PEMERINTAH KABUPATEN MAJALENGKA
DINAS KOMUNIKASI DAN INFORMATIKA
Alamat : Jalan Pangeran Muhammad KM. 5 Simpeureum Tlp/Fax (0233) 8292292 -Majalengka 45476
Email :*diskominfo@majalengkakab.go.id* Website : diskominfo.majalengkakab.go.id

KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MAJALENGKA
NOMOR : 800/246-Diskominfo/ 2024

TENTANG
BUKU PANDUAN PEMBANGUNAN/PENGEMBANGAN/
PEMELIHARAAN APLIKASI

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MAJALENGKA

Menimbang : a. bahwa standardisasi pembangunan aplikasi sebagai sarana untuk mewujudkan sistem informasi yang terintegrasi, data yang terstruktur, aksesibilitas, kapasitas, keamanan, keandalan, penetrasi layanan, terjangkau, legitimasi, dukungan teknis agar pelaksanaannya selaras dengan misi pembangunan daerah dan tata kelola pemerintah yang baik, perlu adanya pengaturan standardisasi pembangunan aplikasi dan sistem informasi;

b. bahwa untuk memenuhi standardisasi pembangunan aplikasi dan sistem informasi sebagaimana dimaksud pada huruf a, perlu membentuk Tim Asesmen Standardisasi Aplikasi dan Sistem Informasi Dinas Komunikasi dan Informatika Kabupaten Majalengka ;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b perlu menetapkan Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Majalengka tentang Buku Panduan Pembangunan/ Pengembangan/ Pemeliharaan Aplikasi.

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
19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
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 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
6. 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);
7. Peraturan Bupati Kabupaten Majalengka Nomor 13 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Majalengka;
8. Peraturan Bupati Kabupaten Majalengka Nomor 44 Tahun 2021 tentang Pedoman layanan pengelolaan nama domain, Subdomain, Hosting, Mail Server dan co-Location Server Di Lingkungan Pemerintah Kabupaten Majalengka;
9. Peraturan Bupati Kabupaten Majalengka Nomor 31 Tahun 2021 tentang pedoman manajemen keamanan informasi sistem pemerintahan berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Majalengka;

10. Keputusan Bupati Kabupaten Majalengka NOMOR: ST.01.00.10/KEP.514-DISKOMINFO/2023 tentang Pengelola Data Statistik Sektoral Pada Perangkat Daerah Bupati Majalengka

MEMUTUSKAN:

Menetapkan :

KESATU : Buku Panduan Pembangunan/ Pengembangan/ Pemeliharaan Aplikasi.

KEDUA : Buku Panduan Pembangunan/ Pengembangan/ Pemeliharaan Aplikasi sebagaimana dimaksud Diktum Kesatu tercantum dalam Lampiran Keputusan ini.

KETIGA : Buku Panduan Pembangunan/ Pengembangan/ Pemeliharaan Aplikasi sebagaimana dimaksud Diktum Kesatu merupakan Pedoman Pembangunan/ Pengembangan/ Pemeliharaan Aplikasi di Lingkungan Pemerintah Kabupaten Majalengka

KEEMPAT : Keputusan Kepala Dinas ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Majalengka
pada tanggal : 04 April 2024

Kepala Dinas Komunikasi dan Informatika
Kab. Majalengka

H. GATOT SULAEMAN, AP., M.Si.
Pembina Utama Muda
NIP. 19760528 199412 1 001

Tembusan:
1. Pj. Bupati Kabupaten Majalengka

BUKU PANDUAN PEMBANGUNAN/ PENGEMBANGAN/ PEMELIHARAAN APLIKASI

A. DOKUMEN TATA KELOLA

1. KERANGKA ACUAN KERJA

Di dalam Kerangka Acuan Kerja pemmbangunan/pengembangan/ pemeliharaan Aplikasi, pada pasal spesifikasi teknis Aplikasi berpedoman pada standarisasi aplikasi yang ditetapkan oleh Dinas Komunikasi dan Informatika Kabupaten Majalengka.

2. LAPORAN AWAL

Laporan awal minimal harus memenuhi hal-hal sebagai berikut:

BAB I (Pendahuluan)

- Latar Belakang Pembangunan Aplikasi
- Teori rencana pengembangan aplikasi menggunakan Sistem Development Life Cycle, Waterfall (Air Terjun), dan RAD (Rapid Application Development);

BAB II (Ruang Lingkup)

- Planning:
  a. Identifying Bussiness Value terdiri atas :System Request (Change/System Request) 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 Kabupaten Majalengka , 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. Ditampilkan setiap halaman dari aplikasi;
d. Desain Tampilan Keluaran Produk Aplikasi. Ditampilkan 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:

- Program Design : desain dan rancangan program aplikasi
    a. Class Diagram (Diagram kelas) adalah diagram pemodelan secara visual yang menggambarkan kelas-kelas dalam sebuah sistem dan hubungannya antara satu dengan yang lain serta dimasukkan pula atribut dan operasi.
    b. Sequence Diagram (diagram urutan) adalah sebuah diagram yang digunakan untuk menjelaskan dan menampilkan interaksi antar objek-objek dalam sebuah sistem secara terperinci Dibuatkan dari setiap tahapan atau aktivitas pada aplikasi;
    c. 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.
- Implementation (implementasi) adalah tahap dimana rencana atau desain diwujudkan menjadi tindakan konkrit atau produk akhir.
    a. Software Construction : spesifikasi teknis aplikasi mencantumkan versi dari Framework, bahasa pemrograman, database, aplikasi webserver, dll.
    b. Struktur Database (struktur basis data);
    c. Software Testing. Software testing dilakukan untuk pengujian semua tahapan atau fungsi pada aplikasi berjalan dengan baik. Pengujian aplikasi dapat menggunakan metode BlackBox Testing;
    d. Spesifikasi Kebutuhan Server terdiri dari kebutuhan atas :
        - Processor
        - RAM
        - 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 sudah 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:

- Jika pengguna aplikasi lebih dari satu Perangkat Daerah danatau Publik, Pendaftaran akun menggunakan email aktif dan menggunakan verifikasi email.
- 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.
- Pastikan terdapat menu ubah kata sandi, yang mewajibkan memasukan kata sandi pengguna saat ini pada proses perubahan kata sandi.
- Menyediakan pengukur kekuatan kata sandi pada aplikasi untuk membantu pengguna dalam membuat kata sandi yang kuat.
- Menyediakan fitur lihat sementara kata sandi pengguna untuk membantu pengguna dalam memasukan kata sandi.
- Mengatur mekanisme pemulihan atau reset kata sandi pengguna. Pemulihan atau reset kata sandi wajib dilakukan mandiri oleh pengguna.
- Mengatur masa berlaku kata sandi selama 1 tahun. Jika masa berlaku berakhir pengguna diwajibkan untuk merubah kata sandi.

- Jika akun penguna dibuat oleh pengembang / Admin aplikasi, maka pengguna wajib merubah kata sandi saat pertama kali masuk kedalam aplikasi.
- Mengatur jumlah salah input kata sandi, batas maksimal 5 kali, pengguna akan tertahan dan bisa input kata sandi kembali setelah 3 menit.
- Penggunaan kata sandi bertingkat diwajibkan bagi aplikasi yang menurut hasil penilaian Tim Asesmen merupakan aplikasi yang mengelola data penting dan sangat rahasia.
- Menjaga kerahasiaan kata sandi yang disimpan pada database melalui mekanisme kriptografi satu arah.
- Menggunakan jalur komunikasi yang diamankan untuk proses autentikasi pada server.
- Penerapan kata sandi sesuai syarat diatas juga termasuk untuk kata sandi pada server.
- Pastikan akun default pada server dirubah (contoh: root)
- Menyediakan Captcha atau oprasi hitung pada halaman login dan pendaftaran.
- 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:

- Pastikan aplikasi tidak pernah mengungkapkan token sesi dalam parameter URL

- Memanfaatkan pengendali sesi yang disediakan oleh framework aplikasi
- Atur pengendali waktu habis sesi (*auto logout*) minimal 10 menit dan maksimal 15 menit
- Pastikan bahwa logout dan kadaluwarsa membatalkan token sesi, sehingga tombol kembali pada browser tidak melanjutkan sesi sebelumya.
- Jika Aplikasi mengijinkan pengguna untuk tetap masuk, pastikan autentikasi ulang dilakukan secara berkala dalam waktu 12 jam.
- 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:

- Menerapkan user level manajemen (minimal terdiri dari tiga level yaitu : superadmin/admin, operator, executive)
- Menyediakan halaman admin untuk pengelolaan konten sesuai hak akses pengguna
- Mengatur verifikasi kebenaran token ketika mengakses data dan informasi agar hanya bisa diakses oleh yang berhak
- Pastikan bahwa semua atribut pengguna dan data serta informasi yang digunakan kontrol akses tidak dapatdimanipulasi oleh pengguna.

- Pastikan aplikasi atau framework memberlakukan mekanisme anti-CSRF (Cross-Site Request Forgery atau anti pemalsuan permintaan lintas situs) yang kuat.
- 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:

- Pastikan bahwa data terstruktur divalidasi dengan kuat menggunakan penentuan jenis karakter, Panjang karakter dan pola yang sesuai.
- 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)
- Pastikan data tidak tersimpan jika terjadi kesalahan pada proses validasi.
- 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*.
- Pastikan aplikasi sudah melakukan pelindungan terhadap serangan *Local File Inclusion* (LFI) atau *Remote File Inclusion* (RFI)
- 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:

- Pastikan bahwa data pribadi, penting dan rahasia dienkripsi menggunakan mekanisme enkripsi satu arah
- 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:

- Pastikan log tidak mencatat informasi sensitif atau dikecualikan
- Mengatur rentang waktu penyimpanan log sesuai kebutuhan aplikasi
- Pastikan log mencatat aktivitas user, Proses berhasil atau gagal login, kesalahan validasi input, dan kesalahan kontrol akses.
- Pastikan log menyertakan informasi tentang garis waktu hari dan jam terperinci (dd/mm/yyyy dan hh:mm:ss)
- Pastikan Log terlindungi dari akses illegal dan modifikasi
- Pastikan zona waktu server sesuai dan benar.
- 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 ini

mengasumsikan bahwa perlindungan data diberlakukan pada sistem terpercaya, seperti server yang telah diperkuat dan memiliki perlindungan yang memadai. Ketentuan proteksi data adalah sebagai berikut:

- Menyediakan prosedur *backup data* secara otomatis sistem
- Menyediakan prosedur *backup data* secara manual melalui superadmin/admin
- Memastikan data yang di-*backup* termasuk *file upload*
- Pastikan data *backup* tersimpan dengan aman
- 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

- Pastikan aplikasi menerapkan protocol HTTPS atau SSL
- Komunikasi dengan server menggunakan jaringan internal Pemerintah Kabupaten Majalengka .

9. Pengendalian Kode Berbahaya

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

10. Logika Bisnis

- Pastikan aplikasi hanya memproses alur bisnis sesuai dengan alur bisnis yang ada dan tidak melewatkan langkah alur bisnis.

- Pastikan aplikasi hanya memproses alur logika bisnis dengan semua langkah lainnya diproses dalam waktu yang realistis.
- Pastikan Aplikasi memiliki kontrol anti-otomatisasi

11. File

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

12. Keamanan API dan Web Service

- API yang dibuat harus menggunakan Token.
- Pastikan URL API tidak mengekspose informasi sensitive, seperti kunci API dan Token Sesi;
- API satuan data yang harus dijaga kerahasiaannya menggunakan Token atau sistem enkripsi dan dekripsi dalam proses transaksi data;
- API dibuat menggunakan aplikasi SPLP (Sistem Penghubung Layanan Pemerintah). Proses integrasi dan interoperabilitas data yang diselenggarakan melalui SPLP Kabupaten Majalengka dilaksanakan oleh unit khusus di luar ketentuan buku panduan ini.

13. Keamanan Konfigurasi

- Pastikan proses pembuatan dan pengembangan aplikasi dilakukan dengan cara yang aman

- Pastikan konfigurasi server disesuaikan dengan hasil analisa kebutuhan server aplikasi
- Pastikan semua data dummy, uji coba dan tidak diperlukan dihapus. (termasuk user, role, table, kolom table, dll)
- Pastikan Setting CSP (*Content Security Policy*) dilakukan untuk mengurangi dampak serangan XSS (*Cross Site Scripting*)
- Pastikan bahwa *header Origin* yang disediakan tidak digunakan untuk keputusan autentikasi atau kontrol akses, karena *header Origin* dapat dengan mudah diubah oleh penyerang
- 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 Kabupaten Majalengka , yang diantaranya:

a. Aplikasi berbasis web harus memiliki kemampuan responsive terhadap rasio layar atau perangkat yang digunakan, bisa menyesuaikan tampilan dengan perangkat yang digunakan;
b. 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;
c. Aplikasi dibangun menggunakan bahasa pemrograman kode sumber terbuka (open source), antara lain: PHP, Java,JavaScript, HTML dan CSS;
d. 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 Kabupaten Majalengka ;

e. Aplikasi yang dibangun harus kompatibel dan berjalan dengan baik pada sistem operasi dan server linux;
f. Aplikasi dibangun menggunakan framework versi terbaru atau satu tingkat dibawah versi terbaru, atau salah satu dari beberapa pilihan arsitektur framework seperti berikut:
    - Menggunakan framework Laravel untuk back end dan front end (Aplikasi kecil, tingkat komplesitasnya rendah, data tidak banyak)
    - Menggunakan framework Laravel untuk back end dan untuk front end menggunakan Java Script (JS) Library seperti: React JS atau Vue JS (Aplikasi kecil dan menengah, tingkat kompleksitas menengah, data banyak)
    - 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)
    - Menggunakan Golang untuk back end dan untuk front end menggunakan Java Script (JS) Library seperti: React JS atau Vue JS.
g. Aplikasi yang telah dibangun dan tidak menggunakan framework, dikonversi/dikembangkan menggunakan framework sebagaimana disebutkan pada huruf f;
h. Aplikasi yang dibangun/dikembangkan menggunakan *framework* selain ketentuan diatas, pengembang berkewajiban memberikan alih pengetahuan kepada tim pengelola aplikasi dan tim standarisasi aplikasi pada Dinas Komunikasi dan Informatika Kabupaten Majalengka serta menjamin keamanan, integrasi dan interoperabilitas data;

i. Pembangunan Aplikasi berbasis Rupa Bumi/*GIS (Geographic Informatic System)* harus berkoordinasi dengan Bappeda Kabupaten Majalengka dan Dinas Komunikasi dan Informatika Kabupaten Majalengka berkaitan dengan standardisasi data rupa bumi (peta) yang digunakan.
    1) 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.
    2) Data *layer* yang digunakan bersumber pada data yang sudah dimiliki oleh Bappeda Kabupaten Majalengka .
    3) Standardisasi data peta yang dihasilkan kegiatan pembangunan/pengembangan aplikasi harus sesuai dengan yang ditetapkan Bappeda Kabupaten Majalengka .
    4) Data peta yang dihasilkan harus diserahkan ke Bappeda Kabupaten Majalengka dan Dinas Komunikasi dan Informatika Kabupaten Majalengka .
j. 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*.
k. 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;
l. 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.

m. Di setiap halaman aplikasi harus menampilkan :
    - Logo resmi Pemerintah Kabupaten Majalengka
    - Copyright terdaftar atas nama Pemerintah Kabupaten Majalengka dengan mencantumkan tahun pembangunan aplikasi
n. Aplikasi harus memuat menu Manjemen Pengetahuan yang berisi diantaranya:
    - FAQ
    - SOP
    - Panduan Penggunaan Aplikasi
    - Video penggunaan aplikasi (sesuai rekomendasi Tim Asesmen)
o. Aplikasi menyediakan web service atau API (Application Programming Interface) yang dibutuhkan untuk integrasi/interoperabilitas data dengan aplikasi milik Pemerintah Kabupaten Majalengka dan aplikasi lainnya;
p. Setiap aplikasi memberikan akses *database read-only* kepada Dinas Komunikasi dan Informatika Kabupaten Majalengka untuk kebutuhan *Data Warehouse* Pemerintah Daerah Kabupaten Majalengka .
q. Menyediakan fasilitas *backend* yang berfungsi untuk mengelola konten aplikasi (content management system : CMS) yang dibutuhkan dalam penyelenggaraan sistem informasi.
r. Aplikasi harus menggunakan Bahasa Indonesia, kecuali Bahasa Asing yang sudah menjadi Bahasa serapan.
s. Aplikasi yang memiliki fungsi persuratan atau tata naskah dinas harus memenuhi kriteria sebagai berikut:
    - Terintegrasi dengan aplikasi TND Kabupaten Majalengka Dan menggunakan Sertifikat Elektronik.
    - Format surat menyesuaikan dengan Peraturan Bupati Kabupaten Majalengka Nomor 28 tahun 2021 tentang Tata Naskah Dinas Elektronik di lingkungan Pemerintah Daerah

Kabupaten Majalengka.

t. Aplikasi yang memiliki fungsi pelaporan harus memenuhi kriteria sebagai berikut:
    - Laporan dieksport ke format PDF untuk memastikan validasi data laporan tercetak, kecuali ada kebutuhan Dinas untuk mengeksport data ke format lain (excel, word, dll)
    - 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
    - Jika ada kebutuhan data sensitif dan atau pribadi untuk ditampilkan di laporan, setiap file yang dihasilkan diberi password untuk membuka file
u. Ukuran field table pada database disetting seoptimal mungkin sesuai dengan kebutuhan data.
v. 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 di*publish* melalui protokol *HTTPS*, me-redirect akses *HTTP* ke *HTTPS* secara otomatis, dimana *SSL* yang digunakan adalah *SSL* Pemerintah Daerah Kabupaten Majalengka yang diberikan Dinas Komunikasi dan Informatika Kabupaten Majalengka 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 Sub Domain kotabogor.go.id diberikan setelah Dinas Komunikasi dan Informatika menerima Surat Permohonan *Hosting* dan Nama Subdomain kotabogor.go.id dan 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 Kabupaten Majalengka.
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

Aplikasi yang belum menggunakan *framework* diatas dan aplikasi telah ada dan digunakan sebelum standardisasi *framework* diatas diterbitkan.

a. Perangkat Daerah dapat menganggarkan kegiatan pengembangan aplikasi yang ruang lingkupnya mencakup juga pembangunan ulang aplikasi menggunakan *framework* yang disyaratkan.
b. 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)

c. Pengembang aplikasi wajib memberikan pelatihan penggunaan aplikasi seluruh pengguna aplikasi.
d. 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.
e. Aplikasi yang dibangun dengan Anggaran APBD Kabupaten Majalengka , Hak Milik dan Hak Cipta Aplikasi tersebut adalah milik Pemerintah Kabupaten Majalengka.

Kepala Dinas Komunikasi dan Informatika
Kab. Majalengka

H. GATOT SULAEMAN, AP., M.Si.
Pembina Utama Muda
NIP. 19760528 199412 1 001