PEMERINTAH KABUPATEN MUARA ENIM
DINAS KOMUNIKASI DAN INFORMATIKA
Jln. Bambang Utoyo No. 19 Kel. Pasar III Muara Enim, 3 1 3 1 4
Sumatera SelatanTelp / Fax(0734) 421175
e-mail:diskominfo@muaraenimkab.go.id Website:www.muaraenimkab.go.id

KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MUARA ENIM
NOMOR 9 /KPTS/DISKOMINFO-III/2022

TENTANG

TIM PELAKSANA MANAJEMEN KEAMANAN
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
PEMERINTAH KABUPATEN MUARA ENIM

Menimbang :

a. bahwa dalam rangka untuk melaksanakan keamanan informasi sistem pemerintahan berbasis elektronik sesuai dengan ketentuan Pasal 41 ayat (4) dan Pasal 48 ayat (5) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
b. bahwa untuk mendukung penyelenggaraan Tugas Pokok dan Fungsi Dinas Komunikasi dan Informatika Kabupaten Muara Enim dalam pelaksanaan keamanan informasi sistem pemerintahan berbasis elektronik;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Kepala Dinas Komunikasi dan Infromatika Kabupaten Muara Enim Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.

Mengingat :

1. Undang-Undang Nomor 28 Tahun 1959 tentang Pembentukan Daerah Tingkat II dan Kota Praja di Sumatera Selatan (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 1821);
2. Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
3. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah, (Lembaran Negara Republik

Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887);

4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Nomor 182 Tahun 2018);
5. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 8 Tahun 2019 Tentang Penyelenggaraan Urusan Pemerintahan Konkuren Bidang Komunikasi dan Informatika;
6. Peraturan Badan Siber Dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah;
7. 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;
8. Peraturan Daerah Nomor 2 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah sebagaimana telah diubah dengan Peraturan Daerah Nomor 8 Tahun 2019 tentang Perubahan Atas Peraturan Daerah Kabupaten Muara Enim Nomor 2 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Muara Enim Tahun 2019 Nomor 8);
9. Peraturan Bupati Muara Enim Nomor 64 Tahun 2018 Tentang Perubahan Kedua Atas Peraturan Bupati Nomor 31 Tahun 2016 Tentang Susunan, Kedudukan, Tugas Fungsi dan Struktur Organisasi Inspektorat, Satuan Polisi Pamong Praja, Dinas, Badan, Kecamatan dan Kelurahan.

MEMUTUSKAN :

Menetapkan :

KESATU : Tim Pelaksana Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

KEDUA : Tim Pelaksana Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik, sebagai berikut :

No	Kedudukan	Nama/Jabatan
1.	Pembina	Kepala Dinas Komunikasi dan Informatika
2.	Penanggung Jawab	Kepala Bidang Persandian dan Keamanan Informasi
3.	Ketua Pelaksana	Sub-Koordinator Keamanan Informasi
4.	Anggota	Sub- Koordinator Pengawasan dan Evaluasi Persandian
5.	Anggota	Pengelola Keamanan Sistem Informasi

KETIGA : Tim Pelaksana Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik sebagaimana terlampir pada Diktum KESATU, dituangkan dalam lampiran Surat Keputusan ini dan menjadi satu kesatuan yang tidak terpisah dengan Surat Keputusan ini;

KEEMPAT : Segala biaya yang timbul akibat dikeluarkannya Keputusan ini dibebankan kepada Anggaran Organisasi Perangkat Daerah Dinas Komunikasi dan Informatika Kabupaten Muara Enim;

KELIMA : Keputusan ini mulai berlaku pada tanggal diterapkan dengan ketentuan apabila terdapat kekeliruan dalam penetapan ini akan diperbaiki sebagaimana mestinya;

Ditetapkan di Muara Enim
Pada Tanggal, 4 Januari 2022

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA,

ARDIAN ARIFANARDI, A.P., M.Si.
Pembina Utama Muda
NIP. 197407201993111001

LAMPIRAN : KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MUARA ENIM
NOMOR : 9 /KPTS/ DISKOMINFO-III/2022
TANGGAL : 4 Januari 2022
TENTANG : Tim Pelaksana Manajemen Keamanan Sistem Pemerintahan Berbasis Elektronik

TATA CARA DAN STANDAR TEKNIS MANAJEMEN KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

I. Pedoman Umum

Pedoman manajemen keamanan informasi SPBE merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi:

a. penetapan ruang lingkup;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan.

Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE paling sedikit meliputi

a. data dan informasi SPBE
b. Aplikasi SPBE
c. aset Infrastruktur SPBE
d. kebijakan keamanan informasi SPBE yang telah dimiliki.

II. Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik

Standar teknis dan prosedur Keamanan SPBE diterapkan untuk:

1. Keamanan data dan informasi

   Standar teknis keamanan data dan informasi terdiri atas terpenuhinya aspek :

   a) Kerahasiaan

      aspek kerahasiaan dilakukan dengan prosedur :

      - menetapkan klasifikasi informasi
      - menerapkan enkripsi dengan sistem kriptografi
      - menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

ditetapkan.

b) Keaslian

aspek keaslian dilakukan dengan prosedur :

- menyediakan mekanisme verifikasi
- menyediakan mekanisme validasi
- menerapkan sistem hash function.

c) Keutuhan

aspek keutuhan dilakukan dengan prosedur menerapkan pendeteksian modifikasi dan menerapkan tanda tangan elektronik tersertifikasi.

d) Kenirsangkalan

aspek kenirsangkalan dilakukan dengan prosedur menerapkan tanda tangan elektronik tersertifikasi dan penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

e) ketersediaan.

Aspek ketersediaan dilakukan dengan prosedur:

- menerapkan sistem pencadangan secara berkala
- membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses
- menerapkan sistem pemulihan.

2. Keamanan Aplikasi SPBE

A. aplikasi berbasis web

Aplikasi berbasis web merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet. Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:

a) autentikasi

Terpenuhinya fungsi autentikasi dilakukan dengan prosedur:

- menggunakan manajemen kata sandi untuk proses autentikasi;
- menerapkan verifikasi kata sandi pada sisi server;
- mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
- mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
- mengatur mekanisme pemulihan kata sandi;
- menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi;
- menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

b) manajemen sesi

Terpenuhinya fungsi manajemen sesi dilakukan dengan prosedur:

- Menggunakan pengendali sesi untuk proses manajemen sesi
- menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi
- mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi
- mengatur kondisi dan jangka waktu habis sesi
- validasi dan pencantuman session id
- pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi
- pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.

c) persyaratan kontrol akses

Terpenuhinya fungsi persyaratan kontrol akses dilakukan dengan prosedur:

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

d) validasi input

Terpenuhinya fungsi validasi input dilakukan dengan prosedur:

- menerapkan fungsi validasi input pada sisi server
- menerapkan mekanisme penolakan input jika terjadi kesalahan validasi
- memastikan runtime environment aplikasi tidak rentan terhadap serangan validasi input
- melakukan validasi positif pada seluruh input
- melakukan filter terhadap data yang tidak dipercaya;
- menggunakan fitur kode dinamis
- melakukan pelindungan terhadap akses yang mengandung konten skrip
- melakukan pelindungan dari serangan injeksi basis data.

e) kriptografi pada verifikasi statis

Terpenuhinya fungsi kriptografi pada verifikasi statis dilakukan dengan prosedur:

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

f) penanganan eror dan pencatatan log

Terpenuhinya fungsi penanganan eror dan pencatatan log dilakukan dengan prosedur:

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

g) proteksi data

Terpenuhinya fungsi proteksi data dilakukan dengan prosedur:

- melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan
- melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi
- melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan
- melakukan penentuan jumlah parameter
- memastikan data disimpan dengan aman
- menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna

- membersihkan memori setelah tidak diperlukan.

h) keamanan komunikasi

Terpenuhinya fungsi keamanan komunikasi dilakukan dengan prosedur:

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

i) pengendalian kode berbahaya

Terpenuhinya fungsi pengendalian kode berbahaya dilakukan dengan prosedur:

- menggunakan analisis kode dalam kontrol kode berbahaya;
- memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan
- mengatur izin terkait fitur atau sensor terkait privasi
- mengatur pelindungan integritas
- mengatur mekanisme fitur pembaruan.

j) logika bisnis

Terpenuhinya fungsi logika bisnis dilakukan dengan prosedur:

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

k) File

Terpenuhinya fungsi file dilakukan dengan prosedur:

- mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah
- melakukan validasi file sesuai dengan tipe konten yang diharapkan
- melakukan pelindungan terhadap metadata input dan metadata file
- melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya
- melakukan konfigurasi server untuk mengunduh file sesuai

ekstensi yang ditentukan.

l) keamanan API dan web service

Terpenuhinya fungsi keamanan API dan web service dilakukan dengan prosedur:

- melakukan konfigurasi layanan web
- memverifikasi uniform resource identifier API tidak menampilkan informasi yang berpotensi sebagai celah keamanan
- membuat keputusan otorisasi
- menampilkanmetode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid
- menggunakan validasi skema dan verifikasi sebelum menerima input
- menggunakan metode pelindungan layanan berbasis web
- menerapkan kontrol antiotomatisasi.

m) keamanan konfigurasi

Terpenuhinya fungsi keamanan konfigurasi dilakukan dengan prosedur:

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

B. Aplikasi berbasis mobile

Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi:

a) penyimpanan data dan persyaratan privasi

Terpenuhinya fungsi penyimpanan data dan persyaratan privasi dilakukan dengan prosedur:

- menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem
- membatasi pertukaran data dan informasi yang dikecualikan dengan third party
- menonaktifkan cache keyboard pada saat memasukkan data dan informasi yang dikecualikan
- melindungi informasi yang dikecualikan saat terjadi inter

process communication
- melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

b) Kriptografi

Terpenuhinya fungsi kriptografi dilakukan dengan prosedur:
- menghindari penggunaan kriptografi simetrik dengan hardcoded key
- mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan
- menghindari penggunaan protokol kriptografi atau algoritme kriptografi yang obsolet
- menghindari penggunaan kunci kriptografi yang sama
- menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

c) autentikasi dan manajemen sesi

Terpenuhinya fungsi autentikasi dan manajemen sesi dilakukan dengan prosedur:
- menerapkan autentikasi pada remote endpoint terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh
- menggunakan session identifier yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan stateful manajemen sesi
- memastikan server menyediakan token yang telah ditandatangani menggunakan algoritme yang aman apabila menggunakan autentikasi stateless berbasis token
- memastikan remote endpoint memutus sesi yang ada saat pengguna log out
- menerapkan pengaturan sandi pada remote endpoint
- membatasi jumlah percobaan log in pada remote endpoint
- menentukan masa berlaku sesi dan masa kedaluwarsa token pada remote endpoint
- melakukan otorisasi pada remote endpoint.

d) komunikasi jaringan

Terpenuhinya fungsi komunikasi jaringan dilakukan dengan prosedur:
- menerapkan secure socket layer atau transport layer security yang tidak obsolet secara konsisten
- memverifikasi sertifikat remote endpoint.

e) interaksi platform

Terpenuhinya fungsi interaksi platform dilakukan dengan prosedur:

- memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan
- melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna
- menghindari pengiriman fungsionalitas sensitif melalui skema custom uniform resource locator dan fasilitas inter process communication
- menghindari penggunaan JavaScript dalam WebView
- menggunakan protokol hypertext transfer protocol secure pada WebView
- mengimplementasikan penggunaan serialisasi API yang aman.

f) kualitas kode dan pengaturan build

Terpenuhinya fungsi kualitas kode dan pengaturan build dilakukan dengan prosedur:

- menandatangani aplikasi dengan sertifikat yang valid
- memastikan aplikasi dalam mode rilis
- menghapus simbol debugging dari native binary
- menghapus kode debugging dan kode bantuan pengembang
- mengidentifikasi kelemahan seluruh komponen third party
- menentukan mekanisme penanganan eror
- mengelola memori secara aman
- mengaktifkan fitur keamanan yang tersedia.

g) Ketahanan

Terpenuhinya fungsi ketahanan dilakukan dengan prosedur:

- mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah
- mendeteksi dan merespons debugger
- mencegah executable file melakukan perubahan pada sumber daya perangkat
- mendeteksi dan merespons keberadaan perangkat reverse engineering
- mencegah aplikasi berjalan dalam emulator
- mendeteksi perubahan kode dan data di ruang memori
- menerapkan fungsi device binding dengan menggunakan property unik pada perangkat;
- melindungi seluruh file dan library pada aplikasi

- menerapkan metode obfuscation.

3. Keamanan Sistem Penghubung Layanan

   Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhinya fungsi:

   a) keamanan interoperabilitas data dan informasi

      Terpenuhinya fungsi keamanan interoperabilitas data dan informasi dilakukan dengan prosedur:

      - menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik
      - menerapkan sistem enkripsi data
      - memastikan data dan informasi selalu dapat diakses sesuai otoritasnya menerapkan sistem hash function pada file.

   b) kontrol sistem integrasi

      Terpenuhinya fungsi kontrol sistem integrasi dilakukan dengan prosedur:

      - menerapkan protokol secure socket layer atau protokol transport layer security versi terkini pada sesi pengiriman data dan informasi
      - menerapkan internet protocol security untuk mengamankan transmisi data dalam jaringan berbasis transmission control protocol/internet protocol
      - menerapkan sistem anti distributed denial of service
      - menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung
      - menerapkan manajemen keamanan sesi
      - menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan
      - menerapkan validasi input
      - menerapkan kriptografi pada verifikasi statis
      - menerapkan sertifikat elektronik pada web authentication
      - menerapkan penanganan eror dan pencatatan log
      - menerapkan proteksi data dan jalur komunikasi
      - menerapkan pendeteksi virus untuk memeriksa beberapa konten file
      - menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus)
      - memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

c) kontrol perangkat integrator

Terpenuhinya fungsi kontrol perangkat integrator dilakukan dengan prosedur:

- menggunakan sistem operasi dan perangkat lunak dengan security patches terkini
- menggunakan anti virus dan anti-spyware terkini
- mengaktifkan fitur keamanan pada peramban web
- menerapkan firewall dan host-based intrusion detection systems
- mencegah instalasi perangkat lunak yang belum terverifikasi
- mencegah akses terhadap situs yang tidak sah
- mengaktifkansistem recovery dan restore pada perangkat integrator.

d) keamanan API dan web service

Terpenuhinya fungsi keamanan API dan web service dilakukan dengan prosedur:

- menerapkan protokol secure socket layer atau protokol transport layer security diantara pengirim dan penerima API
- menerapkan protokol open authorization versi terkini untuk menjembatani interaksi antara resource owner, resource server dan/atau third party
- menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid
- melindungi layanan web RESTful yang menggunakan cookie dari cross-site request forgery
- memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

e) keamanan migrasi data

Terpenuhinya fungsi keamanan migrasi data dilakukan dengan prosedur:

- memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem
- memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
- mendokumentasikan format sistem basis data lama secara rinci
- melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data

- menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data
- melakukan validasi data ketika proses migrasi data selesai.

4. Keamanan Jaringan Intra

Standar teknis keamanan Jaringan Intra terdiri atas terpenuhinya:

a) aspek administrasi keamanan Jaringan Intra

Terpenuhinya aspek administrasi keamanan Jaringan Intra dilakukan dengan prosedur:

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

b) kontrol akses dan autentikasi

Terpenuhinya kontrol akses dan autentikasi dilakukan dengan prosedur:

- menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah
- menggunakan autentikasi untuk mengakses Jaringan Intra
- menerapkan pembatasan akses dalam Jaringan Intra
- mematikan atau membatasi protocol, port, dan layanan yang tidak digunakan
- menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya
- menerapkan fungsi honeypot untuk menganalisis celah keamanan berdasarkan jenis serangan
- menerapkan virtual private network dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan
- memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra
- menerapkan secure endpoints
- memblokir layanan yang tidak dikenal
- menerapkan secure socket layer atau transport layer security versi terkini pada jalur akses Jaringan Intra
- menerapkan server perantara saat client mengakses server database dalam rangka pemeliharaan.

c) persyaratan perangkat dan aplikasi keamanan Jaringan Intra

Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra dilakukan dengan prosedur:

- menggunakan perangkat security information and event management untuk network logging dan monitoring
- menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan
- menggunakan perangkat firewall
- menggunakan perangkat intrusion detection systems dan intrusion prevention systems
- menerapkan virtual private network terenkripsi untuk penggunaan akses jarak jauh secara terbatas
- menerapkan kontrol update patching pada infrastruktur Jaringan Intra dan sistem komputer
- menggunakan perangkat web application firewall
- menggunakan perangkat load balancer untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi
- memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
- mengunduh perangkat lunak melalui enterprise software distribution system
- menerapkan sertifikat elektronik.

d) kontrol keamanan gateway

Terpenuhinya kontrol keamanan gateway dilakukan dengan prosedur:

- menerapkan content filtering
- menerapkan inspection packet filtering untuk memeriksa packet yang masuk pada Jaringan Intra
- menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat gateway
- memastikan perangkat gateway yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik
- melaksanakan manajemen traffic gateway
- memastikan port tidak dibuka secara default

e) kontrol konfigurasi access point pada jaringan nirkabel

Terpenuhinya kontrol konfigurasi access point pada jaringan nirkabel dilakukan dengan prosedur:

- menggunakan kata sandi yang kuat
- menggunakan protokol model authentication authorization dan accounting pada perangkat infrastruktur jaringan

untuk management user atau otentikasi administrator access point

- memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan
- mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel
- menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

f) kontrol keamanan access point pada jaringan nirkabel

Terpenuhinya kontrol keamanan access point pada jaringan nirkabel dilakukan dengan prosedur:

- menerapkan protokol keamanan access point nirkabel dan teknologi enkripsi terkini
- menerapkan media access control pada address filtering
- menerapkan dedicated service set identifier
- menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan
- menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah
- menerapkan manajemen vulnerability secara berkala dan berkelanjutan
- melakukan patching firmware secara rutin.

5. Keamanan Pusat Data

Standar teknis keamanan Pusat Data sebagaimana dimaksud terdiri atas terpenuhinya:

a) persyaratan keamanan fisik dan manajemen Pusat Data

Terpenuhinya persyaratan keamanan fisik dan manajemen Pusat Data dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.

b) persyaratan koneksi perangkat ke Pusat Data

Terpenuhinya persyaratan koneksi perangkat ke Pusat Data dilakukan dengan prosedur:

- memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data
- memutus akses fisik atau logic dari perangkat yang tidak terotorisasi
- memastikan akses tingkat administrator ke server dan perangkat jaringan utama tidak boleh dilakukan secara

- memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data
- melakukan backup informasi dan perangkat lunak yang berada di Pusat Data Nasional secara berkala
- memastikan perangkat komputer Pusat Data terbebas dari virus dan malware
- melakukan pembatasan akses pemanfaatan removable media di area Pusat Data
- memastikan pengaktifan konfigurasi port universal serial bus telah mendapatkan izin dari personil yang berwenang
- memastikan setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data Nasional menggunakan internet protocol address dan hostname yang telah ditentukan
- menerapkan server perantara saat client mengakses server database dalam rangka pemeliharaan.

Ditetapkan di Muara Enim
Pada Tanggal, 4 Januari 2022

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA,

DINAS KOMUNIKASI DAN INFORMATIKA

ARDIAN ARIFANARDI, A.P., M.Si.
Pembina Utama Muda
NIP. 197407201993111001