COACHING CLINIC

KEGIATAN PERSANDIAN PEMERINTAH DAERAH

Cholilah, S.E., M.M.

Rizki Barokah, S.Tr.TP

DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAH DAERAH

BADAN SIBER DAN SANDI NEGARA

KEWENANGAN PEMERINTAH DAERAH DALAM UU 23 TAHUN 2014 BIDANG PERSANDIAN

SUB URUSAN	PEMERINTAH PUSAT	DAERAH PROVINSI	DAERAH KAB/KOTA
PERSANDIAN UNTUK PENGAMANAN INFORMASI	1. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Pusat. 2. Penetapan pola hubungan komunikasi sandi antarkementerian/lembaga, antara Pemerintah Pusat dengan Daerah provinsi dan Daerah kabupaten/kota. 3. Pengelolaan kunci sandi.	1. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah provinsi. 2. Penetapan pola hubungan komunikasi sandi antarPerangkat Daerah provinsi.	1. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah kabupaten/kota. 2. Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah kabupaten/kota.

BADAN SIBER DAN SANDI NEGARA

KEGIATAN/SUB KEGIATAN URUSAN PERSANDIAN (1/2) merefer pada Kepmendagri 900.1.15.5-3406 Tahun 2024

Kegiatan: 2.21.02.2.01-Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah

No	Kode	Sub Kegiatan	Kinerja	Indikator	Satuan
1	2.21.02.1.01.0001 2.21.02.2.01.0001	Penetapan Kebijakan Tata Kelola Keamanan Informasi dan Jaring Komunikasi Sandi Pemerintah Daerah Provinsi	Ditetapkannya Kebijakan Tata Kelola Keamanan Informasi dan Jaring Komunikasi Sandi Pemerintah Daerah Provinsi	Jumlah Kebijakan Tata Kelola Keamanan Informasi dan Jaring Komunikasi Sandi Pemerintah Daerah yang Ditetapkan	Dokumen
2	2.21.02.1.01.0002 2.21.02.2.01.0002	Pelaksanaan Analisis Kebutuhan dan Pengelolaan Sumber Daya Keamanan Informasi Pemerintah Daerah Provinsi	Terlaksananya Analisis Kebutuhan dan Pengelolaan Sumber Daya Keamanan Informasi Pemerintah Daerah Provinsi	Jumlah Laporan Analisis Kebutuhan dan Pengelolaan Sumber Daya Keamanan Informasi Pemerintah Daerah Provinsi	Laporan
3	2.21.02.1.01.0003 2.21.02.2.01.0003	Pelaksanaan Keamanan Informasi Pemerintahan Daerah Provinsi Berbasis Elektronik dan Non Elektronik	Terlaksananya Keamanan Informasi Pemerintahan Daerah Provinsi Berabasis Elektronik dan Non Elektronik	Jumlah Laporan Pelaksanaan Keamanan Informasi Pemerintahan Daerah Provinsi Berbasis Elektronik dan Non Elektronik	Laporan
4	2.21.02.1.01.0004 2.21.02.2.01.0004	Penyediaan Layanan Keamanan Informasi Pemerintah Daerah Provinsi	Tersedianya Layanan Keamanan Informasi untuk Perangkat Daerah di Tingkat Provinsi	Jumlah Perangkat Daerah yang Telah Menggunakan Layanan Keamanan Informasi	Perangkat Daerah

BADAN SIBER DAN SANDI NEGARA

KEGIATAN/SUB KEGIATAN URUSAN PERSANDIAN (2/2) merefer pada Kepmendagri 900.1.15.5-3406 Tahun 2024

Kegiatan: 2.21.02.2.02-Penetapan Pola Hubungan Komunikasi Sandi Antar Perangkat Daerah

No	Kode	Sub Kegiatan	Kinerja	Indikator	Satuan
1	2.21.02.1.02.0001 2.21.02.2.02.0001	Operasionalisasi Jaring Komunikasi Sandi Pemerintah Daerah Provinsi	Terlaksananya Operasioalisasi Jaring Komunikasi Sandi Perangkat Daerah	Jumlah Perangkat Daerah yang Terhubung dalam Jaring Komunikasi Sandi	Perangkat Daerah

BADAN SIBER DAN SANDI NEGARA

Pelaksanaan Persandian Untuk Keamanan Informasi di Pemda Peraturan BSSN Nomor 10 Tahun 2019

A. Penyusunan Kebijakan Pengamanan Informasi

Yang harus pemerintah daerah susun:

- Rencana Strategis Pengamanan Informasi
- Arsitektur Keamanan Informasi
- Aturan Tata Kelola Keamanan Informasi

B. Pengelolaan Sumber Daya Keamanan Informasi

Yang terdiri dari:

- Pengelolaan Aset Keamanan TIK
- Pengelolaan SDM
- Manajemen Pengetahuan

BADAN SIBER DAN SANDI NEGARA

Pelaksanaan Persandian Untuk Keamanan Informasi di Pemda Peraturan BSSN Nomor 10 Tahun 2019

C. Pengamanan Sistem Elektronik dan Pengamanan Informasi Non Elektronik

Pengamanan Sistem Elektronik

PENJAMINAN

- ❑ Kerahasiaan
- ❑ Keutuhan
- ❑ Ketersediaan
- ❑ Nir-sangkal

- ❑ Ketersediaan Infrastruktur

- ❑ Keutuhan, Ketersediaan, dan Keaslian Aplikasi

- Pusat Data
- Jaringan Intra
- Sistem Penghubung Layanan

- Identifikasi
- Proteksi
- Deteksi
- Insiden Respon

Sertifikat Elektronik → Balai Sertifikasi Elektronik → Penyelenggaraan SPBE

Pengamanan Informasi Non-Elektronik

- Pemrosesan
- Pengiriman
- Penyimpanan
- Pemusnahan

Dalam penyelenggaraan fungsi huruf C ini, Pemerintah Daerah perlu melaksanakan:

AUDIT KEAMANAN INFORMASI

- Audit Keamanan Sistem Elektonik
- Audit Pelaksanaan Sistem Manajemen

BADAN SIBER DAN SANDI NEGARA

Pelaksanaan Persandian Untuk Keamanan Informasi di Pemda Peraturan BSSN Nomor 10 Tahun 2019

D. Penyediaan Layanan Keamanan Informasi

Ditujukan kepada:

- Kepala Daerah dan Wakil
- Perangkat Daerah
- Pegawai & Aparatur Sipil
- Pihak Lainnya

Maka pemda perlu membentuk dan Menyusun:

Pedoman Manajemen Layanan Keamanan Informasi

Mengacu pada:

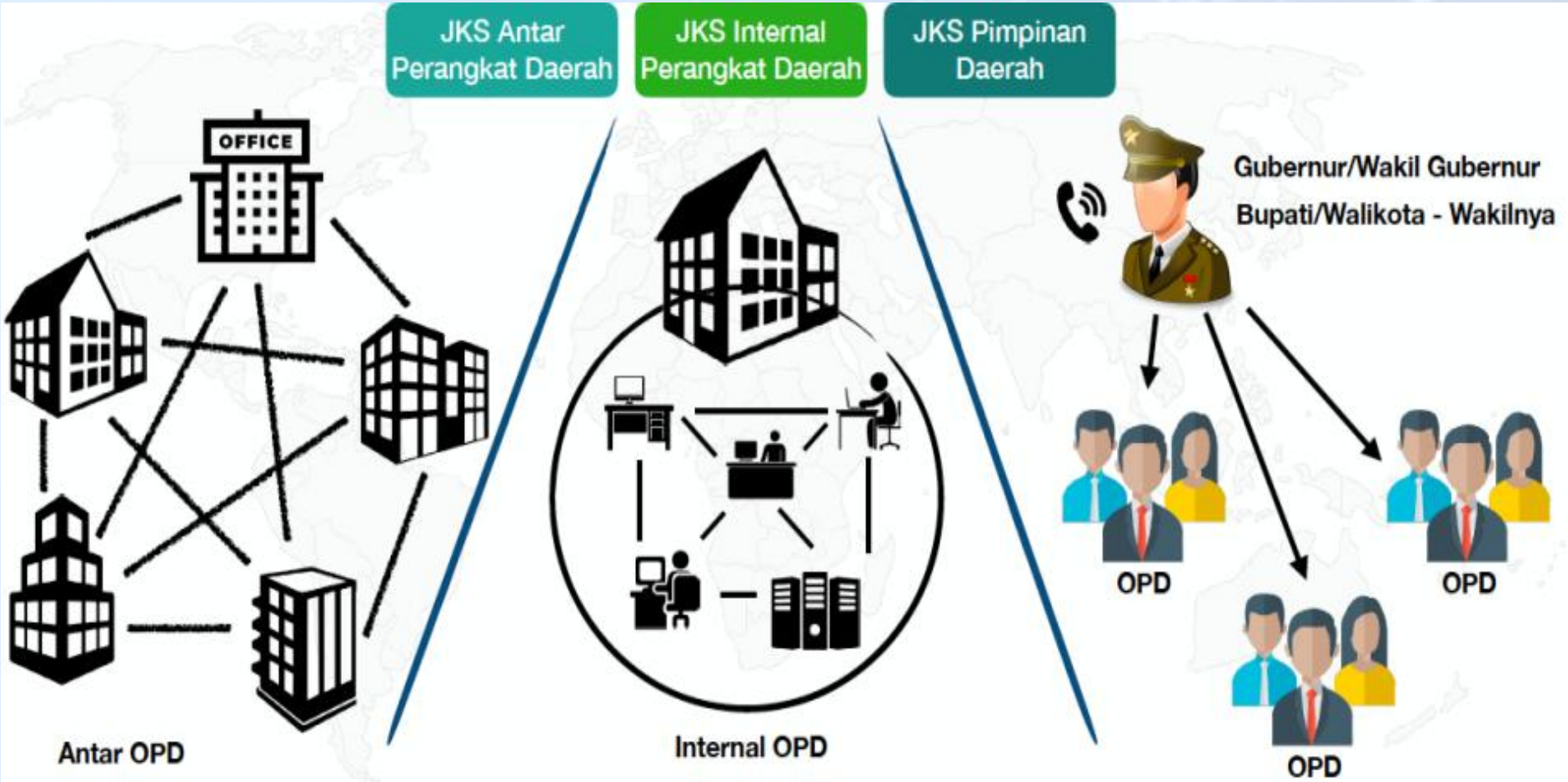
Peraturan BSSN Nomor 4 Tahun 2021

JENIS LAYANAN KEAMANAN INFORMASI

Identifikasi Kerentanan & Penilaian Resiko	Peningkatan Kompetensi SDM
Asistensi & Fasilitas Penguatan	Pengelolaan Pusops Paminfo
Penerapan Sertifikat Elektronik	Penanganan Insiden Paminfo
Penyediaan Perangkat Kaminfo & JKS	Forensik Digital
Sertifikasi Manajemen Kaminfo	Pengamanan Sinyal
Audit Keamanan Sistem Elektronik	Kontra Penginderaan
Audit Keamanan Pelaksanaan Sistem Manajemen	Konsultasi Keamanan Informasi
Literasi Keamanan Informasi	Layanan Kaminfo Lainnya

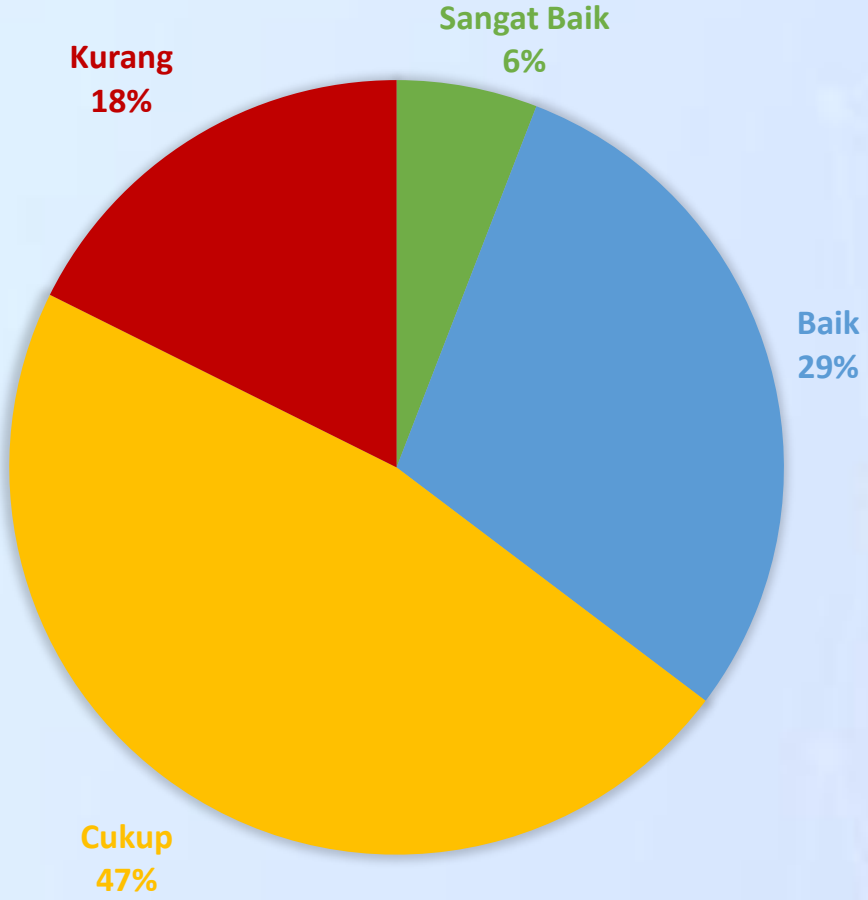
Pelaksanaan Persandian Untuk Keamanan Informasi di Pemda Peraturan BSSN Nomor 10 Tahun 2019

E. Pola Hubungan Komunikasi Sandi



BADAN SIBER DAN SANDI NEGARA

Profil Kepatuhan Pelaksanaan Pengamanan Informasi



Hasil Pengukuran
Tahun 2024

Area Pengukuran

1. Kebijakan Pengamanan Informasi
2. Pengelolaan Sumber Daya Keamanan Informasi
3. Pengamanan Sistem Elektronik dan Informasi Non-Elektronik
4. Layanan Keamanan Informasi
5. Pola Hubungan Komunikasi Sandi

Tingkat Kepatuhan	2022	2023	2024
Sangat Baik	0	1	2
Baik	4	8	10
Cukup	17	17	16
Kurang	13	8	6

Upaya Peningkatan Kinerja Urusan Persandian

Penetapan NSPK Urusan Persandian

Sebagai Pedoman dalam pelaksanaan urusan Persandian untuk pengamanan Informasi

Fasilitasi Layanan Keamanan Informasi

Asistensi penguatan fungsi Persandian melalui layanan Keamanan Informasi sebagaimana tercantum dalam penetapan nomenklatur program dan kegiatan bidang Persandian Tahun 2025-2026

Fasilitasi Peningkatan Kematangan Keamanan Siber

Pendampingan perbaikan Tata Kelola Keamanan Siber untuk mendorong peningkatan kerjasama lintas bidang maupun Pemda dalam rangka perbaikan nilai kematangan keamanan siber

Peningkatan Kapabilitas Sumber Daya Pemda

Melalui kegiatan pendampingan, asistensi, literasi, bimtek, workshop dan cyberdrill keamanan siber secara periodik

Rapat Koordinasi Urusan Persandian

Sarana pembinaan dan pengawasan teknis urusan Persandian yang dikolaborasikan dengan kegiatan tahunan CSIRT/TTIS

Lampiran I.
Nomor : 5451/BSSN/D3/PS.02.01/11/2022
Tanggal : 30 November 2022

Contoh Format

GUBERNUR/BUPATI/WALI KOTA [NAMA DAERAH]

PERATURAN [JABATAN PIMPINAN DAERAH] [NAMA DAERAH]
NOMOR TAHUN

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
DI LINGKUNGAN [NAMA PEMDA]

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR/WALI KOTA/BUPATI [NAMA DAERAH],

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan [Nama Pemda], perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi; (opsi konsideran 1 landasan akademis digunakan jika tidak ada peraturan sebelumnya yang mengamanatkan);

a. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan [Nama Pemda] dari segala jenis

---

TERBATAS

BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar No .70, Kel. Duren Mekar, Kec Bojong Sari, Depok 16518
Telepon (021) 77973360, Faksimile (021) 78844104, 77973579
***Website*: https://bssn.go.id , *E-mail*: humas@bssn.go.id**

Nomor : T.113/BSSN/D3/KS.02.05/01/2025 Depok, 15 Januari 2025
Klasifikasi : Terbatas
Lampiran : 1 berkas
Hal : Permintaan Laporan Hasil Pemantauan dan Evaluasi Pelaksanaan Urusan Persandian Pemda T.A 2024

Yth. 1. Kepala Dinas Komunikasi dan Informatika Provinsi se - Indonesia
2. Kepala Dinas Komunikasi dan Informatika Kabupaten/Kota se - Indonesia

di -
Tempat

1. Dasar:
   a. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana terakhir kali diubah dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah;
   b. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; dan
   c. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah.
2. Dalam rangka melaksanakan ketentuan Pasal 26 dan Pasal 27 Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah, dimohon agar Perangkat Daerah pelaksana urusan persandian di Pemerintah Daerah menyampaikan Laporan Pemantauan dan Evaluasi Pelaksanaan Urusan Persandian periode Januari s.d Desember T.A 2024 sebagaimana contoh terlampir.
3. Ketentuan penyampaian Laporan Pemantauan dan Evaluasi Pelaksanaan Urusan Persandian merujuk ketentuan pada Pasal 26 Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah, yaitu:

BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar Nomor 70, Kel. Bojongsari Lama, Kec. Bojongsari, Depok 16518
Telepon (021) 77973360, Faksimile (021) 78844104, 77973579
***Website* : https://bssn.go.id, *E-mail* : humas@bssn.go.id**

Nomor : 1746/BSSN/D3/KS.02.01/03/2025 Depok, 4 Maret 2025
Sifat : Biasa
Lampiran : 4 (empat) berkas
Perihal : Penyampaian Pedoman Penetapan Nomenklatur Program Kegiatan Urusan Persandian 2025-2027 serta Pemetaan Satuan Unit Kerja Pelaksana Urusan Persandian

Kepada Yth.
(Daftar Terlampir)
di tempat

1. Dasar :
   a. Undang-Undang 23 Tahun 2014 tentang Pemerintahan Daerah;
   b. Peraturan Pemerintah Republik Indonesia Nomor 18 Tahun 2016 Tentang Perangkat Daerah;
   c. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara;
   d. Peraturan Menteri Dalam Negeri Nomor 18 Tahun 2020 tentang Peraturan Pelaksanaan Peraturan Pemerintah Nomor 13 Tahun 2019 tentang Laporan dan Evaluasi Penyelenggaraan Pemerintahan Daerah;
   e. Peraturan Menteri Dalam Negeri Nomor 90 Tahun 2021 tentang Klasifikasi, Kodefikasi, dan Nomenklatur Perencanaan Pembangunan dan Keuangan Daerah;
   f. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
   g. 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.
2. Dalam mendukung pelaksanaan persandian di pemerintah daerah oleh Badan Perencanaan Pembangunan Daerah (Bappeda) dan Dinas Komunikasi dan Informatika (Diskominfo) dengan merujuk pada Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah bahwa Diskominfo melaksanakan program atau kegiatan Layanan Keamanan Informasi.

PEDOMAN
PENETAPAN NOMENKLATUR PROGRAM DAN KEGIATAN BIDANG PERSANDIAN JENIS LAYANAN KEAMANAN INFORMASI DI PEMERINTAH DAERAH
PERIODE 2025-2027

LAYANAN KEAMANAN INFORMASI

Kegiatan atau program kerja dalam satu tahun anggaran yang harus dilaksanakan sebagai bagian dari kegiatan persandian di Pemerintah Daerah

PRINSIP KEAMANAN

1. Kerahasiaan
2. Keutuhan
3. Ketersediaan
4. Keaslian
5. Kenirsangkalan

MANDATORY

Pekerjaan yang harus dilaksanakan unit kerja pengampu keamanan siber dan sandi yang diamanatkan dalam Peraturan Perundang-undangan dalam mendukung penyelenggaraan persandian untuk pengamanan informasi

OPSIONAL

Pekerjaan yang dapat dipilih untuk dilaksanakan unit kerja pengampu keamanan siber dan sandi dalam mendukung penyelenggaraan persandian untuk pengamanan informasi

2.21.02.1.01.01
2.21.02.2.01.01

PENETAPAN KEBIJAKAN TATA KELOLA KEAMANAN INFORMASI DAN JARING KOMUNIKASI SANDI PEMERINTAH DAERAH

- Pekerjaan Mandatory

1.Penyusunan Kebijakan Internal Manajemen Keamanan Informasi proses merumuskan sampai dengan mengevaluasi kebijakan internal untuk melindungi aset informasi suatu organisasi di lingkungan Pemerintah Daerah

- Output
  Dokumen Kebijakan Internal
- Outcome
  Kepatuhan terhadap Kebijakan

SALINAN

MENTERI
PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA

PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 59 TAHUN 2020
TENTANG
PEMANTAUAN DAN EVALUASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BADAN SIBER DAN SANDI NEGARA
Jalan Raya Muchtar Nomor 70, Kel. Bojongsari Lama, Kec. Bojongsari, Depok 16518
Telepon (021) 77973360, Faksimile (021) 78844104, 77973579
Website : https://bssn.go.id, E-mail : humas@bssn.go.id

Nomor : 5451/BSSN/D3/PS.02.01/11/2022 Jakarta, 30 November 2022
Sifat : Biasa
Lampiran : 1 (satu) berkas
Perihal : Penyampaian Contoh Format Kebijakan Internal Manajemen Keamanan Informasi SPBE

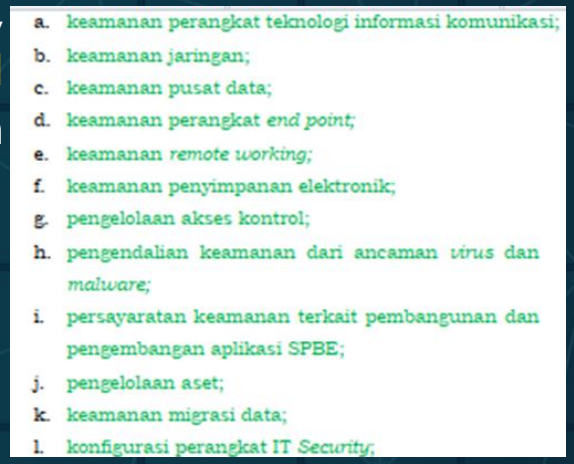
Kepada Yth.
1. Kepala Dinas Komunikasi dan Informatika Provinsi Se Indonesia
2. Kepala Dinas Komunikasi dan Informatika Kabupaten/Kota Se Indonesia
di
Tempat

1. Dasar :
   a. Peraturan Presiden Nomor 98 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE);
   b. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE;
   c. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi SPBE;
   d. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2021 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2021 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi.
2. Berdasarkan dasar tersebut diatas, khususnya amanat dari Permen PAN & RB Nomor 59 Tahun 2020 pada indikator 8 tentang keharusan tersedianya kebijakan internal manajemen keamanan informasi SPBE, selain itu kebijakan tersebut juga merupakan dokumen yang

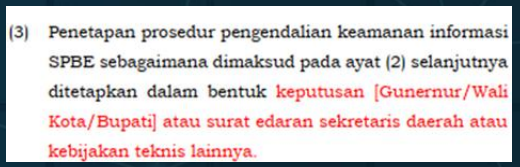
- Pekerjaan Opsional

2.Penyusunan Pedoman Teknis Kebijakan Internal Manajemen Keamanan Informasi proses merumuskan sampai dengan mengevaluasi aturan, prosedur, dan pedoman teknis berdasarkan Kebijakan Internal Manajemen Keamanan Informasi di lingkungan Pemerintah Daerah

- Output
  Dokumen Pedoman Teknis Kebijakan Internal Manajemen Keamanan Informasi
- Outcome
  Implementasi Kebijakan yang Konsisten



a. keamanan perangkat teknologi informasi komunikasi;
b. keamanan jaringan;
c. keamanan pusat data;
d. keamanan perangkat *end point*;
e. keamanan *remote working*;
f. keamanan penyimpanan elektronik;
g. pengelolaan akses kontrol;
h. pengendalian keamanan dari ancaman *virus* dan *malware*;
i. persayaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat IT *Security*;



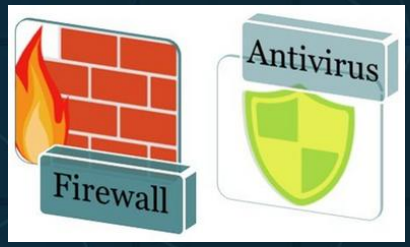
(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk keputusan [Gunernur/Wali Kota/Bupati] atau surat edaran sekretaris daerah atau kebijakan teknis lainnya.

2.21.02.1.01.02
2.21.02.2.01.02

PELAKSANAAN ANALISIS KEBUTUHAN DAN PENGELOLAAN SUMBER DAYA KEAMANAN INFORMASI PEMERINTAH DAERAH

- Pekerjaan Mandatory

1.Analisis Kebutuhan Sumber Daya Keamanan Siber dan Sandi proses untuk mengidentifikasi dan menentukan sumber daya yang diperlukan untuk melindungi sistem dan informasi dari ancaman siber dalam menjalankan pelayanan publik di Pemerintah Daerah



- Output
  Laporan Analisis Kebutuhan Sumber Daya Keamanan Siber dan Sandi
- Outcome
  Meningkatnya kepatuhan organisasi

2.Pengukuran Tingkat Kematangan Keamanan Siber proses verifikasi atas evaluasi pelaksanaan persandian di organisasi dalam penerapan keamanan informasi

- Output
  Laporan Penilaian Kematangan
- Outcome
  Peningkatan Kematangan Keamanan

INDEKS KEAMANAN INFORMASI

IKAS Pemerintahan

2.21.02.1.01.02
2.21.02.2.01.02
PELAKSANAAN ANALISIS KEBUTUHAN DAN PENGELOLAAN SUMBER DAYA KEAMANAN INFORMASI PEMERINTAH DAERAH

- Pekerjaan Opsional

1.Pengembangan Kompetensi Sumber Daya Manusia bidang Keamanan Siber dan Sandi

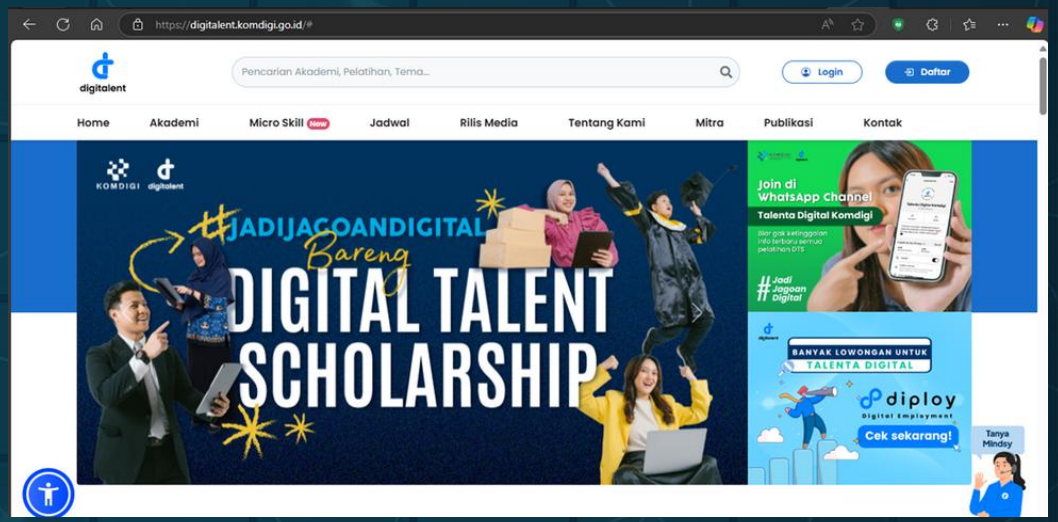
langkah fundamental Pemerintah Daerah dalam menghadapi tantangan keamanan siber yang semakin kompleks. Sumber Daya Manusia yang memiliki pengetahuan dan kompetensi merupakan aset Pemerintah Daerah sebagai penggerak untuk melindungi data, dan mencegah serangan siber yang dapat merugikan organisasi.

- Output

Sertifikat Pelatihan

- Outcome

Peningkatan Kompetensi SDM

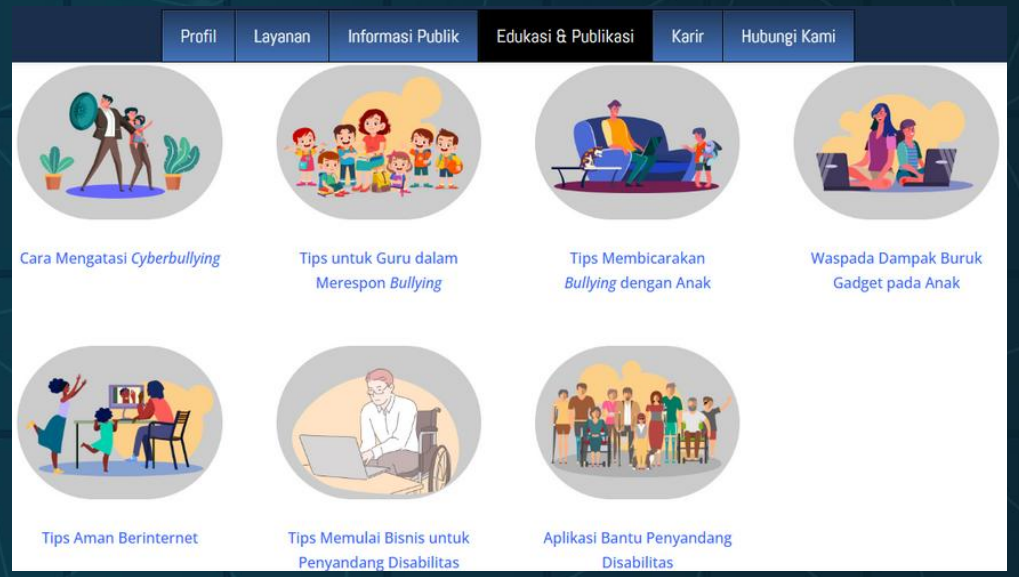


2.21.02.1.01.03
2.21.02.2.01.03
PELAKSANAAN KEAMANAN INFORMASI PEMERINTAHAN DAERAH BERBASIS ELEKTRONIK DAN NON ELEKTRONIK

- Pekerjaan Mandatory

1.Edukasi Kesadaran Keamanan SPBE

upaya meningkatkan kesadaran dan pengetahuan tentang keamanan SPBE di lingkungan Pemerintah Daerah untuk memastikan pelindungan data, kelancaran layanan publik berbasis elektronik, dan mencegah kerugian yang lebih besar.



- Output
  Laporan Kegiatan Edukasi
- Outcome
  Peningkatan Kesadaran Keamanan

2.Penilaian Kerentanan Keamanan SPBE

proses untuk mengidentifikasi, menganalisis, dan mengevaluasi kelemahan atau kerentanan yang ada dalam Sistem Elektronik SPBE Pemerintah Daerah

- Output
  Laporan Identifikasi Kerentanan
- Outcome
  Mitigasi Kerentanan

2.21.02.1.01.03
2.21.02.2.01.03
PELAKSANAAN KEAMANAN INFORMASI PEMERINTAHAN DAERAH BERBASIS ELEKTRONIK DAN NON ELEKTRONIK

- Pekerjaan Mandatory

3.Peningkatan Keamanan SPBE

upaya yang dilakukan untuk memperkuat pelindungan terhadap sistem, data, dan layanan SPBE di Pemerintah Daerah setelah dilaksanakannya Penilaian Kerentanan Keamanan SPBE

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

- Output
  Laporan Peningkatan Keamanan SPBE
- Outcome
  Peningkatan Keamanan Sistem

4.Penanganan Insiden SPBE

upaya untuk merespons dan mengatasi insiden keamanan siber yang terjadi pada Sistem Elektronik SPBE

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2020
TENTANG
TIM TANGGAP INSIDEN SIBER

- Output
  Laporan Insiden
- Outcome
  Pemulihan Sistem yang Cepat

GOV-CSIRT INDONESIA

2.21.02.1.01.03
2.21.02.2.01.03
PELAKSANAAN KEAMANAN INFORMASI PEMERINTAHAN DAERAH BERBASIS ELEKTRONIK DAN NON ELEKTRONIK

- Pekerjaan Mandatory

5.Penilaian Risiko Keamanan Informasi

proses sistematis dan berkesinambungan yang dilakukan Pemerintah Daerah untuk mengidentifikasi, mengevaluasi, dan memprioritaskan potensi ancaman dan kerentanan terhadap organisasi

- Output
  Laporan Penilaian Risiko
- Outcome
  Pengurangan Risiko

NO	ASET/PROSES/LAYANAN	DESKRIPSI RISIKO - DAMPAK (*RISK DESCRIPTION - IMPACT*)				PEMILIK RISIKO (*RISK OWNER*)	PENGENDALIAN YANG ADA (*EXISTING CONTROL*)	RISIKO SAAT INI (*CURRENT RISK*)			KEPUTUSAN
		Kerawanan (*Vulnerability*)	Ancaman (*Threat*)	Aspek Risiko (C / I / A)	Uraian Dampak (*Impact Description*)			Kemungkinan (*Likelihood*)	Nilai Dampak (*Impact Score*)	Nilai Risiko (*Risk Score*)	
1	2	3	4	5	6	10	11	12	13	14	15
A	INFORMASI (Cetak/Elektronik)										
1	Data Pribadi Pengguna	belum optimalnya prosedur back up data pengguna	informasi hilang/data corrupt	*Availability*	Adanya kebocoran informasi terhadap data pribadi yang digunakan	Kepala Dinas Kominfo	melakukan prosedur backup data pada server lain	Possible	Critical	Critical	Mitigate
B	SOFTWARE (Software aplikasi, S/W sistem, development tools)										
1	Aplikasi A	pengujian software yang masih terbatas	penyalahgunaan hak akses oleh pihak yang tidak berwenang	*Integrity*	Terganggunya Layanan	Kepala Dinas Kominfo	melakukan kontrol akses administrator pada saat mengakses databese	Possible	High	High	Mitigate
C	INFRASTRUKTUR HARDWARE & NETWORK										
1	Router	tidak dilakukan konfigurasi secara aman sesuai standar	adanya serangan terhadap router	*Confidentiality*	Potensi adanya celah lubang keamanan dari serangan DOS	Kepala Dinas Kominfo	melakukan pencatatan konfigurasi yang telah dilakukan	Unlikely	Critical	High	Mitigate
D	SARANA PENDUKUNG (UTILITY)										
1	UPS	belum optimalnya mekanisme pemeliharaan UPS	tidak berfungsinya UPS	*Availability*	Terganggunya Layanan	Kepala Dinas Kominfo	pembuatan jadwal pemeriksaan UPS	Unlikely	Medium	Medium	Mitigate
E	SUMBER DAYA MANUSIA & PIHAK KETIGA										
1	Programer	Adanya kesulitan dalam melakukan modifikasi pemrograman.	Pemrograman tidak terstruktur sulit dibaca.	Availability	ditemukannya bugs dan terdapat error	Kepala Dinas Kominfo	melakukan pendokumentasian dengan menggunakan gitlab	Unlikely	Medium	Medium	Mitigate

Kategori Risiko	Risiko Inheren	Risiko Residual Saat Ini	Risiko Residual Yang Diharapkan
Risiko Penyalahgunaan Kontrol Akses	RENDAH	RENDAH	RENDAH
Risiko Pencurian Data Pribadi	RENDAH	RENDAH	RENDAH
Risiko Insiden Web Defacement	TINGGI	TINGGI	RENDAH
Risiko Keamanan Cloud Service	RENDAH	TINGGI	RENDAH
Risiko Keamanan Infrastruktur	SEDANG	SEDANG	RENDAH
Risiko Ketidaksesuaian Pengelolaan Aplikasi	RENDAH	RENDAH	RENDAH
Risiko Kesalahan Pengelolaan Data dan Informasi Terbatas	RENDAH	RENDAH	RENDAH
Risiko Kesalahan Pengelolaan SDM	RENDAH	RENDAH	RENDAH
Risiko Kesalahan Pengelolaan Aset	TINGGI	TINGGI	RENDAH
Risiko Kesalahan Pengelolaan oleh Pihak Ketiga	RENDAH	RENDAH	RENDAH
Risiko Terganggunya Keberlangsungan Layanan	SEDANG	RENDAH	RENDAH
Risiko Serangan Malware	TINGGI	EKSTRIM	RENDAH

2.21.02.1.01.03
2.21.02.2.01.03
PELAKSANAAN KEAMANAN INFORMASI PEMERINTAHAN DAERAH BERBASIS ELEKTRONIK DAN NON ELEKTRONIK

- Pekerjaan Opsional

1.Pengadaan Perangkat Keamanan TIK

proses dari analisis kebutuhan, pengadaan, pengujian, implementasi dan pemeliharaan perangkat lunak dan perangkat keras untuk melindungi Sistem Elektronik Pemerintah Daerah dari ancaman siber

- Output
  Perangkat Keamanan TIK
- Outcome
  Peningkatan Keamanan Sistem

2.Pelindungan Informasi melalui pengamanan sinyal dan kegiatan kontra penginderaan

kegiatan antisipasi dan pencegahan dini di lingkungan Pemerintah Daerah terhadap kebocoran dan pencurian informasi oleh pihak yang tidak bertanggung jawab.

- Output
  Laporan Hasil Kegiatan
- Outcome
  Antisipasi dan pencegahan dini di lingkungan Pemerintah Daerah terhadap kebocoran dan pencurian informasi kedinasan yang berklasifikasi

2.21.02.1.01.03
2.21.02.2.01.03
PELAKSANAAN KEAMANAN INFORMASI PEMERINTAHAN DAERAH BERBASIS ELEKTRONIK DAN NON ELEKTRONIK

- Pekerjaan Opsional

3.Pendampingan Pelaksanaan Audit Keamanan SPBE

proses bantuan teknis yang diberikan oleh Dinas Komunikasi dan Informatika kepada Inspektorat dalam melakukan audit keamanan SPBE di lingkup Pemerintah Daerah

- Output
  Laporan Audit Keamanan
- Outcome
  Peningkatan Keamanan SPBE

SALINAN

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

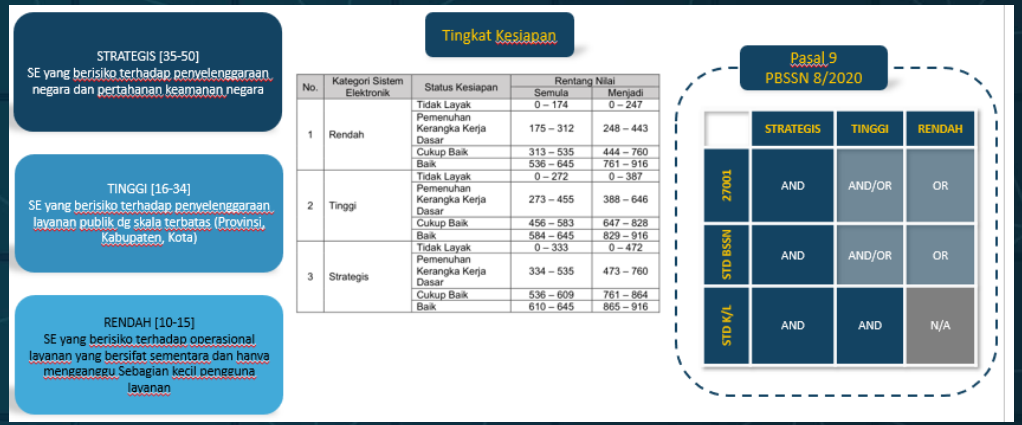
PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR 16 TAHUN 2022
TENTANG
KEBIJAKAN UMUM PENYELENGGARAAN
AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2024
TENTANG
STANDAR DAN TATA CARA PELAKSANAAN AUDIT KEAMANAN
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

4.Kategorisasi Sistem Elektronik

bagian dari penyelenggaraan Sistem Manajemen Pengamanan Informasi yang merupakan pengaturan kewajiban bagi Penyelenggara Sistem Elektronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko

- Output
  Hasil penilaian mandiri dan verifikasi atas kategorisasi sistem elektronik
- Outcome
  Terciptanya kategorisasi Sistem Elektronik yang dimiliki oleh Penyelenggara Sistem Elektronik

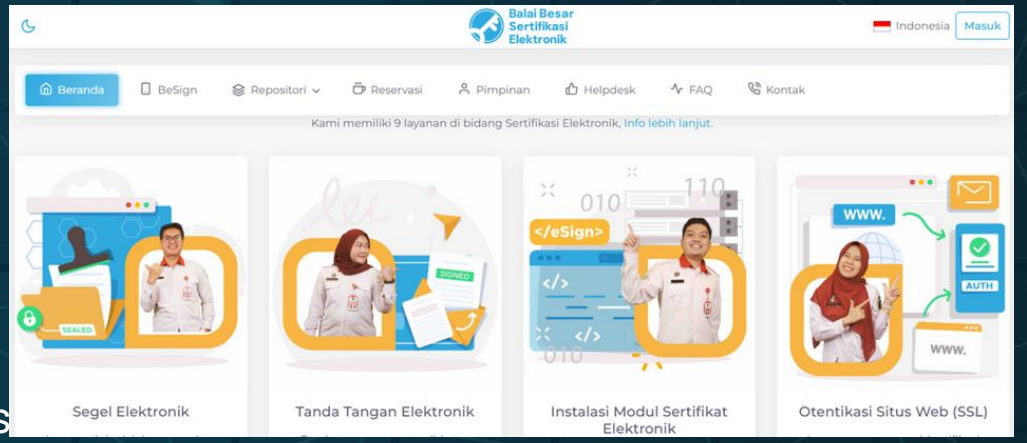


2.21.02.1.01.04
2.21.02.2.01.04
PENYEDIAAN LAYANAN KEAMANAN INFORMASI PEMERINTAH DAERAH

- Pekerjaan Mandatory

1.Penerapan Sertifikat Elektronik

pemanfaatan sertifikat yang bersifat elektronik oleh Pemerintah Daerah yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik



- Output
  Laporan Penerbitan Sertifikat
- Outcome
  Peningkatan Keamanan Transaks Elektronik

2.Analisis Pengguna dan Pengelola Layanan Keamanan Informasi

proses untuk memahami kebutuhan, harapan, dan perilaku pengguna serta pengelola terkait dengan layanan keamanan informasi Pemerintah Daerah

- Output
  Laporan Analisis Pengguna dan Pengelola
- Outcome
  Peningkatan Efektivitas Layanan

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;
b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
c. sarana dan prasarana yang digunakan; dan
d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
a. kepala daerah dan wakil;
b. perangkat daerah;
c. pegawai atau aparatur sipil negara pada pemerintah daerah; dan
d. pihak lainnya.

2.21.02.1.01.04
2.21.02.2.01.04
PENYEDIAAN LAYANAN KEAMANAN INFORMASI PEMERINTAH DAERAH

- Pekerjaan Opsional

1.Pengelolaan Pusat Operasi Pengamanan Informasi/ SOC

salah satu fungsi pendukung pelaksanaan keamanan informasi dan teknologi dalam suatu organisasi. SOC terdiri atas tim keamanan siber yang ditugaskan untuk melakukan pemantauan dan analisa keamanan organisasi serta merespon potensi pelanggaran di keamanan siber

- Output
  Laporan Kegiatan Monitoring Keamanan Siber
- Outcome
  Meningkatkan postur keamanan siber nasional

2.Pengelolaan Informasi Dini Serangan Siber Melalui Honeynet

salah satu sistem deteksi dini ancaman siber yang dapat digunakan untuk mendukung terciptanya ranah siber yang aman dan tahan dari serangan siber

- Output
  Laporan Log Monitoring Sensor Honeypot
- Outcome
  Memberikan deteksi dini serangan siber

https://www.bssn.go.id/honeynet-project/

2.21.02.1.02.01
2.21.02.2.02.01
OPERASIONALISASI JARING KOMUNIKASI SANDI PEMERINTAH DAERAH

- Pekerjaan Mandatory

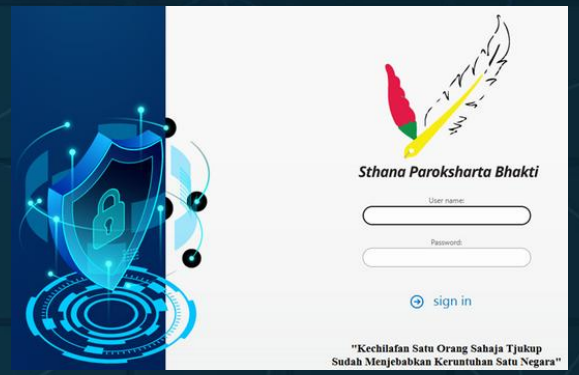
1.Penyusunan dan Implementasi Keputusan Kepala Daerah terkait Pola Hubungan Komunikasi Sandi langkah strategis untuk memastikan keamanan informasi di lingkungan Pemerintah Daerah. Keputusan ini menjadi landasan hukum bagi pengelolaan komunikasi sandi yang efektif, terutama dalam melindungi data-data sensitif pemerintah dan mencegah kebocoran informasi

- Output

Dokumen Keputusan Kepala Daerah

- Outcome

Keamanan Informasi yang Meningkat



BAB III

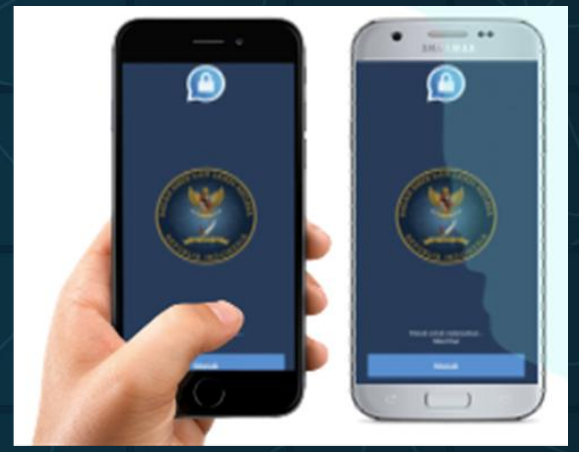
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH PROVINSI DAN KABUPATEN/KOTA

Pasal 24

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota sebagaimana dimaksud dalam Pasal 3 huruf b ditetapkan oleh Gubernur dan Bupati/Wali Kota.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:

a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;
b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
c. sarana dan prasarana yang digunakan; dan
d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.



PEDOMAN
PEMETAAN SATUAN UNIT KERJA PELAKSANA URUSAN PERSANDIAN

- Outcome

Menguatnya keamanan siber dan sandi lingkungan Pemerintah Daerah

- Indikator Kinerja Kunci Outcome

Persentase Tingkat Kematangan Keamanan Siber dan Sandi Pemerintah Daerah

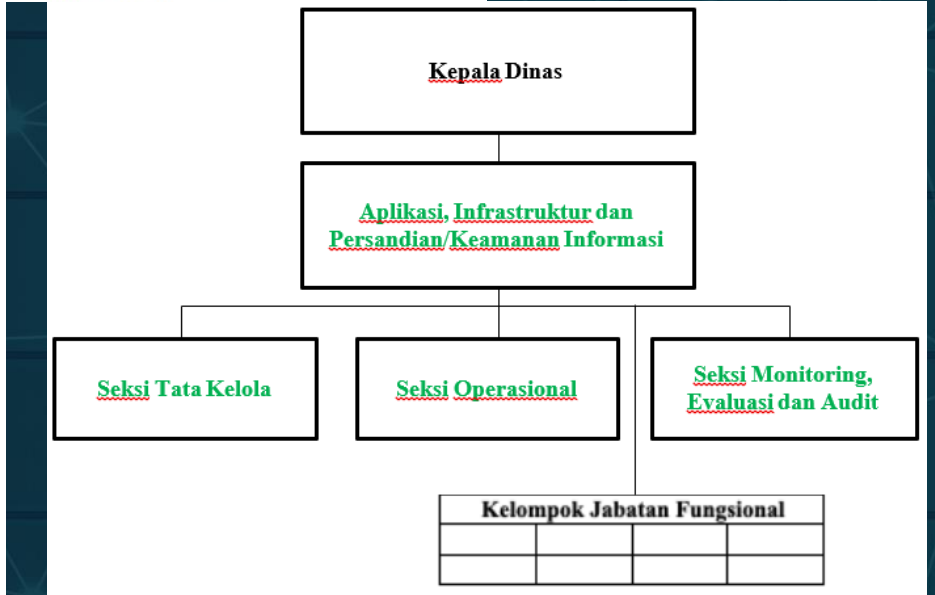
- Alat ukur

Indeks Keamanan Informasi

SALINAN

PRESIDEN
REPUBLIK INDONESIA

PERATURAN PEMERINTAH REPUBLIK INDONESIA
NOMOR 18 TAHUN 2016
TENTANG
PERANGKAT DAERAH



Tipe Dinas Daerah: **A B C**

Tugas dan Fungsi Bidang urusan persandian:

- **pengamanan informasi elektronik** (aplikasi dan infrastruktur)
- **pengamanan informasi non elektronik**

Proses bisnis keamanan:

- **berjalan** dan **dipimpin** oleh Bidang urusan persandian
- **berkoordinasi** pada bidang yang mengelola aplikasi dan infrastruktur dan bidang terkait

SDM Bidang urusan persandian:

- **Fungsional Sandiman**
- **Fungsional Manggala Informatika**

TERIMA KASIH

https://s.id/LayananD32

Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
kss.pemda@bssn.go.id
kss.pemda@sanapati.net