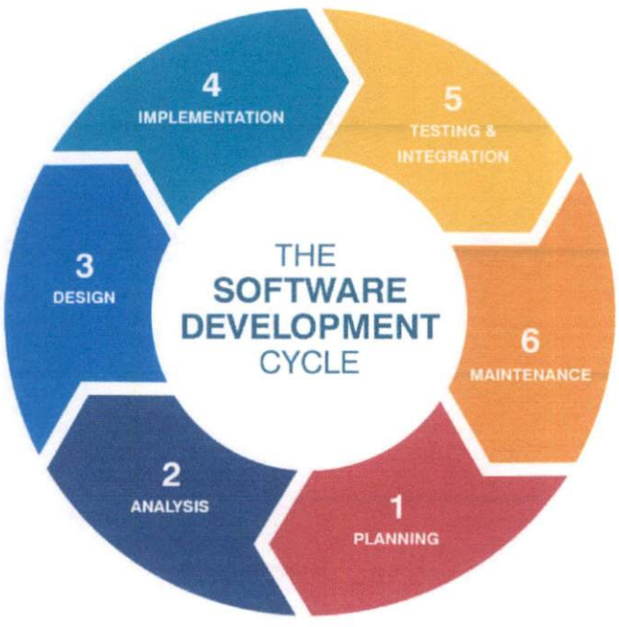
LAMPIRAN
KEPUTUSAN WALI KOTA PARIAMAN
NOMOR 241 /500.12/2025
TENTANG
PANDUAN PEMBANGUNAN/ PENGEMBANGAN/ PEMELIHARAAN APLIKASI DAN SISTEM INFORMASI

PEDOMAN PEMBANGUNAN/PENGEMBANGAN/PEMELIHARAAN APLIKASI DAN SISTEM INFORMASI

A. DOKUMEN TATA KELOLA

1. KERANGKA ACUAN KERJA (KAK)
   Di dalam KAK Pembangunan/pengembangan/pemeliharaan Aplikasi, pada pasal spesifikasi teknis Aplikasi dan Sistem Informasi berpedoman pada standarisasi aplikasi dan Sistem Informasi yang ditetapkan oleh Sekretaris Daerah Kota Pariaman.

2. LAPORAN AWAL
   Laporan awal menjelaskan rencana pengembangan aplikasi berbasis teori dan metodologi SDLC (*System Development Life Cycle*), serta identifikasi kebutuhan pengguna dan studi awal sistem yang sedang berjalan. SDLC (Software Development Life Cycle) adalah suatu pendekatan yang terstruktur untuk merencanakan, mengembangkan, menguji, dan memelihara sistem perangkat lunak. SDLC memberikan panduan untuk tim pengembangan perangkat lunak agar proses pembuatan perangkat lunak menjadi lebih efisien dan terorganisir. Tahapan SLDC dapat dilihat pada Gambar 1 berikut.



Gambar 1. Tahapan SLDC

a. Perencanaan (Planning)
   1) Pada tahap ini, tujuan dari proyek perangkat lunak ditentukan, serta kebutuhan dan ekspektasi dari pengguna atau stakeholder. Tim pengembang melakukan analisis untuk memahami apa yang diinginkan oleh klien atau pengguna akhir, serta menentukan batasan-batasan teknis dan anggaran yang ada.
   2) Output: Dokumen spesifikasi proyek dan rencana pengembangan.
b. Analisis Kebutuhan (Feasibility Study & Requirement Analysis)
   1) Tahap ini melibatkan pengumpulan kebutuhan dari stakeholder dan mendokumentasikan fitur serta fungsi yang diinginkan dalam sistem perangkat lunak.
   2) Analisis dilakukan untuk memastikan apakah proyek ini dapat dilaksanakan dari segi teknis, ekonomi, dan hukum.
   3) Output: Dokumen spesifikasi kebutuhan perangkat lunak (SoftwareRequirements Specification/SRS).
c. Desain Sistem (System Design)
   1) Desain arsitektur perangkat lunak dan desain sistem dilakukan untuk memenuhi persyaratan yang telah ditentukan sebelumnya. Proses ini mencakup desain antarmuka pengguna (UI), desain database, dan desain fungsionalitas.
   2) Output: Dokumen desain sistem, desain teknis, dan spesifikasi antarmuka.
d. Pengembangan (Implementation)
   1) Pada tahap ini, pengembang mulai menulis kode perangkat lunak berdasarkan desain yang telah dibuat sebelumnya. Kode ditulis dalam bahasa pemrograman yang sesuai dan pengujian awal dilakukan untuk memastikan bahwa kode berfungsi sesuai dengan spesifikasi.
   2) Output: Kode sumber perangkat lunak.
e. Pengujian dan Integrasi (Testing & Integration)
   1) Setelah perangkat lunak selesai dikembangkan, tahap pengujian dilakukan untuk memastikan kualitasnya. Pengujian dapat mencakup uji unit (untuk fungsi individu), uji integrasi (untuk memastikan bahwa bagian-bagian perangkat lunak bekerja bersama-sama dengan baik), serta uji sistem dan uji penerimaan pengguna.
   2) Output: Laporan hasil pengujian, perbaikan bug, dan pembaruan perangkat lunak.
f. Pemeliharaan (Maintenance)
   1) Setelah perangkat lunak diimplementasikan, tahap pemeliharaan dimulai. Pemeliharaan mencakup perbaikan bug, pembaruan untuk meningkatkan kinerja, dan menambahkan fitur tambahan sesuai dengan kebutuhan pengguna.
   2) Output: Pembaruan perangkat lunak dan dokumentasi.

Laporan awal minimal harus memenuhi hal-hal sebagai berikut:
BAB I (Pendahuluan)
a. Latar Belakang Pembangunan Aplikasi dan Sistem Informasi.
b. Teori rencana pengembangan aplikasi menggunakan *Sistem Development Life Cycle.*

BAB II (Ruang Lingkup/ *Planning*)

a. Identifying Bussiness Value terdiri atas: *System Request* (Kebutuhan Sistem) berisi analisa kebutuhan yang akan dibangun/dikembangkan sesuai dengan tujuan layanan aplikasi, urusan dan kewenangan yang diampu oleh Perangkat Daerah.
b. Organizational Feasibility: Analisis kebutuhan organisasi yang mencakup penjelasan tentang dukungan aplikasi tersebut terhadap pencapaian visi dan misi Kota Pariaman, kesesuaian dengan renstra dan Indikator Kinerja Individu Kepala Dinas, keselarasan proses bisnis aplikasi dengan proses bisnis unit kerja, maksud dan tujuan pembangunan/pengembangan/pemeliharaan aplikasi, pemangku kepentingan yang terlibat, identifikasi pengguna akhir (*end user*), efisiensi dan efektifitas yang dapat dicapai dan keuntungan (*profit*) yang dapat diperoleh (jika ada).
c. Bussiness Process Indentification: Identifikasi proses bisnis aplikasi dituangkan dalam bentuk *Use Case Diagram*.

BAB III (Pembahasan)
a. Bussiness Process Modelling Model: Proses bisnis dituangkan dalam bentuk alur/flowchart/gambar yang menggambarkan seluruh alur pada aplikasi.
b. Bisnis Proses Realization: Realisasi proses bisnis dituangkan dalam bentuk Diagram Aktifitas (Activity Diagram). Digambarkan dari setiap tahapan atau aktifitas pada aplikasi.
c. Desain awal tampilan aplikasi: Gambaran desain setiap halaman dari aplikasi.
d. Desain Tampilan Keluaran Produk Aplikasi: Gambaran desain hasil keluaran dari aplikasi.

BAB IV Timeline
Berisi rencana jadwal, jangka waktu pelaksanan tahapan pekerjaan, jumlah tenaga ahli dan peralatan yang dibutuhkan.

3. SURAT KEPUTUSAN/ SURAT PERINTAH TIM PENGELOLA APLIKASI
Surat Keputusan atau Surat Perintah yang diterbitkan oleh pemilik aplikasi yang menyatakan struktur tim serta tugas dan kewenangan tim pengelola aplikasi. Apabila pengguna lintas Perangkat Daerah, Surat Keputusan atau Surat Perintah diterbitkan oleh Sekretaris Daerah selaku Ketua Tim Koordinasi SPBE.

4. SURAT KEPUTUSAN/ SURAT PERINTAH TIM HELPDESK APLIKASI
Surat Keputusan atau Surat Perintah yang diterbitkan oleh pemilik aplikasi untuk menentukan narahubung serta menyatakan tugas dan kewenangan narahubung aplikasi tersebut.

5. LAPORAN AKHIR
Laporan akhir berisi pendokumentasian tahapan design dan implementasi pembangunan/pengembangan/pemeliharaan aplikasi. Sekurang-kurangnya harus memenuhi hal-hal sebagai berikut:
a. Program Design : desain dan rancangan program aplikasi
   1) Use Case Diagram adalah pemodelan untuk perilaku sistem informasi yang akan dibuat. Use case diagram fokus dalam mendeskripsikan interaksi/hubungan antara aktor dengan sistem informasi yang akan dibuat.

2) Class diagram adalah diagram yang mengambarkan pembagian dan relasi/hubungan antar kelas–kelas dalam sistem informasi yang akan dibuat. Class Diagram akan menghasilkan sebuah objek dan merupakan inti dari pengembangan dan desain berorientasi objek.
3) Activity diagram mengambarkan alur aktivitas yang akan dilakukan aktor dalam sistem informasi yang akan dibuat. Activity diagram berfungsi untuk mengambarkan aliran kerja dari sistem informasi
4) Sequence diagram menggambarkan kelakuan objek yang ada pada use case diagram dengan mendeskripsikan waktu hidup /lifeline objek dan message yang akan dikirimkan dan diterima antar objek
5) User Interface Design (Desain Antarmuka Pengguna atau rekayasa antarmuka pengguna) adalah desain untuk komputer, peralatan, mesin, perangkat komunikasi mobile, aplikasi perangkat lunak,dan situs web yang berfokus pada pengalaman pengguna dan interaksi. Ditampilkan setiap halaman pada aplikasi.

b. Implementation (implementasi) adalah tahap dimana rencana atau desain diwujudkan menjadi tindakan konkrit atau produk akhir.
   1) Software Construction: Spesifikasi teknis aplikasi yang mencantumkan versi dari Framework, bahasa pemrograman, database, aplikasi webserver, dll.
   2) Struktur Database (struktur basis data).
   3) Software Testing: Software testing dilakukan untuk pengujian semua tahapan atau fungsi pada aplikasi berjalan dengan baik. Pengujian aplikasi dapat menggunakan metode BlackBox Testing.
   4) Spesifikasi Kebutuhan Server terdiri dari kebutuhan atas :
      i. Processor
      ii. RAM
      iii. Storage

6. STANDAR OPERASIONAL PROSEDUR (SOP)
   SOP penggunaan aplikasi dibuat untuk masing-masing user level manajemen.

7. BUKU PANDUAN PENGELOLAAN APLIKASI
   Panduan penggunaan aplikasi dibuat meliputi semua menu yang ada pada aplikasi.

8. VIDEO TUTORIAL PENGGUNAAN APLIKASI
   Apabila aplikasi digunakan oleh lebih dari 1 (satu) perangkat daerah dan atau masyarakat umum, disarankan ada video panduan.

9. PANDUAN INSTALASI APLIKASI DI SERVER
   Berisi buku panduan instalasi dan konfigurasi aplikasi di server linux.

10. DOKUMEN MANAJEMEN RISIKO
    Buat dokumen manajemen risiko aplikasi dan rencana tindak pengendalian risiko-risiko tersebut untuk menjamin keberlangsungan layanan

11. DOKUMEN API
    Diberikan apabila semua prosedur sdh selesai dan sesuai standar.

12. SOURCE CODE
    Diserahkan setelah semua tahapan asesmen dilalui dan aplikasi dinyatakan lulus asesmen. Dikirimkan dalam bentuk *softcopy*.

B. STANDAR KEAMANAN INFORMASI
Standar keamanan informasi yang diterapkan berpedoman pada 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.

1. Otentikasi
   Otentikasi adalah tindakan menetapkan, atau mengkonfirmasi, seseorang (atau sesuatu) sebagai otentik dan bahwa klaim yang dibuat oleh seseorang atau tentang perangkat adalah benar, tahan terhadap peniruan identitas, dan mencegah pemulihan atau intersepsi kata sandi.
   Ketentuan keamanan kata sandi sebagai berikut :
   a. Jika pengguna aplikasi lebih dari satu Perangkat Daerah dan atau Publik, Pendaftaran akun menggunakan email aktif dan menggunakan verifikasi email.
   b. Verifikasi bahwa kata sandi yang ditetapkan pengguna memiliki Panjang minimal 8 karakter, kombinasi antara huruf kecil, huruf besar, angka, dan special karakter (*symbol*). Dilakukan validasi dari sistem jika format tidak sesuai maka tidak bisa diproses. Berlaku untuk pembuatan maupun perubahan kata sandi. Ditambahkan keterangan persyaratan kata sandi pada kolom input kata sandi.
   c. Pastikan terdapat menu ubah kata sandi, yang mewajibkan memasukan kata sandi pengguna saat ini pada proses perubahan kata sandi.
   d. Menyediakan pengukur kekuatan kata sandi pada aplikasi untuk membantu pengguna dalam membuat kata sandi yang kuat.
   e. Menyediakan fitur lihat sementara kata sandi pengguna untuk membantu pengguna dalam memasukan kata sandi.
   f. Mengatur mekanisme pemulihan atau reset kata sandi pengguna. Pemulihan atau reset kata sandi wajib dilakukan mandiri oleh pengguna.
   g. Mengatur masa berlaku kata sandi selama 1 tahun. Jika masa berlaku berakhir pengguna diwajibkan untuk merubah kata sandi.
   h. Jika akun penguna dibuat oleh pengembang / Admin aplikasi, maka pengguna wajib merubah kata sandi saat pertama kali masuk kedalam aplikasi.
   i. Mengatur jumlah salah input kata sandi, batas maksimal 5 kali, pengguna akan tertahan dan bisa input kata sandi kembali setelah 3 menit.
   j. Penggunaan kata sandi bertingkat diwajibkan bagi aplikasi yang menurut hasil penilaian Tim Asesmen merupakan aplikasi yang mengelola data penting dan sangat rahasia.
   k. Menjaga kerahasiaan kata sandi yang disimpan pada database melalui mekanisme kriptografi satu arah.

l. Menggunakan jalur komunikasi yang diamankan untuk proses autentikasi pada server.
m. Penerapan kata sandi sesuai syarat diatas juga termasuk untuk kata sandi pada server.
n. Pastikan akun default pada server dirubah (contoh: *root*)
o. Menyediakan *Captcha* atau oprasi hitung pada halaman login dan pendaftaran.
p. Menyediakan checklist box pernyataan atas kebenaran data yang diberikan pada halaman pendaftaran.

2. Manajemen Sesi
Salah satu komponen inti dari setiap aplikasi berbasis web atau API stateful adalah mekanisme yang digunakan untuk mengontrol dan mempertahankan status untuk pengguna atau perangkat yang berinteraksi dengannya. Manajemen sesi mengubah protokol stateless menjadi stateful, yang sangat penting untuk membedakan pengguna atau perangkat yang berbeda. Ketentuan Keamanan Manajemen Sesi Dasar adalah sebagai berikut:
a. Pastikan aplikasi tidak pernah mengungkapkan token sesi dalam parameter URL.
b. Memanfaatkan pengendali sesi yang disediakan oleh framework aplikasi.
c. Atur pengendali waktu habis sesi (auto logout) minimal 10 menit dan maksimal 15 menit.
b. Pastikan bahwa logout dan kadaluwarsa membatalkan token sesi, sehingga tombol kembali pada browser tidak melanjutkan sesi sebelumya.
c. Jika Aplikasi mengijinkan pengguna untuk tetap masuk, pastikan autentikasi ulang dilakukan secara berkala dalam waktu 12 jam.
d. Lakukan pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna. Satu akun pengguna tidak diperbolehkan digunakan secara bersamaan di beda perangkat. Jika penyelanggara sistem elektronik menghendaki satu akun pengguna dapat digunakan di beda perangkat maka seluruh risiko menjadi tanggung jawab penyelenggara.

3. Kontrol Akses
Otorisasi adalah konsep yang memungkinkan akses ke sumber daya hanya untuk mereka yang diizinkan untuk menggunakannya. Ketentuan kontrol akses adalah sebagai berikut :
a. Menerapkan user level manajemen (minimal terdiri dari tiga level yaitu : superadmin/admin, operator, executive).
b. Menyediakan halaman admin untuk pengelolaan konten sesuai hak akses pengguna.
c. Mengatur verifikasi kebenaran token ketika mengakses data dan informasi agar hanya bisa diakses oleh yang berhak.
d. Pastikan bahwa semua atribut pengguna dan data serta informasi yang digunakan kontrol akses tidak dapatdimanipulasi oleh pengguna.
e. Pastikan aplikasi atau framework memberlakukan mekanisme *anti-CSRF* (*Cross-Site Request Forgery* atau anti pemalsuan permintaan lintas situs) yang kuat.

f. Pastikan bahwa penjelajahan direktori dinonaktifkan, pastikan juga aplikasi tidak boleh mengizikan pengungkapan metadata atau direktori.

4. Validasi Input
Kontrol validasi input yang diterapkan dengan benar, menggunakan daftar allow positif dan pengetikan data yang kuat, dapat menghilangkan lebih dari 90% dari semua serangan injeksi. Pemeriksaan panjang dan jangkauan dapat mengurangi hal ini lebih lanjut. Ketentuan validasi input adalah sebagai berikut:
   a. Pastikan bahwa data terstruktur divalidasi dengan kuat menggunakan penentuan jenis karakter, Panjang karakter dan pola yang sesuai.
   b. Pastikan pada setiap form atau field input pengguna dilakukan sanitasi terhadap jumlah dan jenis karakter yang diizinkan (tidak boleh menerima karakter *script*). Serta melakukan setting anti *Cross Site Scripting (XSS).*
   c. Pastikan data tidak tersimpan jika terjadi kesalahan pada proses validasi.
   d. Melakukan pelindungan dari serangan injeksi basis data antara lain dengan *query sql* menggunakan storage *procedure, function procedure, setting environment* menjadi *production* dan tidak menampilkan *error system.*
   e. Pastikan aplikasi sudah melakukan pelindungan terhadap serangan *Local File Inclusion (LFI) atau Remote File Inclusion (RFI).*
   f. Pastikan aplikasi sudah melakukan pelindungan terhadap serangan *XPath injection or XML injection attacks.*

5. Kriptografi
Aset terpenting adalah data yang diproses, disimpan, atau ditransmisikan oleh aplikasi. Selalu lakukan penilaian dampak privasi untuk mengklasifikasikan kebutuhan perlindungan data dari setiap data yang disimpan dengan benar. Ketentuan kriptografi adalah sebagai berikut :
   a. Pastikan bahwa data pribadi, penting dan rahasia dienkripsi menggunakan mekanisme *enkripsi* satu arah.
   b. Pastikan *enkripsi* tidak menggunakan metode atau algoritma yang tidak aman.

6. Penanganan Error dan Pencatatan Log
Tujuan utama penanganan error dan pencatatan log adalah untuk memberikan informasi yang berguna bagi pengguna, administrator, dan tim respons insiden. Tujuannya bukan untuk membuat log dalam jumlah besar, tetapi log berkualitas tinggi. Ketentuan penanganan error dan pencatatan log adalah sebagai berikut :
   a. Pastikan log tidak mencatat informasi sensitif atau dikecualikan.
   b. Mengatur rentang waktu penyimpanan log sesuai kebutuhan aplikasi.
   c. Pastikan log mencatat aktivitas user, Proses berhasil atau gagal login, kesalahan validasi input, dan kesalahan kontrol akses.
   d. Pastikan log menyertakan informasi tentang garis waktu hari dan jam terperinci (dd/mm/yyyy dan hh:mm:ss).
   e. Pastikan Log terlindungi dari akses illegal dan modifikasi.
   f. Pastikan zona waktu server sesuai dan benar.

g. Pastikan mengatur tampilan pesan saat terjadi kesalahan atau error.

7. Proteksi Data
   Ada tiga elemen kunci untuk pelindungan data yang baik: Kerahasiaan, Integritas, dan Ketersediaan. Standar proteksi data mengasumsikan bahwa perlindungan data diberlakukan pada sistem terpercaya, seperti server yang telah diperkuat dan memiliki perlindungan yang memadai. Ketentuan proteksi data adalah sebagai berikut :
   a. Menyediakan prosedur *backup data* secara otomatis sistem.
   b. Menyediakan prosedur *backup data* secara manual melalui superadmin/admin.
   c. Memastikan data yang di-*backup* termasuk *file upload*.
   d. Pastikan data *backup* tersimpan dengan aman.
   e. Jika aplikasi memiliki fungsi *export* data dalam bentuk *file* (*pdf*, *xls*, *doc*, *ppt* dan sejenisnya) dimana didalamnya mengandung informasi sensitif, data pribadi, dan atau data rahasia, *file* keluaran wajib menggunakan *password*, diatur dalam SOP terpisah.

8. Keamanan Komunikasi
   a. Pastikan aplikasi menerapkan protocol HTTPS atau SSL.
   b. Komunikasi dengan server menggunakan jaringan internal Pemerintah Kota Pariaman.

9. Pengendalian Kode Berbahaya
   a. Pastikan Kode Sumber Aplikasi dan *Library* tidak mengandung backdoor dan kode berbahaya lainnya.
   b. Pastikan melakukan pengaturan *Content Security Policy* (CSP) dan *Cross-Origin Resource Sharing* (CORS).
   c. Pastikan bahwa aplikasi meminta izin ke pengguna sebelum memanfaatkan fitur dan sensor dari pengguna.
   d. Pastikan aplikasi hanya meminta izin yang diperlukan.

10. Logika Bisnis
    a. Pastikan aplikasi hanya memproses alur bisnis sesuai dengan alur bisnis yang ada dan tidak melewatkan langkah alur bisnis.
    b. Pastikan aplikasi hanya memproses alur logika bisnis dengan semua langkah lainnya diproses dalam waktu yang realistis.
    c. Pastikan Aplikasi memiliki kontrol anti-otomatisasi.

11. File
    a. Pastikan Aplikasi tidak akan menerima file dengan ukuran besar yang akan membebani penyimpanan.
    b. Pastikan aplikasi melakukan validasi terhadap type, ukuran dan jumlah file yang di upload oleh pengguna.
    c. Pastikan aplikasi menerapkan pengacakan nama file yang diupload dan tersimpan di server.
    d. Pastikan aplikasi menyimpan file upload diluar *root web*.
    e. Pastikan bahwa permintaan langsung ke file yang diupload tidak akan dijalankan sebagai konten HTML/JavaScript.

12. Keamanan API dan Web Service
    a. API yang dibuat harus menggunakan Token.
    b. Pastikan URL API tidak mengekspose informasi *sensitive*, seperti kunci API dan Token Sesi.
    c. API satuan data yang harus dijaga kerahasiaannya menggunakan Token atau sistem *enkripsi* dan *dekripsi* dalam proses transaksi data.
    d. API dibuat menggunakan aplikasi SPLP (Sistem Penghubung Layanan Pemerintah). Proses integrasi dan interoperabilitas data yang diselenggarakan melalui SPLP KOTA PARIAMAN dilaksanakan oleh unit khusus di luar ketentuan buku panduan ini.

13. Keamanan Konfigurasi
    a. Pastikan proses pembuatan dan pengembangan aplikasi dilakukan dengan cara yang aman.
    b. Pastikan konfigurasi server disesuaikan dengan hasil analisa kebutuhan server aplikasi.
    c. Pastikan semua data *dummy*, uji coba dan tidak diperlukan dihapus. (termasuk *user*, *role*, *table*, kolom *table*, dll).
    d. Pastikan Setting CSP (*Content Security Policy*) dilakukan untuk mengurangi dampak serangan XSS (*Cross Site Scripting*).
    e. Pastikan bahwa *header Origin* yang disediakan tidak digunakan untuk keputusan autentikasi atau kontrol akses, karena *header* Origin dapat dengan mudah diubah oleh penyerang.
    f. Pastikan Setting CORS (*Cross-origin resource sharing*) menggunakan daftar domain yang terpercaya tidak menggunakan "null" atau "*".

C. SPESIFIKASI TEKNIS APLIKASI

Aplikasi yang dibangun/dikembangkan harus memenuhi Standar Pembangunan dan Pengembangan Aplikasi di Pemerintah KOTA PARIAMAN, yang diantaranya :

1. Aplikasi berbasis web harus memiliki kemampuan *responsive* terhadap rasio layar atau perangkat yang digunakan, bisa menyesuaikan tampilan dengan perangkat yang digunakan.
2. Aplikasi dapat dibangun atau dikembangkan sebagai aplikasi berbasis mobile seperti Android atau IOS dengan mengikuti persyaratan yang ditetapkan oleh pihak ketiga pendukung platform Android dan IOS tersebut.
3. Aplikasi dibangun menggunakan bahasa pemrograman kode sumber terbuka (*open source*), antara lain: PHP, Java, JavaScript, HTML dan CSS.
4. Database yang digunakan dalam aplikasi harus database kode sumber terbuka (*open source*), antara lain: MySQL, PostgreSQL. Penggunaan database berbayar seperti SQLServer atau Oracle harus berdasarkan kebutuhan aplikasi dengan menyertakan alasan yang kuat dan mendapat rekomendasi dari Dinas Komunikasi dan Informatika Kota Pariaman.
5. Aplikasi yang dibangun harus kompatibel dan berjalan dengan baik pada sistem operasi dan server linux.
6. Aplikasi dibangun menggunakan framework versi terbaru atau satu tingkat dibawah versi terbaru, atau salah satu dari beberapa pilihan arsitektur framework seperti berikut :

a. Menggunakan framework Laravel untuk backend dan frontend (Aplikasi kecil, tingkat komplesitasnya rendah, data tidak banyak).
b. Menggunakan framework Laravel untuk backend dan untuk frontend menggunakan Java Script (JS) Library seperti: React JS atau Vue JS (Aplikasi kecil dan menengah, tingkat kompleksitas menengah, data banyak).
c. Menggunakan Node JS, Express JS untuk back end dan untuk front end menggunakan Java Script (JS) Library seperti: React JS atau Vue JS. (Aplikasi menengah dan besar, tingkat kompleksitas tinggi, data banyak dan sangat banyak).
d. Menggunakan Golang untuk back end dan untuk front end menggunakan Java Script (JS) Library seperti: React JS atau Vue JS.

7. Aplikasi yang telah dibangun dan tidak menggunakan framework, dikonversi/dikembangkan menggunakan framework sebagaimana disebutkan pada angka 6.
8. Aplikasi yang dibangun/dikembangkan menggunakan framework selain ketentuan diatas, pengembang berkewajiban memberikan alih pengetahuan kepada tim pengelola aplikasi dan tim standardisasi aplikasi pada Dinas Komunikasi dan Informatika Kota Pariaman serta menjamin keamanan, integrasi dan interoperabilitas data.
9. Pembangunan Aplikasi berbasis Rupa Bumi/GIS (Geographic Informatic System) harus berkoordinasi dengan Bappeda Kota Pariaman dan Dinas Komunikasi dan Informatika Kota Pariaman berkaitan dengan standardisasi data rupa bumi (peta) yang digunakan.
    a. Peta dasar yang digunakan harus menggunakan Peta Open Source seperti: Open Street Map, peta dasar yang disediakan BIG (Badan Informasi Geospasial) atau pihak ketiga lain yang tidak berbayar.
    b. Data layer yang digunakan bersumber pada data yang sudah dimiliki oleh Bappeda Kota Pariaman.
    c. Standardisasi data peta yang dihasilkan kegiatan pembangunan/pengembangan aplikasi harus sesuai dengan yang ditetapkan Bappeda Kota Pariaman.
    d. Data peta yang dihasilkan harus diserahkan ke Bappeda Kota Pariaman dan Dinas Komunikasi dan Informatika Kota Pariaman.
10. Aplikasi non GIS yang menampilkan fasilitas peta yang tidak kompleks, bisa dibangun/ dikembangkan tanpa Server GIS, melainkan langsung menggunakan library javascript kode sumber terbuka (open source) seperti leaflet dan open layer.
11. Aplikasi GIS (Geographic Informatic System) kompleks minimal memiliki infrastruktur Server GIS kode sumber terbuka (open source). Spesifikasi perangkat Geo Server dan antar muka aplikasi harus sesuai dengan spesifikasi yang dibutuhkan oleh aplikasi yang dibangun/dikembangkan;
    a. Aplikasi yang dibangun menyediakan Halaman Dashboard atau Laporan yang dapat terdiri dari : rekap data, berita, artikel, galeri setiap hari, jumlah pengunjung, laporan yang masuk, laporan yang telah ditangani, jumlah pengguna berdasarkan level, sesuai dengan data yang ada di aplikasi dan ditampilkan dalam bentuk grafik, diagram maupun tabel, kritik/saran, layanan chat admin, kontak kami (nama, alamat, email, telepon, medsos perangkat daerah) dan lain-lain sesuai kebutuhan aplikasi.
12. Di setiap halaman aplikasi harus menampilkan:

a. Logo resmi Pemerintah Kota Pariaman.
b. *Copyright* terdaftar atas nama Pemerintah Kota Pariaman dengan mencantumkan tahun pembangunan aplikasi.

13. Aplikasi harus memuat menu Manajemen Pengetahuan yang berisi diantaranya :
    a. FAQ.
    b. SOP.
    c. Panduan Penggunaan Aplikasi.
    d. Video penggunaan aplikasi (sesuai rekomendasi Tim Asesmen).
14. Aplikasi menyediakan *web service* atau API (*Application Programming Interface*) yang dibutuhkan untuk integrasi/ interoperabilitas data dengan aplikasi milik Pemerintah Kota Pariaman dan aplikasi lainnya.
15. Setiap aplikasi memberikan akses *database read-only* kepada Dinas Komunikasi dan Informatika Kota Pariaman untuk kebutuhan Data *Warehouse* Pemerintah Daerah Kota Pariaman.
16. Menyediakan fasilitas backend yang berfungsi untuk mengelola konten aplikasi (*content management system:* CMS) yang dibutuhkan dalam penyelenggaraan sistem informasi.
17. Aplikasi harus menggunakan Bahasa Indonesia, kecuali Bahasa Asing yang sudah menjadi Bahasa serapan.
18. Aplikasi yang memiliki fungsi persuratan atau tata naskah dinas harus memenuhi kriteria sebagai berikut:
    a. Terintegrasi dengan aplikasi Tata Naskah Dinas Kota Pariaman dan menggunakan Sertifikat Elektronik dan tidak merupakan replikasi dari aplikasi SRIKANDI.
    b. Format surat menyesuaikan dengan Peraturan Menteri Dalam Negeri Nomor 1 tahun 2023 tentang Tata Naskah Dinas di Lingkungan Pemerintah Daerah.
19. Aplikasi yang memiliki fungsi pelaporan harus memenuhi kriteria sebagai berikut:
    a. Laporan dieksport ke format PDF untuk memastikan validasi data laporan tercetak, kecuali ada kebutuhan Dinas untuk mengeksport data ke format lain (excel, word, dll);
    b. Dalam data yang tercetak, jika ada data sensitif dan pribadi (NIK, Nomor Rekening, Alamat, dll), ditampilkan dalam bentuk data masking, atau tidak ditampilkan ke format laporan, kecuali sangat dibutuhkan;
    c. Jika ada kebutuhan data sensitif dan atau pribadi untuk ditampilkan di laporan, setiap file yang dihasilkan diberi password untuk membuka file.
20. Ukuran field table pada database disetting seoptimal mungkin sesuai dengan kebutuhan data.
21. Jika ada menu upload file, real path file yang diupload, dan tag html file tidak disimpan dalam field table database, hanya nama file saja.

D. RUANG LINGKUP INFRASTRUKTUR

1. Untuk keamanan data aplikasi, pengembang harus membuat proses *backup database* secara rutin harian yang disimpan pada *folder* khusus di Server Aplikasi. *Backup* tersimpan adalah 7 hari terakhir.
2. Aplikasi dipublish melalui protokol *HTTPS*, me-redirect akses *HTTP* ke *HTTPS* secara otomatis, dimana *SSL* yang digunakan adalah *SSL* Pemerintah Daerah Kota Pariaman yang diberikan Dinas Komunikasi dan Informatika Kota Pariaman atau *SSL* resmi lain dan bukan SSL

Gratis. Untuk menerapkan ini diperlukan seting di sisi Server dan sisi Aplikasi.

3. Aplikasi Khusus Spesifik yang besar (Tinggi dan Strategis), mencakup data yang besar, mencakup pengguna seluruh perangkat daerah atau masyarakat luas, akan memerlukan server tersendiri (*Server Aplikasi*, *Data Storage*, dan *Server Backup*). Untuk aplikasi dengan kriteria ini, Perangkat Daerah mengadakan kegiatan pengadaan Server dan berkoordinasi dengan Dinas Komunikasi dan Informatika.
4. Fasilitas *Hosting* dan nama *Subdomain* diberikan setelah Dinas Komunikasi dan Informatika menerima Surat Permohonan Hosting dan nama *Subdomain* setelah aplikasi tersebut selesai diasesmen oleh Tim Asesmen Standardisasi.
5. Penggunaan/Pemanfaatan Aplikasi dalam bentuk Sewa Pakai harus memenuhi prinsip kemandirian data dan keamanan data milik Pemerintah Daerah Kota Pariaman.
6. Penempatan aplikasi pada pusat data milik non pemerintah dilaksanakan sesuai dengan peraturan perundang-undangan yang berlaku.
7. Kebutuhan terhadap aplikasi berskala enterprise perolehan dan penyelenggaraannya diatur dalam aturan tersendiri.

E. KETENTUAN LAINNYA

1. Aplikasi yang belum menggunakan *framework* dan aplikasi telah ada dan digunakan sebelum standardisasi *framework* diatas diterbitkan.
2. Aplikasi yang cakupan proses bisnisnya besar dan memiliki tingkat kompleksitas tinggi atau tidak memiliki anggaran cukup untuk dibangun ulang agar sesuai dengan *framework* yang disyaratkan, dapat tetap menggunakan *framework* yang lama, dengan syarat tetap mengikuti update spesifikasi sistem (misal: mendukung PHP versi terbaru, MySQL versi terbaru, dukungan *software* ter-*update* agar lebih aman dan harus lulus uji keamanan aplikasi).
3. Untuk menjamin kelayakan teknis dan waktu pengerjaan aplikasi, setiap rencana pembangunan/pengembangan/pemeliharaan aplikasi harus mencantumkan klasifikasi tingkat kompleksitas serta estimasi waktu pengerjaan yang sesuai. Klasifikasi waktu dan kompleksitas (mudah, sedang, sulit) aplikasi dapat dirincikan sebagai berikut.
   a. Klasifikasi waktu pengerjaan
      1) Tingkat kompleksitas mudah: Waktu Maksimal Pengerjaan adalah 1(satu) bulan
      2) Tingkat kompleksitas sedang: Waktu Maksimal Pengerjaan adalah 6(enam) bulan
      3) Tingkat kompleksitas sulit: Waktu Maksimal Pengerjaan adalah 12(dua belas) bulan
   b. Kriteria kompleksitas aplikasi
      1) Tingkat kompleksitas mudah: Aplikasi hanya berisi formulir isian sederhana, seperti (menambahkan, mengubah, dan menghapus data), Tidak terhubung atau digunakan bersama oleh perangkat daerah lain, Hanya digunakan oleh satu jenis pengguna (tidak ada pembagian hak akses atau login berbeda), Tidak membutuhkan pengolahan data dalam jumlah besar, Tidak menggunakan fitur Sistem Informasi Geografis (GIS) beserta dengan server GIS, dan Tidak perlu terhubung dengan aplikasi lain.

2) Tingkat kompleksitas sedang: Aplikasi digunakan oleh beberapa jenis pengguna dengan hak akses berbeda seperti (user, operator, admin, dan super admin), Menyediakan tampilan ringkasan data atau laporan dalam bentuk grafik atau tabel, Terhubung dengan aplikasi lain yang dimiliki oleh Pemerintah Kota Pariaman, Memiliki fitur untuk mengelola isi aplikasi seperti (berita, informasi, atau galeri), Menggunakan fitur Sistem Informasi Geografis (GIS) beserta dengan server GIS, dan Memerlukan pengecekan data yang dimasukkan dan fitur unggah file seperti foto atau dokumen.
3) Tingkat kompleksitas sulit: Aplikasi digunakan oleh banyak perangkat daerah atau masyarakat umum secara luas, Memiliki alur kerja atau proses yang rumit dan berjenjang, mampu terhubung dengan sistem atau aplikasi pemerintah lainnya secara otomatis, Mengolah dan menyimpan data dalam jumlah sangat besar, termasuk data penting dan rahasia, Membutuhkan server khusus karena kapasitas dan keamanannya lebih tinggi, dan Memiliki fitur tambahan seperti laporan resmi, sistem surat-menyurat, keamanan tingkat lanjut, dan panduan dalam bentuk video

4. Pengembang aplikasi wajib memberikan pelatihan penggunaan aplikasi seluruh pengguna aplikasi.
5. Pengembang aplikasi harus memberikan pendampingan/ Helpdesk selama 1 tahun setelah pengembangan aplikasi. Mencakup memberikan bantuan jika ada kendala saat penerapan aplikasi dan bug-bug yang harus diperbaiki pada aplikasi.
6. Perangkat Daerah dapat menganggarkan kegiatan pengembangan aplikasi yang ruang lingkupnya mencakup juga pembangunan ulang aplikasi menggunakan framework yang disyaratkan.
7. Aplikasi yang dibangun dengan Anggaran APBD Kota Pariaman, Hak Milik dan Hak Cipta Aplikasi tersebut adalah milik Pemerintah Kota Pariaman.

WALI KOTA PARIAMAN,

YOTA BALAD

PARAF KOORDINASI
PRODUK HUKUM KOTA PARIAMAN