KEMENTERIAN PERENCANAAN PEMBANGUNAN NASIONAL/
BADAN PERENCANAAN PEMBANGUNAN NASIONAL
REPUBLIK INDONESIA

Yth. Pejabat dan Pegawai Kementerian PPN/Bappenas

SURAT EDARAN
SEKRETARIS KEMENTERIAN PERENCANAAN PEMBANGUNAN NASIONAL/
SEKRETARIS UTAMA BADAN PERENCANAAN PEMBANGUNAN NASIONAL
NOMOR 2 TAHUN 2022
TENTANG
PEMBANGUNAN APLIKASI DAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

A. LATAR BELAKANG

Bahwa berdasarkan Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional (UU SPPN), perencanaan merupakan suatu proses untuk menentukan tindakan masa depan yang tepat, melalui urutan pilihan, dengan memperhatikan sumber daya yang tersedia. Dalam menyelenggarakan perencanaan suatu pembangunan, dilakukan dengan beberapa proses dan tahapan yang tidak sederhana, perlu adanya dukungan berupa sarana dan prasarana teknologi, informasi, dan komunikasi (TIK) yang memadai guna mempermudah proses penyelenggaraan perencanaan pembangunan tersebut. Untuk merealisasikannya, dibutuhkan adanya perhatian yang menyeluruh dalam membangun dan mengelola aplikasi sehingga kegiatan perencanaan serta penganggaran dapat terlaksana dan terintegrasi sesuai dengan ketentuan yang berlaku.

Terkait hal tersebut, dalam rangka melaksanankan Peraturan Menteri Perencanaan Pembangunan Nasional/Badan Perencanaan

Pembangunan Nasional Nomor 7 tahun 2021 tentang Penerapan Sistem Pemerintahan Berbasis Elektronik di Internal Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional (Kementerian PPN/Bappenas) serta dalam rangka meningkatkan kualitas aplikasi yang dibangun oleh seluruh unit kerja di Kementerian PPN/Bappenas dan menjaga keamanan informasi yang terdapat di dalam suatu aplikasi, diperlukan keterlibatan dari seluruh pimpinan dan pegawai yang melakukan pembangunan aplikasi di lingkungan Kementerian PPN/Bappenas untuk mengacu pada Kebijakan Teknis Pembangunan dan Pengembangan Aplikasi di Kementerian PPN/Bappenas dan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE).

B. MAKSUD DAN TUJUAN

1. Maksud:

   Surat Edaran ini dimaksudkan sebagai kebijakan tata kelola pembangunan aplikasi dan keamanan informasi SPBE yang terpadu dan terkendali bagi seluruh unit kerja yang melakukan kegiatan pembangunan aplikasi SPBE dan bagi unit kerja yang menangani teknologi informasi dan komunikasi (TIK), serta sebagai kebijakan perlindungan aset data dan informasi dari segala bentuk ancaman.

2. Tujuan:

   Surat Edaran ini bertujuan untuk:

   a. mengatur pembangunan dan pengembangan aplikasi SPBE di Kementerian PPN/Bappenas.

   b. mengatur mengenai kebijakan manajemen keamanan informasi SPBE di Kementerian PPN/Bappenas.

C. DASAR HUKUM

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 dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846).
3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038).
4. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksana Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.
5. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
6. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
8. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.
9. Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Nomor 7 Tahun 2021 tentang Penerapan Sistem Pemerintahan Berbasis Elektronik di Internal Kementerian PPN/Bappenas.
10. Keputusan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Nomor KEP.24/M.PPN/HK/03/2022 tentang Penetapan Arsitektur dan Peta Rencana Sistem Pemerintahan Berbasis Elektronik di Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional.
11. Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala

Badan Perencanaan Pembangunan Nasional Nomor 3 Tahun 2022 tentang Organisasi dan Tata Kerja Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional.

D. RUANG LINGKUP

Surat Edaran ini meliputi kebijakan tentang:

1. pembangunan dan pengembangan aplikasi; dan
2. manajemen keamanan informasi sistem pemerintahan berbasis elektronik

E. ISI EDARAN

1. Seluruh unit kerja dalam melakukan pembangunan aplikasi mengikuti pedoman aplikasi dan melaksanakan manajemen keamanan informasi sesuai dengan ketentuan sebagaimana diatur dalam Surat Edaran ini.
2. Tata cara pelaksanaan pembangunan aplikasi dan manajemen keamanan informasi SPBE mengacu pada ketentuan sebagaimana diatur dalam Lampiran Surat Edaran ini.
3. Dalam proses perencanaan, pembangunan pengujian, proses penyebaran (*deployment),* dan monitoring aplikasi yang dibangun, seluruh pimpinan dan pegawai unit kerja di Kementerian PPN/Bappenas dilaksanakan dengan melibatkan unit kerja yang menangani TIK.
4. Kebijakan teknis dalam rangka pelaksanaan surat edaran ini ditetapkan oleh Kepala Pusat Data dan Informasi Perencanaan Pembangunan.

F. PENUTUP

1. Seluruh pejabat dan pegawai di Kementerian PPN/Bappenas melaksanakan Surat Edaran ini.
2. Surat Edaran ini berlaku sejak tanggal ditetapkan.

Demikian Surat Edaran ini dibuat, untuk dilaksanakan sebagaimana mestinya.

Ditetapkan di Jakarta
pada tanggal 13 Juni 2022

SEKRETARIS KEMENTERIAN
PERENCANAAN PEMBANGUNAN NASIONAL/
SEKRETARIS UTAMA BADAN
PERENCANAAN PEMBANGUNAN NASIONAL,

TAUFIK HANAFI

LAMPIRAN I
SURAT EDARAN SESMEN PPN/ SESTAMA BAPPENAS
NOMOR 2 TAHUN 2022
TENTANG
PEMBANGUNAN APLIKASI DAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

PEMBANGUNAN DAN PENGEMBANGAN APLIKASI DI KEMENTERIAN PPN/BAPPENAS

BAB I KETENTUAN PENGEMBANGAN APLIKASI

A. KETENTUAN

1. Aplikasi harus dibangun dan/atau dikembangkan oleh pemilik proses bisnis sesuai dengan tugas dan fungsinya.
2. Unit Kerja bertanggung jawab atas aplikasi yang dibangun dan/atau dikembangkan.
3. Setiap Pimpinan Unit Kerja (pemilik proses bisnis) bertanggung jawab dalam penerapan standar dan prosedur pembangunan dan pengembangan aplikasi yang ada.
4. Setiap Unit Kerja yang melakukan pembangunan dan pengembangan aplikasi di Kementerian PPN/Bappenas mengikuti dan menerapkan standar dan prosedur yang ada.
5. Aplikasi yang dibangun oleh Unit Kerja memperhatikan standar dan prosedur yang bersifat terintegrasi dan mencegah adanya redudansi data.
6. Integrasi data di dalam aplikasi dapat memanfaatkan Bappenas Service Bus (BSB).

7. Penyelenggara pembangunan dan pengembangan aplikasi adalah pihak yang ditunjuk oleh pemilik proses bisnis untuk membangun dan mengembangkan aplikasi mulai dari perencanaan, implementasi, hingga pemeliharaannya.
8. Setiap kegiatan pembangunan dan pengembangan aplikasi harus dibentuk tim pembangunan dan pengembangan aplikasi yang sekurang-kurangnya terdiri atas:
    a. Manajer Proyek sekaligus dapat berperan sebagai pemilik proses bisnis, yang wajib dipimpin oleh sekurang-kurangnya 1 (satu) orang PNS,
    b. Sistem Analis,
    c. Pemrogram *(Programmer) back end/ front end/ full stack,*
    d. Penguji aplikasi.
9. Aplikasi yang dibangun dan dikembangkan oleh Unit Kerja diilakukan monitoring dan evaluasi secara berkala dan dibuktikan dengan adanya dokumen monitoring dan evaluasi aplikasi yang dilaksanakan dan disusun oleh Unit Kerja.
10. Pelaksanaan operasional, pemeliharaan, *back up* aplikasi yang telah dibangun dan/atau dikembangkan dilakukan oleh Unit Kerja.
11. Unit Kerja harus berkoordinasi dengan Pusdatinrenbang selama proses pembangunan dan pengembangan aplikasi sampai dengan operasionalisasi aplikasi.
12. Pusdatinrenbang sebagai pengatur, pembina, dan pengawas TIK di Kementerian memiliki kewenangan untuk memastikan bahwa proses pembangunan dan pengembangan telah sesuai dengan standar dan prosedur pembangunan dan pengembangan aplikasi.
13. Aplikasi yang dibangun menggunakan teknologi berbasis PHP, *database* MYSQL/ MariaDB, serta Javascript.
14. Aplikasi yang telah dikmbangkan oleh Unit Kerja di Kementerian PPN/Bappenas dengan penganggaran negara (APBN) dan hibah, serta pemanfaatannya untuk kepentingan Kementerian, perencanaan dan pengendalian pembangunan, ditempatkan

(*hosting*) di Pusat Data (*Data Center*) yang dikelola oleh Pusdatinrenbang.

15. Aplikasi yang sudah dibangun dan dikembangkan menjadi milik Kementerian dan tidak boleh digunakan di luar kepentingan Kementerian tanpa izin dari pejabat yang berwenang.

B. TANGGUNG JAWAB

1. Pihak-pihak terkait dalam proses pembangunan dan pengembangan aplikasi di Kementerian PPN/Bappenas, antara lain:

   a) Pemilik Proses Bisnis.
   b) Pusdatinrenbang.

2. Pemilik Proses Bisnis, mempunyai tanggung jawab untuk:

   a. bertanggung jawab atas aplikasi yang dikembangkan.
   b. melakukan koordinasi dengan Pusdatinrenbang sebelum membangun aplikasi agar:
      1) tidak terjadi redudansi/ duplikasi pembangunan aplikasi sejenis,
      2) mengikuti standar dan prosedur yang berlaku.
   c. menyediakan SDM secara mandiri untuk berperan sebagai:
      1) operator, melakukan pembaharuan *(updating)* konten/ isi dari aplikasi yang dibangun,
      2) pemrogram *(programmer),* melakukan pengembangan terhadap aplikasi yang telah dibangun.
   d. dalam hal pelaksanaan pengembangan aplikasi, Pemilik Proses Bisnis dapat melakukan pengembangan secara swakelola atau dapat juga melakukan pengembangan secara pihak ketiga (penyedia jasa).
   e. melaksanakan pengujian (*user acceptance testing/* UAT) terhadap fungsi-fungsi pada aplikasi yang dibangun dan dikembangkan.

f. bertanggung jawab dan memastikan bahwa aplikasi yang akan ditempatkan (*hosting*) di Pusat Data *(Data Center*) Kementerian PPN/Bappenas sudah bebas dari *bug* dan *error*.
g. bertanggung jawab atas dokumentasi yang disusun oleh Pengembang Aplikasi/Pemrogram, antara lain:
h. dokumen teknis desain perangkat lunak, serta menyampaikannya ke Pusdatinrenbang,
i. dokumen manual penggunaan sistem untuk *end user*,
j. dokumen manual penggunaan sistem untuk *admin*,
k. laporan monitoring evaluasi atau pengembangan *(versioning)* aplikasi.
l. memberikan masukan kepada pengembang aplikasi terkait pengembangan dan penyempurnaan aplikasi.
m. melakukan monitoring secara berkala, serta evaluasi pasca implementasi dan menyampaikan hasilnya kepada Pusdatinrenbang.
n. menyediakan anggaran pengembangan aplikasi dengan memperhatikan ketentuan mengenai pembiayaan TIK yang ada.
o. terkait proses pembangunan aplikasi, perlu untuk memperhatikan hal teknis antara lain:
    1) mengikuti siklus pembangunan aplikasi serta standar dan prosedur yang berlaku,
    2) menempatkan aplikasi yang akan ditempatkan (*hosting*) di Pusat Data *(Data Center)* Kementerian PPN/Bappenas sudah bebas dari *bug* dan *error*,
    3) menyusun dokumentasi sesuai standar dan prosedur, antara lain:
p. dokumen identifikasi dan analisis kebutuhan,
q. dokumen teknis desain perangkat lunak, serta menyampaikannya ke Pusdatinrenbang,
r. dokumen manual penggunaan sistem untuk *end user*.

s. dokumen manual penggunaan sistem untuk *admin*,
t. laporan monitoring evaluasi atau pengembangan *(versioning)* aplikasi.
u. menyusun laporan penyelesaian pekerjaan.

3. Pusdatinrenbang, mempunyai tanggung jawab untuk:

a. memberikan pendampingan kepada unit kerja/ Pemilik Proses Bisnis yang akan melakukan kegiatan pembangunan atau pengembangan aplikasi.
b. memastikan tidak terjadi redundansi pembangunan aplikasi untuk produk aplikasi sejenis.
c. dapat terlibat dalam proses pengujian aplikasi dan pengujian keamanan aplikasi yang akan ditempatkan *(hosting)* ke Pusat Data *(Data Center).*
d. memberikan persetujuan dalam penyusunan laporan pengendalian mutu *(quality assurance)* dalam setiap tahapan pengembangan aplikasi.
e. memastikan bahwa kegiatan pembangunan atau pengembangan aplikasi yang dihasilkan sesuai dengan standar dan prosedur pembangunan dan pengembangan aplikasi yang berlaku di Kementerian.
f. memastikan bahwa Pengembang Aplikasi/ Pemrogram telah menyusun dokumentasi sesuai standar dan prosedur.
g. menyusun Katalog Aplikasi Kementerian untuk kemudian dilaporkan kepada Sekretaris Kementerian di setiap akhir tahun anggaran.

BAB II STANDAR PROSEDUR PEMBANGUNAN DAN PENGEMBANGAN APLIKASI

Pembangunan dan pengembangan aplikasi di lingkungan Kementerian dilakukan dengan memperhatikan proses bisnis dan paling sedikit memenuhi standar dan prosedur pembangunan aplikasi sebagai berikut:

A. SIKLUS PEMBANGUNAN DAN PENGEMBANGAN APLIKASI

Terbagi menjadi beberapa tahapan yang terdiri atas:

1. Tahap analisis kebutuhan, merupakan tahapan (proses) mengumpulkan/ identifikasi dan menganalisis kebutuhan suatu bisnis untuk dibuat ke dalam suatu aplikasi dengan rinci.

    1.1 Tahap analisis kebutuhan, mencakup kegiatan:

    a. pengumpulan, analisis, penyusunan, dan pendokumentasian spesifikasi kebutuhan bisnis dan aplikasi yang mencakup:

        1) kebutuhan aplikasi termasuk fungsi kemampuan yang diinginkan, target kinerja, tingkat keamanan, dan kebutuhan spesifik lainnya.
        2) identifikasi dan analisis risiko teknologi serta rencana mitigasi.
        3) deskripsi aplikasi yang sudah ada (jika ada), dan analisis kesenjangannya (*gap analysis*) dari target aplikasi yang diinginkan.
        4) target waktu pengembangan aplikasi.
        5) rencana kapasitas (*capacity planning*).
        6) infrastruktur pendukung.

    b. pendokumentasian perubahan analisis dan spesifikasi kebutuhan aplikasi yang terjadi dalam tahap ini.

1.2 Tahap analisis kebutuhan, menghasilkan keluaran:

a) dokumentasi analisis dan spesifikasi kebutuhan aplikasi, dan

b) dokumentasi perubahan analisis dan perubahan spesifikasi kebutuhan aplikasi.

Dokumentasi-dokumentasi di atas, akan terangkum di dalam Dokumen Teknis Pembangunan Perangkat Lunak dengan *template* yang tersedia pada bagian lampiran Pedoman Teknis ini.

2. Tahap perancangan/ desain aplikasi, yaitu proses penyusunan rancangan aplikasi berdasarkan hasil identifikasi dan analisis kebutuhan, selanjutnya hasil analisis kebutuhan akan digunakan sebagai acuan dalam proses pembangunan aplikasi.

2.1 Tahap perancangan/ desain aplikasi, mencakup kegiatan:

a. Penyusunan dan pendokumentasian rancangan sistem aplikasi dan basis data, yang mencakup:

1) kebutuhan informasi dan struktur informasi.
2) penyusunan desain struktur data, relasi tabel, dan diagram alir.
3) pemetaan hak akses atas informasi oleh peran-peran yang terlibat.
4) infrastruktur pendukung yang mencakup jaringan komunikasi, sistem keamanan, *server, workstation,* perangakat pendukung, perangkat lunak dan media penyimpanan data.
5) pendokumentasian rancangan yang antara lain mencakup:

a) rancangan kebutuhan sistem aplikasi dan basis data serta infrastruktur pendukung dengan mengacu pada hasil analisis kebutuhan dan

diperjelas dengan adanya desain struktur data, relasi tabel, dan diagram alir.

b) rancangan antarmuka pengguna *(user interface)*/ rancangan tampilan untuk memasukan data *(data entry screen design),* pencarian *(inquiry),* menu bantuan, dan navigasi dari layer ke layer sesuai dengan tingkatan pengguna dan pemisahan fungsi tugas.

c) rancangan antarmuka dan integrasi sistem informasi yang lain.

d) rancangan kendali internal yang diperlukan dalam kegiatan seperti validasi, otorisasi, audit.

e) rancangan keamanan logika *(logic).*

f) rancangan proses *real-time* dan/ atau proses *batch.*

g) seluruh rancangan di atas, akan terangkum di dalam Dokumen Teknis Pembangunan Perangkat Lunak dengan *template* yang tersedia pada bagian lampiran Pedoman Teknis ini.

h) penyusunan dan pendokumentasian rancangan sistem keamanan dan sistem jaringan utama dan/atau pendukung aplikasi, yang mencakup:

6) Gambaran secara garis besar mengenai penempatan dan integrasi aplikasi pada sistem jaringan yang ada.

a) Pendokumentasian rancangan yang mencakup:

i. rancangan integrasi aplikasi dengan sistem jaringan yang sudah ada.

ii. rancangan keamanan aplikasi.

iii. rancangan penempatan dan pemasangan sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Kementerian.

b) Seluruh rancangan di atas, akan terangkum di dalam Dokumen Teknis Pembangunan Perangkat Lunak dengan *template* yang tersedia pada bagian lampiran Pedoman Teknis ini.

2.2 Tahap perancangan/ desain aplikasi, menghasilkan keluaran Dokumen Teknis Pembangunan Perangkat Lunak yang berisi rancangan-rancangan dari:

a) sistem aplikasi dan basis data, dan
b) sistem keamanan dan sistem jaringan.

3. Tahap pemrograman *(coding)* pembangunan aplikasi**,** yaitu proses yang dilakukan dengan membuat sederet kodefikasi pemrograman *(code)* untuk membangun aplikasi sesuai dengan kebutuhan proses bisnis dan berdasarkan rancangan/ desain yang telah disusun.

3.1 Tahap pemrograman *(coding)* pembangunan aplikasi, mencakup kegiatan:

a. pelaksanaan tahapan pembangunan aplikasi, yang mencakup:

1) pelaksanaan pemrograman *(coding)* aplikasi dan basis data sesuai dengan rancangan rinci yang telah disetujui.

2) pengelolaan perubahan dalam pemrograman *(coding)* aplikasi dan basis data.

3) pengendalian terhadap kode program (*source code*) yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Kementerian.

b. pendokumentasian tahapan pembangunan aplikasi, yang mencakup:

1) kode program *(source code)* disertai dengan riwayat perubahan yang terdapat penjelasan *versioning source code* menggunakan Git.

3.2 Tahap pemrograman (coding) pembangunan aplikasi, menghasilkan keluaran Akses ke *tools versioning source code* (Git) yang dapat diakses oleh pihak tertentu, yang dapat dituliskan aksesnya ke dalam Pembangunan Perangkat Lunak dengan *template* yang tersedia pada bagian lampiran Pedoman Teknis ini.

4 Tahap pengujian aplikasi, yaitu tahapan pengecekan maupun pengujian aplikasi setelah dikembangkan untuk mengetahui fungsionalitas fitur/ sistem sesuai kebutuhan.

4.1 Tahap pengujian aplikasi, mencakup kegiatan:

a. Penyusunan rencana pengujian dengan mempertimbangkan dan mencakup antara lain:

1) tujuan dan sasaran.
2) strategi dan metode, termasuk langkah-iangkah alternatif apabila aplikasi gagal dalam pengujian.
3) ruang lingkup.
4) asumsi dan batasan.
5) jadwal.
6) pihak pelaksana dan kompetensi yang dibutuhkan.
7) alat bantu.
8) bagian dari aplikasi yang akan diuji, meliputi menu, fitur, dan fungsi yang telah dibangun di dalam aplikasi.
9) kriteria penerimaan (*acceptance criteria*).
10) sumber daya yang diperlukan, termasuk penyiapan lingkungan pengujian yang mencerminkan lingkungan operasional.

b. pelaksanaan setiap jenis pengujian dengan mengacu pada rencana dan skenario. Jenis pengujian terdiri dari:

1) *User Acceptence Test* (UAT); dan
2) *Vulnerability Assesment.*

c. pelaksanaan analisis hasil pengujian.

4.2 Tahap pengujian aplikasi, menghasilkan keluaran:

a. dokumen hasil *penetration test* tanpa medium dan high treat.
b. formulir pengujian yang di dalamnya meliputi: bagian dari aplikasi yang akan diuji, hasil uji, dan analisis hasil pengujian, dengan mengikuti *template* yang tersedia pada bagian lampiran Pedoman Teknis ini. Formulir ini selanjutnya akan dituangkan ke dalam Dokumen Teknis Pembangunan Perangkat Lunak dengan *template* yang tersedia pada bagian lampiran Pedoman Teknis ini.

5 Tahap Implementasi aplikasi, merupakan proses penerapan aplikasi yang dibangun atau dikembangkan pada lingkungan operasional.

5.1 Tahap implementasi aplikasi, mencakup kegiatan:

a. persiapan rencana implementasi aplikasi yang mencakup antara lain:
   1) kebutuhan sumber daya.
   2) urutan langkah implementasi dari setiap tahap pelaksanaan implementasi aplikasi.
b. pemindahan perangkat lunak (yang sedang dibangun) dari perangkat keras *(server) developing* ke perangkat keras *(server) production.*
c. pelaksanaan *back up* aplikasi *(back up plan)* untuk mengantisipasi kegagalan dalam implementasi aplikasi.
d. implementasi aplikasi dilakukan sesuai rencana implementasi dengan memperhatikan kebijakan standar

dan prosedur pembangunan dan pengembangan aplikasi yang berlaku di Kementerian.

e. pelaksanaan pelatihan, transfer pengetahuan, dan serah terima pekerjaan.

5.2 Tahap implementasi aplikasi, menghasilkan keluaran:
Dokumen Teknis Pembangunan Perangkat Lunak yang di dalamnya terdapat:

a. penjelasan rencana implementasi aplikasi.
b. pelaksanaan kegiatan implementasi aplikasi.
c. petunjuk instalasi sistem aplikasi dan basis data.
d. penjelasan tentang rencana ataupun teknis pelaksanaan kegiatan *back up* aplikasi.
e. pedoman Penggunaan Aplikasi untuk Admin dan untuk Pengguna (sebagai lampiran).
f. dokumen Berita Acara Serah Terima Aplikasi.

6 Tahap Tinjauan aplikasi, merupakan tahapan akhir pasca implementasi aplikasi yang berisi monitoring dan evaluasi terhadap semua fitur, rencana pengembangan lanjutan bila ada.

6.1 Tahap tinjauan aplikasi, mencakup kegiatan:

a. pencapaian tujuan pembangunan aplikasi sebelumnya.
b. pemantauan terhadap pembangunan aplikasi sebelumnya.
c. pelaksanaan pengembangan aplikasi.

6.2 Tahap tinjauan aplikasi menghasilkan keluaran laporan pengelolaan dan pengembangan aplikasi atau dokumen *versioning*.

SEKRETARIS KEMENTERIAN PERENCANAAN PEMBANGUNAN NASIONAL/
SEKRETARIS UTAMA BADAN PERENCANAAN PEMBANGUNAN NASIONAL,

TAUFIK HANAFI

LAMPIRAN II
SURAT EDARAN SESMEN PPN/ SESTAMA BAPPENAS
NOMOR 2 TAHUN 2022
TENTANG
PEMBANGUNAN APLIKASI DAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI KEMENTERIAN PPN/BAPPENAS

BAB I PENGELOLAAN KEAMANAN INFORMASI SPBE

A. Organisasi Keamanan Informasi SPBE

1. Sekretaris Kementerian Perencanaan Pembangunan Nasional/Sekretaris Utama Badan Perencanaan Pembangunan Nasional selaku Penanggung Jawab, bertanggungjawab untuk:
    a. memastikan berjalannya proses pengembangan, pelaksanaan dan pemeliharaan Keamanan Informasi SPBE di Kementerian PPN/Bappenas.
    b. mengawasi pelaksanaan Keamanan Informasi SPBE untuk memastikan kehandalan dan validitas dari Keamanan Informasi SPBE.
    c. merekomendasikan penyediaan perangkat penunjang yang diperlukan untuk pelaksanaan Keamanan Informasi SPBE di Kementerian PPN/Bappenas.

d. memfasilitasi kebutuhan pengguna dan seluruh hal yang terkait dengan Keamanan Informasi SPBE.

2. Kepala Pusat Data dan Informasi Kementerian PPN/Bappenas selaku Pelaksana Teknis mempunyai tugas antara lain:

   a. menerima dan merekam laporan tentang kemungkinan terjadinya insiden Keamanan Informasi yang terkait dengan TI, baik berupa laporan dari Pengguna, dari Atasan Langsung, maupun langsung dari perangkat Sistem Informasi terkait.
   b. melakukan analisis awal terhadap laporan insiden keamanan informasi dan mengkoordinasikan penyelesaiannya dengan fungsi-fungsi terkait, seperti administrator system, dan sebagainya.

3. Pengguna yang merupakan setiap pihak yang menggunakan layanan TIK, yang memiliki tugas:

   a. sadar dan patuh terhadap seluruh peraturan yang ditetapkan dalam Keamanan Informasi SPBE dan petunjuk pendukungnya.
   b. berkontribusi secara aktif dalam melindungi Aset Kementerian PPN/Bappenas dari segala risiko Keamanan Informasi.
   c. melaporkan temuan kelemahan pengelolaan Keamanan Informasi kepada unit terkait atau Pelaksana Teknis.
   d. melaporkan segala pelanggaran Keamanan Informasi SPBE kepada Pelaksana Teknis.

4. Pejabat struktural yang merupakan atasan langsung Pengguna, bertugas untuk:

   a. melakukan fungsi pembinaan, pengawasan dan pengendalian terhadap aktivitas Pengguna yang berkaitan dengan penggunaan Informasi serta kepatuhan terhadap aturan yang berlaku.

b. memberikan teguran dan peringatan terhadap setiap pelanggaran terkait Keamanan Informasi SPBE yang dilakukan oleh Pengguna.

B. Perencanaan Keamanan Informasi SPBE

1. pelaksana teknis Keamanan SPBE melakukan Perencanaan manajemen keamanan informasi SPBE.
2. perencanaan manajemen keamanan informasi SPBE sebagaimana dimaksud pada angka 1 dilakukan untuk merumuskan program kerja keamanan informasi SPBE berdasarkan kategori risiko keamanan informasi SPBE dan target realisasi program kerja keamanan informasi SPBE.
3. program kerja manajemen keamanan informasi SPBE sebagaimana dimaksud pada angka 2 terdiri atas:
   a. edukasi kesadaran keamanan informasi SPBE bagi pegawai Kementerian PPN/Bappenas melalui sosialisasi dan/atau pelatihan.
   b. penilaian kerentanan keamanan informasi SPBE yang dapat dilakukan melalui:
      1) menginvetarisasi status dan kondisi seluruh aset informasi SPBE meliputi data dan informasi, aplikasi, dan infrastruktur.
      2) mengidentifikasi kerentanan dan ancaman terhadap aset SPBE.
      3) mengukur tingkat risiko keamanan informasi SPBE.
      4) melakukan monitoring dan evaluasi secara berkala terhadap tata Kelola keamanan informasi SPBE.
   c. koordinasi dengan pihak eksternal yang terkait dengan keamanan informasi SPBE seperti BSSN.
   d. menyusun anggaran untuk mendukung pengoperasian keamanan informasi SPBE.

C. Dukungan Pengoperasian

Koordinator SPBE melakukan dukungan pengoperasian keamanan informasi SPBE untuk meningkatkan kapasitas terhadap Sumber Daya Manusia Keamanan Informasi SPBE dan Anggaran Keamanan informasi SPBE.

1. Sumber daya manusia keamanan informasi SPBE yang memiliki kompetensi paling sedikit tentang Keamanan infrastruktur teknologi, informasi dan komunikasi, dan Keamanan aplikasi.
2. Untuk memenuhi kompetensi SDM keamanan informasi SPBE, dapat dilakukan paling sedikit melalui:
   a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi, dan keamanan aplikasi;
   b. bimbingan teknis mengenai standar Keamanan informasi SPBE.
3. Dukungan anggaran Keamanan Informasi SPBE disusun berdasarkan perencaaan yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

D. Evaluasi Kinerja Keamanan Informasi SPBE

Evaluasi kinerja Manajemen Keamanan Informasi SPBE dilakukan oleh koordinator SPBE yang dilaksanakan dengan:

1. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan informasi SPBE;
2. menetapkan indikator kinerja pada setiap area proses;
3. memformulasikan pelaksanaan Keamanan Informasi SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan.
4. menganalisis efektifitas pelaksanaan keamanan informasi SPBE;
5. mendukung dan merealisasikan program audit Keamanan informasi SPBE;
6. evaluasi kinerja dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

E. Perbaikan Berkelanjutan

1. Perbaikan berkelanjutan dilakukan oleh tim Pelaksana Teknis SPBE yang merupakan tindak lanjut dari hasil evaluasi kinerja keamanan informasi SPBE.
2. Perbaikan berkelanjutan dapat dilakukan dengan:
   a. mengatasi permasalahan dalam pelaksanaan keamanan informasi SPBE;
   b. memperbaiki pelaksanaan Keamanan Informasi SPBE secara periodik.

BAB II STANDAR TEKNIS DAN PROSEDUR KEAMANAN SPBE

A. Keamanan Data dan Informasi

Standar teknis keamanan data dan informasi terdiri atas terpenuhinya aspek kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan ketersediaan. Berikut prosedur masing-masing aspek:

1. aspek kerahasiaan, dilakukan dengan prosedur:
   a. menetapkan klasifikasi informasi.
   b. menerapkan enkripsi dengan system kriptografi.
   c. menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.
2. aspek keaslian, dilakukan dengan prosedur:
   a. menyediakan mekanisme verifikasi.
   b. menyediakan mekanisme validasi.
   c. menerapkan system *hash function.*
3. aspek keutuhan, dilakukan dengan prosedur:
   a. menerapkan pendeteksian modifikasi.
   b. menerapkan tanda tangan elektronik tersertifikasi.
4. aspek kenirsangkalan, dilakukan dengan prosedur:
   a. menerapkan tanda tangan elektronik tersertifikasi.
   b. penjaminan oleh penyelenggara sertifikat elektronik melalui sertifikat elektronik.
5. aspek ketersediaan, dilakukan dengan prosedur:
   a. menerapkan system pencadangan secara berkala.
   b. membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses.
   c. menerapkan system pemulihan.

B. Keamanan Aplikasi SPBE

Standar teknis dan prosedur keamanan Aplikasi SPBE diterapkan pada aplikasi berbasis web dan aplikasi berbasis *mobile.* Pengujian keamanan Aplikasi SPBE dapat dilakukan setiap periode tertentu dengan cara:

1. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan.
2. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan.
3. melakukan pemindaian otomatis dan/atau pengujian penetrasi system.
4. mengidentifikasi kerentatan dan mengelola ancaman sejak awal siklus pengembangan aplikasi SPBE.
5. menganalisis kerentanan.

1.1. Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:

a. authentikasi, yang dapat dilakukan dengan prosedur:

1) menggunakan manajemen kata sandi untuk proses autentikasi.
2) menerapkan verifikasi kata sandi pada sisi server.
3) mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi.
4) mengatur jumlah maksimum kesalahan dalam memasukkan kata sandi.
5) mengatur mekanisme pemulihan kata sandi.
6) menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi.
7) menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

b. Manajemen sesi, yang dapat dilakukan dengan prosedur:

1) menggunakan pengendali sesi untuk proses manajemen sesi.

2) menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi.
3) mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi.
4) mengatur kondisi dan jangka waktu habis sesi.
5) validasi dan pencantuman *session id.*
6) perlindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi.
7) perlindungan terhadap diplikasi dan mekanisme persetujuan pengguna.

c. Persyaratan Kontrol Akses yang dapat dilakukan dengan prosedur:

1. menetapkan otorisasi pengguna untuk membatasi kontrol akses.
2. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus menerus pada fungsi.
3. mengatur antarmuka pada sisi administrator.
4. mengatur verifikasi kebenaran token Ketika mengakses data dan informasi yang dikecualikan.

d. Validasi Input yang dapat dilakukan dengan prosedur:

1. menerapkan fungsi validasi input pada sisi server.
2. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi.
3. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input.
4. melakukan validasi positif pada seluruh input.
5. melakukan filter terhadap data yang tidak dipercaya.
6. menggunakan fitur kode dimanis.
7. melakukan perlindungan terhadap akses yang mengandung konten skrip.

8. melakukan perlindungan dan serangan injeksi berbasis data.

e. Terpenuhinya fungsi kriptografi pada verifikasi statis dapat dilakukan dengan prosedur:

1. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptograsi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan.
2. melakukan autentikasi data yang dienkripsi
3. menerapkan manajemen kunci kriptografi.
4. membuat angka acak yang menggunakan generator angka acak kriptograsi.

f. Penangangan eror dan pencatatan log dapat dilakukan dengan prosedur:

1. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan.
2. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani.
3. tidak mencantumkan informasi yang dikecualikan dalam pencatatan log.
4. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden.
5. mengatur perlindungan log aplikasi dari akses dan modifikasi yang tidak sah.
6. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log.
7. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

g. Proteksi data dapat dilakukan dengan prosedur:

1. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan.

2. melakukan perlindungan dari akses yang tidak sah terhadap informasi yang dikecualikasn yang disimpan sementara dalam aplikasi.
3. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan.
4. melakukan penentuan jumlah paramenter.
5. memastikan data disimpan dengan aman.
6. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna.
7. membersihkan memori setelah tidak diperlukan.

h. Keamanan komunikasi dilakukan dengan prosedur:

1. menggunakan komunikasi terenkripsi.
2. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna.
3. mengatur jenis algoritma yang digunakan dan alat pengujiannya.
4. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikat elektronik.

i. Pengendalian kode berbahaya dapat dilakukan dengan prosedur:

1. menggunakan analisis kode dalam kontrol kode berbahaya.
2. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan.
3. mengatur izin terkait fitur atau sensor terkait privasi.
4. mengatur perlindungan integritas.
5. mengatur mekanisme fitur pembaruan.

j. Terpenuhinya fungsi logika bisnis dapat dilakukan dengan prosedur:

1. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis.
2. memastikan logika bisnis memiliki batasan dan validasi.
3. memonitor aktivitas yang tidak biasa.
4. membantu dalam kontrol antiotomatisasi.
5. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

k. Terpenuhinya fungsi *file* dapat dilakukan dengan prosedur:

1. mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran file yang diunggah.
2. melakukan validasi file sesuai dengan tipe konten yang diharapkan.
3. melakukan perlindungan terhadap metadata input dan metadata file.
4. melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya.
5. melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

l. Keamanan API dan *web service* dapat dilakukan dengan prosedur:

1. melakukan konfigurasi layanan web.
2. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan.
3. membuat keputusan otorisasi.
4. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid.
5. menggunakan validasi skema dan verifikasi sebelum menerima input.
6. menggunakan metode perlindungan layanan berbasis web.
7. menerapkan kontrol antiotomatisasi.

m. Keamanan konfigurasi dapat dilakukan dengan prosedur:

1. mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan.
2. mendokumentasi, menyalin konfigurasi, dan semua dependensi.
3. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan.
4. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal.
5. menggunakan respons aplikasi dan konten yang aman.

1.2 Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi:

a. penyimpanan data dan persyaratan privasi dapat dilakukan dengan prosedur:

1. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial system.
2. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*.
3. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan.
4. melindungi informasi yang dikecualikan saat terjadi *inter process communication.*
5. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

b. fungsi kriptograsi dapat dilakukan dengan prosedur:

1. menghindari penggunaan kriptograsi simetrik dengan *hardcoded key*.
2. mengimplementasikan metode kriptograsi yang sudah teruji sesuai kebutuhan.

3. menghindari penggunaan protokol kriptograsi atau algoritma kriptograsi yang *obsolete*.
4. menghindari penggunaan kunci kriptograsi yang sama.
5. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

c. Autentikasi dan manajemen sesi dapat dilakukan dengan prosedur:

1. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh.
2. menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi.
3. memastikan server menyediakan token yang telah ditandatangani menggunakan algoritme yang aman apabila menggunakan autentikasi *stateless* berbasis token.
4. memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out.*
5. menerapkan pengaturan sandi pada *remote endpoint.*
6. membatasi jumlah percobaan *log in* pada *remote endpoint.*
7. menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint.*
8. melakukan otorisasi pada *remote endpoint.*

d. Komunikasi jaringan dapat dilakukan dengan prosedur:

1. menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolete secara konsisten.
2. memverifikasi sertifikat *remote endpoint*.

e. Interaksi platform dapat dilakukan dengan prosedur:

1. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan.

2. melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna.
3. menghindari pengiriman fungsionalitas sensitive melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*.
4. menghindari penggunaan *JavaScript* dalam *WebView.*
5. menggunakan protokol *hypertext transfer protocol secure* pada *WebView.*
6. mengimplementasikan penggunaan serialisasi API yang aman.

f. Kualitas kode dan pengaturan *build* dapat dilakukan dengan prosedur:

1. menandatangai aplikasi dengan sertifikat yang valid.
2. memastikan aplikasi dalam mode rilis.
3. menghapus symbol *debugging* dari *native binary.*
4. menghapus kode *debugging* dan kode bantuan pengembang.
5. mengidentifikasi kelemahan seluruh komponen *third party.*
6. menentukan mekanisme penanganan eror.
7. mengelola memori secara aman.
8. mengaktifkan fitur keamanan yang tersedia.

g. Fungsi ketahanan dapat dilakukan dengan prosedur:

1. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah.
2. mendeteksi dan merespons *debugger*.
3. mencegah *executable file* melakukan perubahan pada sumber daya perangkat.
4. mendeteksi dan merespons keberadaan perangkat *reverse engineering.*
5. mencegah aplikasi berjalan dalam emulator.
6. mendeteksi perubahan kode dan tata di ruang memori.

7. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat.
8. melindungi seluruh *file* dan *library* pada aplikasi.
9. menerapkan metode *obfuscation.*

E. Keamanan Sistem Penghubung Layanan

Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhinya fungsi keamanan interoperabilitas data dan informasi, kontrol system integrasi, kontrol perangkat integrator, keamanan API dan *web service,* dan keamanan migrasi data.

a. Keamanan interoperabilitas data dan informasi, dilakukan dengan prosedur:
    a. menerapkan system dan tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
    b. menerapkan system enkripsi data;
    c. memastikan data dan informasi selalu dapat diakses sesuai otoritasnya;
    d. menerapkan system *hash function* pada *file.*
b. kontrol system integrasi, dilakukan dengan prosedur:
    a. menerapkan protokol *secure socket layer* atau protokol *transfer layer security* versi terkini pada sesi pengiriman data dan informasi;
    b. menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/ internet protocol;*
    c. menerapkan system anti *distributed denial of service;*
    d. menerapkan autentikasi untuk memverifikasi identitas eksternal antar layanan SPBE yang terhubung;
    e. menerapkan manajemen keamanan sesi;
    f. menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;

g. menerapkan validasi input;
h. menerapkan kriptografi pada verifikasi statis;
i. menerapkan sertifikat elektronik pada *web authentication;*
j. menerapkan penanganan eror dan pencatatan log;
k. menerapkan proteksi data dan jalur komunikasi;
l. meneapkan pendeteksi virus untuk memeriksa bebeapa konten file;
m. menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus); dan
n. memastikan system integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

c. Kontrol perangkat integrator, dilakukan dengan prosedur:

a. menggunakan sisem operasi dan perangkat lunan dengan *security patches* terkini;
b. menggunakan anti virus dan anti-*spyware* terkini;
c. mengaktifkan fitur keamanan pada peramban web;
d. menerapkan *firewall* dan *host-based intrusion detection systems;*
e. mencegah instalasi perangkat lunak yang belum terverifikasi.
f. mencegah akses terhadap situs yang tidak sah; dan
g. mengaktifkan system *revocery* dan *restore* pada perangkat integrator.

d. Terpenuhinya Fungsi keamanan API dan *web service* dapat dilakukan dengan prosedur:

a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima api;
b. menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner, resource server* dan/atau *third party;*
c. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;

d. melindungi layanan RESTful yang menggunakan *cookie* dan *cross-site request forgery*;
e. memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valida dan tidak menyebabkan kerusakan.

e. Terpenuhinya Fungsi Keamanan migrasi data dapat dilakukan dengan prosedur:

a. memastikan migrasi data dilakukan secara bertahap dan terprogram oleh system;
b. memastikan aplikasi yang menggunakan system basis data lama tetap dipertahankan sampai system pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
c. mendokumentasikan format system basis data lama secara rinci.
d. melakukan pencadangan seluruh data yang tersimpan pada system sebelum melakukan migrasi data.
e. menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data.
f. melakukan validasi data Ketika proses migrasi data selesai.

E. Keamanan Jaringan Intra

Standar teknis keamanan Jaringan Intra diterapkan pada Jaringan Intra Pemerintah dan Jaringan Intra Instansi Pusat dan Pemerintah Daerah, dimana terdiri atas terpenuhinya: aspek administrasi keamanan Jaringan Intra, kontrol akses dan autentikasi, persyaratan perangkat dan aplikasi keamanan Jaringan Intra, kontrol keamanan *gateway,* kontrol keamanan *access point* pada jaringan nirkabel, dan kontrol konfigurasi *access point* pada jaringan nirkabel.

a. aspek administrasi keamanan Jaringai Intra dapat dilakukan dengan prosedur:

1) menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra.
2) mengidentifikasi seluruh aset infrastruktur jaringan.
3) menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra.
4) membuat laporan pengawasan keamanan jaringan secara periodik.

b. Kontrol akses dan authentikasi dapat dilakukan dengan dengan prosedur:

1) menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah.
2) menggunakan autnetikasi untuk mengakses Jaringan Intra.
3) menerapkan pembatasan akses dalam Jaringan Intra.
4) mematikan atau membatasi *protocol, port,* dan layanan yang tidak digunakan.
5) menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya.
6) menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan.
7) menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan.
8) memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi system dalam jaringan intra.
9) menerapkan *secure endpoints.*
10) memblokir layanan yang tidak dikenal.
11) menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses jaringan intra.
12) menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

c. Persyaratan perangkat dan aplikasi keamanan Jaringan Intra dapat dilakukan dengan prosedur:

1) menggunakan perangkat *security information and event management* untuk network *logging* dan *monitoring*.
2) menerapkan system deteksi dini kerentanan keamanan perangkat jaringan.
3) menggunakan perangkat *firewall*.
4) menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*.
5) menerapkan *virtual private network* terenkropsi untuk penggunaan akses jarak jauh secara terbatas.
6) menerapkan kontrol *update patching* pada infrastruktur jaringan intra dan system computer.
7) menggunakan perangkat *web application firewall*.
8) menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi.
9) memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisir celah peretas.
10) mengunduh perangkat lunak melalui *enterprise software distribution system*.
11) menerapkan sertifikat elektronik.

d. Kontrol keamanan *gateway* dapat dilakukan dengan prosedur:

1) menerapkan *content filering*.
2) menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada jaringan intra.
3) menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*.
4) memastikan perangkat *gateway* yang menghubungkan antar jaringan intra tidak terkoneksi langsung dengan jaringan publik.
5) melaksanakan manajemen *traffic gateway*.
6) memastikan *port* tidak terbuka secara default.

e. Kontrol keamanan *access point* pada jaringai nirkabel dapat dilakukan dengan prosedur:

1) menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini.
2) menerapkan *media access kontrol* pada *address filtering.*
3) menerapkan *dedicated service set identifier*.
4) menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan.
5) menerapkan pembatasan terkait penambahan perangkat nirkabel yang terpasang secara tidak sah.
6) menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan.
7) melakukan *patching firmware* secara rutin.

f. Kontrol konfigurasi *access point* pada jaringan nirkabel dapat dilakukan dengan prosedur:

1) menggunakan kata sandi yang kuat.
2) menggunakan protokol model *authentication, authorization, dan accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point.*
3) memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan.

4) mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel.
5) menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

SEKRETARIS KEMENTERIAN PERENCANAAN PEMBANGUNAN NASIONAL/
SEKRETARIS UTAMA BADAN PERENCANAAN PEMBANGUNAN NASIONAL,

TAUFIK HANAFI