Peningkatan Kapasitas CSIRT dalam Mendukung Ketahanan Siber Kota Magelang

Penerapan Praktik Dasar Keamanan Siber pada 29 OPD & 17 Kelurahan

2

2 November 2026

RISTANTORO
DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAH DAERAH

Amanat Regulasi

01

Perpres 95 Tahun 2018 ttg SPBE

Pasal 41

(1) Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan SPBE

02

Perpres 82 tahun 2022 ttg Perlindungan Infrastruktur Informasi Vital

Pasal 11

(1) Penanganan insiden siber dilaksanakan oleh Tim Tanggap Insiden Siber

Pasal 12

(3) Penyelenggara IIV membentuk Tim Tanggap Insiden Siber organisasi

03

Peraturan BSSN 1 tahun 2024 ttg Pengelolaan Insiden Siber

Pasal 3 (1)

Penanganan insiden siber dilaksanakan oleh Tim Tanggap Insiden Siber organisasi

04

PP 71 Tahun 2019 ttg Penyelenggaraan Sistem dan Transaksi Elektronik

Pasal 24

(2) PSE wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkana ganggua, kegagalan, dan kerugian.

05

Peraturan BSSN 4 tahun 2021 ttg Pedoman MKI SPBE

Pasal 8 (3)

Program kerja keamanan SPBE paling sedikit meliputi :

a. edukasi kesadaran keamanan SPBE
b. penilaian kerentanan keamanan SPBE
c. peningkatan keamanan SPBE
d. penanganan insiden keamanan SPBE, dan
e. audit keamanan SPBE

Peraturan Pemerintah (PP) Nomor 33 Tahun 2026
adalah aturan pelaksana resmi dari Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) di Indonesia.

Implikasi UU No. 27 Tahun 2022 tentang PDP bagi Badan Publik

Tanggung Jawab Pengendali Data

OPD dan Kelurahan wajib menjaga keamanan data kependudukan dan layanan publik dari kebocoran.

Kewajiban Notifikasi 3×24 Jam

Insiden kegagalan perlindungan data pribadi wajib dilaporkan ke Lembaga PDP dan pemilik data.

Sanksi Hukum & Administratif

Peringatan tertulis, penghentian pemrosesan data, hingga sanksi pidana atas penyalahgunaan data.



Tim Tanggap Insiden Siber - CSIRT

> sekelompok orang yang bertanggung jawab melakukan pengelolaan penanganan Insiden Siber pada lingkup organisasi atau institusi.

sekelompok profesional ini bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas penanganan insiden keamanan siber.



TREN ANCAMAN SIBER PADA INSTANSI PEMERINTAH

WASPADA PERGESERAN POLA SERANGAN DI ERA SPBE

6 ANCAMAN SIBER UTAMA

1

RANSOMWARE & DOUBLE EXTORTION
Penguncian data penting & ancaman pembucoran dokumen rahasia.

2

KEBOCORAN DATA (DATA BREACH)
Eksploitasi celah aplikasi web & penjualan basis data.

3

PHISHING BERBASIS AI
Pesan spear-phishing tingkat tinggi pencuri kredensial ASN.

4

SUPPLY CHAIN ATTACKS
Peretasan melalui celah keamanan aplikasi pihak ketiga / vendor IT.

5

DDOS
Membanjiri lalu lintas layanan publik sast momen puncak (CPNS/PPDB)

6

HACKTIVISM & DEFACEMENT
Mengubah tampilan situs web (.go.id) untuk tujuan pulitik dan merusak reputasi.

FAKTOR PENGHAMBAT KERENTANAN UTAMA

Akses Tanpa MFA: Penggunaan kata sandi lemah & belum ada verifikasi ganda.



Sistem Outdated: Keterlambatan pembaruan keamanan pada server dan CMS.



Human Error: Rendahnya kesadaran keamanan siber di lingkungan pegawai.



4 PILAR MITIGASI STRATEGIS



PENGUATAN CSIRT
Respons cepat penanganan insiden (containment & recovery).

PRINSIP ZERO TRUST
Verifikasi ketat seluruh akses jaringan dan pengguna.

AUDIT KEAMANAN BERKALA
Penetration testing & asesmen kematangan (IKASANDI/TMPI).

KEPATUHAN UU PDP
Enkripsi ketat dan perlindungan data pribadi masyarakat.

Sumber Data: Analisis Lanskap Keamanan Siber SPBE

Keamanan Siber Adalah Tanggung Jawab Bersama

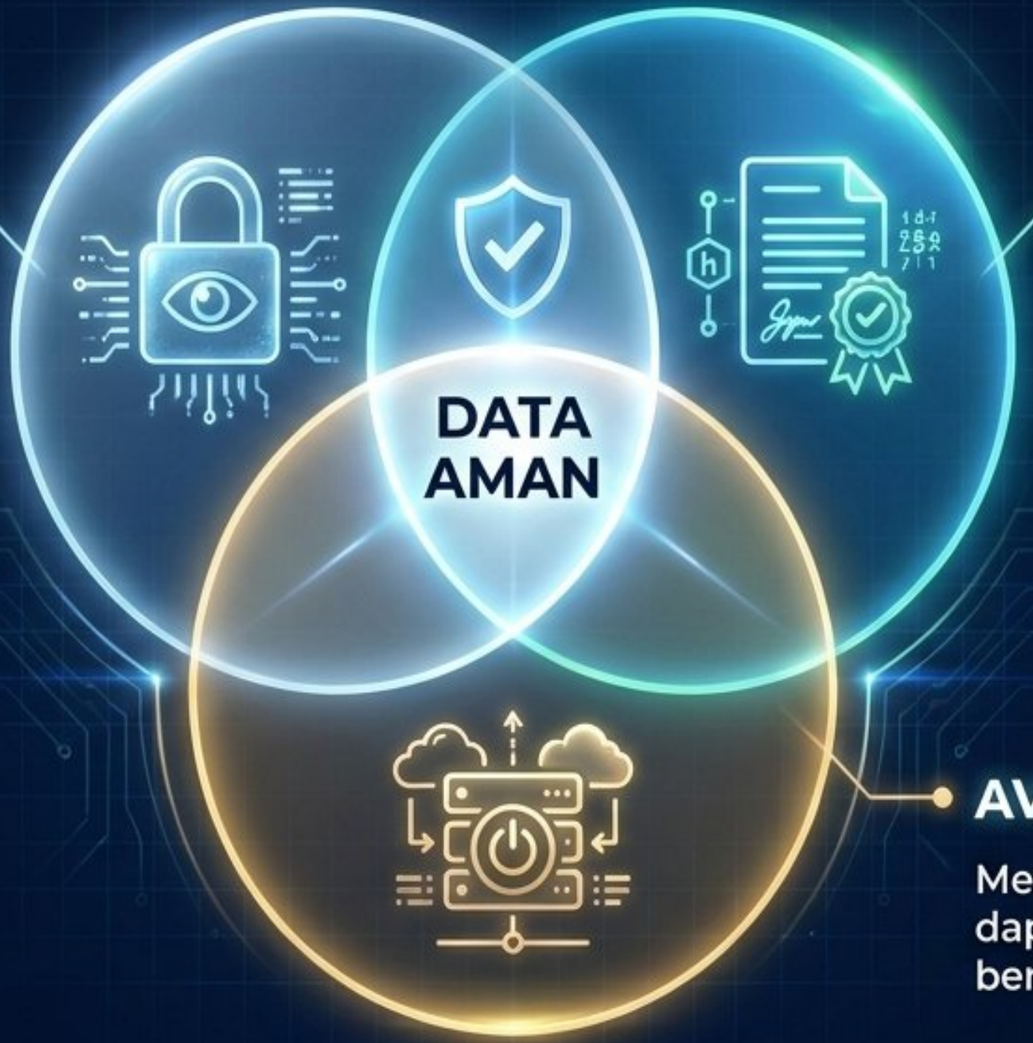


KEAMANAN INFORMASI

PERISAI KEAMANAN INFORMASI: CIA TRIAD

CONFIDENTIALITY

Melindungi data dari akses tidak sah. Hanya untuk pihak berwenang.



INTEGRITY

Menjamin keakuratan data. Mencegah modifikasi tanpa izin.

AVAILABILITY

Memastikan data selalu dapat diakses. Sistem tetap beroperasi.

Pilar 1: Kerahasiaan

Memastikan Hanya Otoritas Resmi yang Mengakses Data

Access Control (RBAC)

Pembatasan hak akses berbasis peran.



MFA

Verifikasi ganda untuk kepastian identitas.

Enkripsi (AES-256)

Mengubah data menjadi kode rahasia.

Tujuan Utama: Mencegah Kebocoran Data.

Prinsip Akses Secukupnya (Least Privilege)

Berikan hak akses minimal yang diperlukan untuk tugas kedinasan, bukan seluas-luasnya.

Peran (*Role*)	Aturan Akses (*Access Rule*)
Pejabat Eselon (eg., Kepala Dinas/Badan)	Akses data strategis penuh HANYA untuk pengambilan keputusan (tupoksi), tidak untuk operasional teknis.
Pegawai Administrasi / Staf TU	Akses terbatas pada data persuratan dan kepegawaian internal, TANPA akses ke data rahasia lintas unit.
Tim Teknis Eksternal / Konsultan IT	Akses khusus terbatas waktu (*timed*) dan dipantau (*audit trail*), HANYA ke sistem spesifik.
Pegawai Purna Tugas / Mutasi	Akses dicabut seketika (*immediate revocation*) saat tanggal serah terima jabatan (pensiun/mutasi).

Protokol Harian Menjaga Kerahasiaan



Standar Password

- Gunakan minimal 8 karakter dengan kombinasi
- Tidak menggunakan password yang sama pada tiap akun.



Pertahanan Akun

- Jangan bagikan password
- Aktifkan MFA pada setiap akun.



Respons Ancaman

- Ganti password secara rutin
- Segera ganti password yang terindikasi bocor.

MATRIKS KEKUATAN PASSWORD: SEBERAPA CEPAT HACKER MEMBOBOL AKUN ANDA?

Jumlah Karakter	Hanya Angka	Huruf Kecil	Kecil & Besar	Angka, Kecil, Besar	Angka, Kecil, Besar, Simbol
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	23 mins	48 mins
7	Instantly	Instantly	7 hours	24 hours	2 days
8	Instantly	1 hour	2 weeks	2 months	5 months
9	Instantly	2 days	2 years	10 years	31 years
10	Instantly	1 month	112 years	651 years	2k years
11	41 mins	3 years	5k years	40k years	153k years
12	7 hours	74 years	303k years	2m years	10m years
13	3 days	1k years	15m years	155m years	751m years
14	4 weeks	50k years	819m years	9bn years	52bn years
15	9 months	1m years	42bn years	596bn years	3tn years
16	8 years	33m years	2tn years	36tn years	257tn years
17	78 years	879m years	115tn years	2qd years	18qd years
18	776 years	22bn years	5qd years	142qd years	1qn years

Terbobol secara instan.

Standar Aman ASN: **12+ Karakter + Simbol + Angka.**

Pilar 2: Keutuhan

Menjamin Data Bebas dari Modifikasi Ilegal



Biometrik: Sidik jari digital data untuk deteksi perubahan.

Menjamin bahwa data **tidak diubah** oleh pihak yang tidak berwenang selama **proses penyimpanan** atau pengiriman.

Nir-Sankal (Non-Repudiation): Bukti mutlak bahwa sebuah tindakan digital benar-benar dilakukan oleh pihak yang bersangkutan melalui Kriptografi Asimetris.

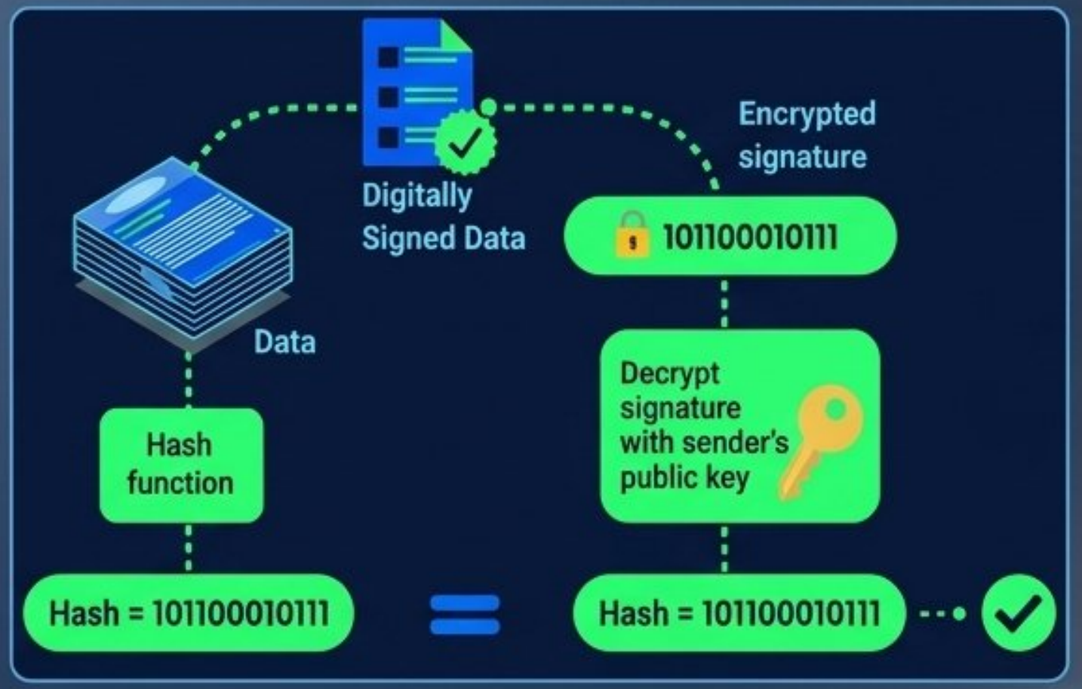
PILAR 2: INTEGRITY & MENJAGA KEASLIAN DATA

ANCAMAN PEMALSUAN



Tanda tangan fisik sangat mudah dipalsukan. Dokumen rentan dimodifikasi.

SOLUSI KRIPTOGRAFI



Solusi TTE (Tanda Tangan Elektronik):
Menggunakan *Asymmetric Cryptography* untuk menjamin *Non-Repudiation* (Nir-Sankal)—pembuat dokumen tidak dapat menyangkal keasliannya.

Protokol Validasi Keaslian Dokumen

1. **Verifikasi Ganda:** Cek validasi TTE dan teliti isi dokumen.
2. **Lapis Keamanan:** Gunakan MFA setiap melakukan TTE dan jangan bagikan Passphrase.
3. **Pantau Masa Aktif:** Perhatikan masa berlaku Sertifikat Elektronik secara berkala.
4. **Tindakan Darurat:** Lakukan Revocation (pencabutan) seketika jika terbukti terkompromi (compromise).

Pilar 3: Ketersediaan

Memastikan Akses Tanpa Hambatan

Menjamin sistem dan data dapat diakses oleh pengguna berwenang kapan saja dibutuhkan tanpa hambatan teknis.

Redundansi Hardware

Mencegah kegagalan tunggal dengan server cadangan.

Disaster Recovery

Pemulihan cepat setelah insiden atau bencana alam.

Mitigasi DDoS

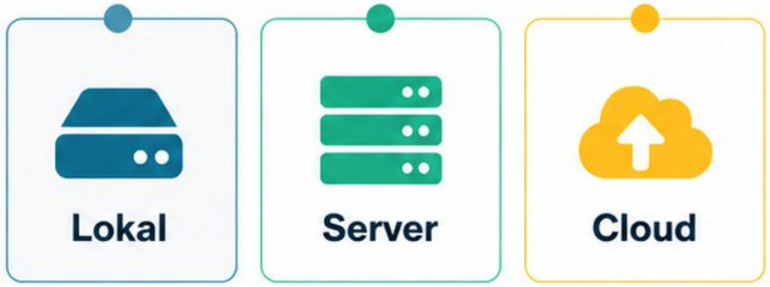
Perlindungan absolut terhadap serangan yang melumpuhkan trafik.

STRATEGI PENCADANGAN (BACKUP)

Pencadangan data adalah proses menyalin data penting organisasi ke lokasi penyimpanan sekunder. Pencadangan data membantu melindungi bisnis dari kehilangan data dengan menyediakan redundansi terhadap lokasi penyimpanan utama apabila lokasi tersebut terganggu atau mengalami kegagalan.

Proses backup dapat dilakukan secara:

- **Otomatis** — dijadwalkan oleh sistem
- **Manual** — dilakukan operator secara langsung





TLP:GREEN

PERTIMBANGAN UTAMA DALAM MELAKUKAN PENCADANGAN

01 Frekuensi Backup

Seberapa sering data harus dicadangkan?

Tentukan berdasarkan tingkat kekritisan data dan seberapa cepat data berubah. Sistem kritis butuh backup lebih sering.



02 Retensi Backup

Berapa lama data cadangan harus disimpan?

Sesuaikan dengan kebijakan organisasi dan regulasi yang berlaku (GDPR, PCI-DSS, dll.).



03 Pemulihan Backup

Bagaimana cara memulihkan data jika terjadi kehilangan?

Uji prosedur pemulihan secara berkala untuk memastikan backup benar-benar bisa dipulihkan.



04 Keamanan Backup

Bagaimana data cadangan dilindungi dari akses tidak sah?

Enkripsi data backup dan batasi akses menggunakan autentikasi yang kuat.



Matriks Diagnostik Keamanan Informasi

	Kerahasiaan	Keutuhan	Ketersediaan
Tujuan Utama	Mencegah Kebocoran Data	Menjaga Keaslian & Nir-Sankal	Memastikan Akses 24/7
Teknologi Kunci	Enkripsi (AES-256), RBAC, MFA	TTE, Kriptografi Asimetris, Biometrik	Redundansi, Disaster Recovery, Anti-DDoS
Kebiasaan Harian	Ubah Password Rutin & Unik	Verifikasi Dokumen & Jaga Passphrase	Backup 3-2-1-0 & Monitoring Aktif



PEOPLE
PROCESS
TECHNOLOGY

Titik Temu Kesempurnaan Keamanan



Keamanan siber bukan soal memiliki teknologi tercanggih, melainkan tentang membangun arsitektur di mana Manusia, Proses, dan Teknologi bekerja dalam satu kesatuan. Hanya ketika ketiganya terintegrasi, tujuan sejati dari Confidentiality, Integrity, dan Availability dapat tercapai.

Arsitektur Pertahanan: Memetakan Peran Ekosistem

Matriks Pemetaan Ekosistem Siber			
	Fungsi Utama	**Fokus Eksekusi**	**Ancaman yang Ditangkal**
PEOPLE (Manusia)	Garis pertahanan pertama	Security awareness, Kompetensi	Phishing, Social Engineering
PROCESS (Proses)	Aturan dan tata kelola	Kebijakan, SOP, Backup	Downtime operasional, Kepanikan insiden
TECHNOLOGY (Teknologi)	Kontrol teknis perlindungan	MFA, Encryption, SIEM	System breach, Malware, Akses ilegal



INSIDEN SIBER

INSIDEN SIBER



"**Suatu pelanggaran atau ancaman** terhadap kebijakan keamanan komputer organisasi, standar keamanan, atau praktik keamanan yang dapat membahayakan integritas, kerahasiaan, atau ketersediaan aset informasi"

Sumber : NIST Special Publication 800-61 Revision 2

INSIDEN SIBER



"**INSIDEN SIBER** adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik"

PERATURAN BSSN 1 / 2024 TENTANG PENGELOLAAN INSIDEN SIBER

Insiden Siber dapat terjadi kapan saja dan dimana saja



STUDI KASUS: Bencana Berawal dari Kelalaian

Mari kita kaitkan teori CIA Triad dengan realita lapangan di Pemerintahan Daerah.

Konteks: Bagaimana satu kelalaian kecil dan pelanggaran protokol dasar dapat melumpuhkan sistem operasional satu instansi.

FASE 1: KESALAHAN MENDASAR & EKSPOSUR

Character Profile Card



Character Profile Card

Nama: Pegawai A

Peran: Staf Administrasi Pemda

THE SETUP

Pegawai A menggunakan password "Bimtek2026" (Tanpa simbol/Lemah) untuk akun pemerintahan DAN akun forum hobi pribadinya. Ia **TIDAK** mengaktifkan MFA.



THE BREACH

Forum hobi diretas. Kredensial masuk ke Darknet Exposure. Hacker mengekstrak password dan menggunakannya untuk masuk ke portal internal Pemda dengan mudah.

(Pelanggaran Confidentiality)

FASE 2: ESKALASI & RESPONS FATAL

THE ESCALATION



Hacker yang telah masuk mencoba memodifikasi nominal dalam dokumen anggaran negara secara ilegal tanpa TTE.

(Ancaman Integrity)

THE FATAL MISTAKE



Pegawai A menyadari ada aktivitas login mencurigakan. Panik dan takut ditegur pimpinan, ia mencoba memperbaiki sistem sendiri dan secara sengaja MENGHAPUS LOG riwayat akses.

PEMBELAJARAN KASUS: APA YANG SEHARUSNYA DILAKUKAN?

✗ Tindakan Pegawai A (SALAH)

- Menggunakan password berulang.
- Tidak memakai MFA.
- Memperbaiki sistem sendiri saat diretas.
- Menghapus log dan jejak digital.

✓ Protokol ASN (BENAR)

- Password unik 12+ karakter + simbol.
- Wajib menggunakan perlindungan MFA.
- Jangan sentuh sistem yang sedang diretas.
- Biarkan jejak forensik utuh & SEGERA LAPOR CSIRT.

PERAN ANDA SAAT TERJADI INSIDEN SIBER



DETEKSI

Kenali **gejala anomali** (website error, data hilang tiba-tiba, peringatan login mencurigakan).

LAPOR

Gunakan **kanal resmi pelaporan** untuk menghubungi Tim Tanggap Insiden Siber (TTIS).

AMANKAN BUKTI

JANGAN HAPUS LOG. Sediakan akses penuh bagi TTIS untuk melakukan analisis forensik. **Jangan pernah mencoba memperbaiki sendiri tanpa koordinasi.**

Peringatan Dini: Apa yang Wajib Segera Dilaporkan oleh Pegawai Instansi?

Jangan ragu atau takut. Pelaporan dini memangkas dampak kerugian operasional dan keamanan data negara secara drastis.

- Pegawai menerima email dinas palsu (*phishing*) yang meminta data sensitif.



- Salah mengirimkan dokumen negara atau data kepegawaian ke pihak luar.



- Menemukan basis data layanan publik tiba-tiba tidak dapat diakses.



LAPORKAN!

- Kehilangan perangkat kerja dinas (laptop/ponsel) yang berisi data dinas.



- Password atau OTP akses sistem pemerintah bocor tanpa sengaja.



- Mendapat notifikasi login asing dari lokasi tidak dikenal atau mencurigakan.





PERAN TTIS

Cyber Security Incident Response Team (CSIRT)

Sekelompok orang yang bertanggung jawab melakukan pengelolaan penanganan Insiden Siber pada lingkup organisasi atau institusi.

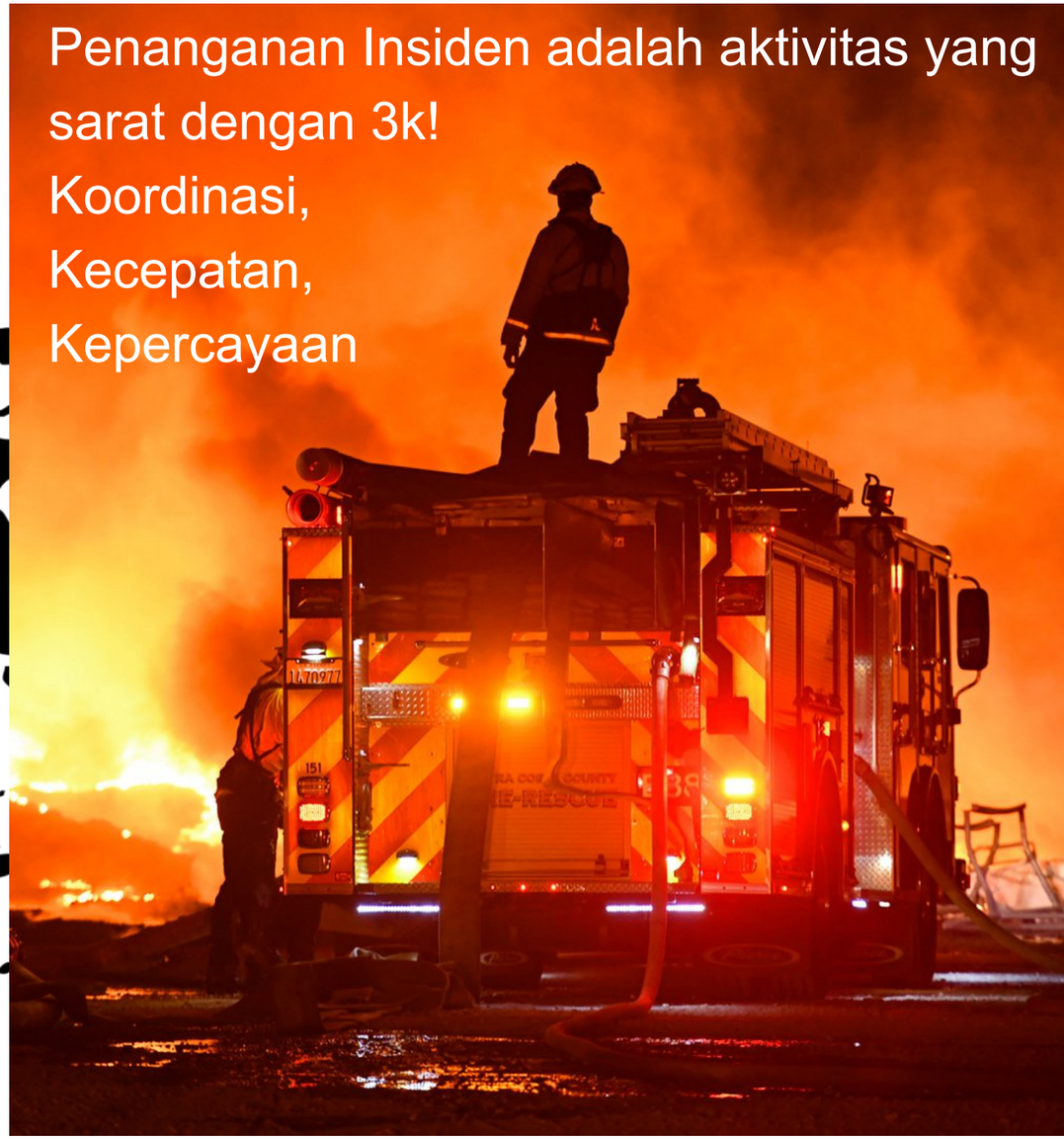


Penanganan Insiden adalah aktivitas yang sarat dengan 3k!

Koordinasi,

Kecepatan,

Kepercayaan





PERATURAN BSSN NOMOR 1 TAHUN 2024

Fungsi Tim Tanggap Insiden Siber (TTIS / CSIRT)

FUNGSI MINIMAL

- Pemberian peringatan terkait Keamanan Siber
- Perumusan panduan teknis penanganan Insiden Siber
- Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
- Pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;
- Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan

FUNGSI LAINNYA

- Penanganan kerentanan Sistem Elektronik
- Penanganan artefak digital
- Pemberitahuan hasil pengamatan potensi ancaman
- Pendeteksian serangan
- Analisis risiko Keamanan Siber
- Konsultasi terkait kesiapan penanganan Insiden Siber
- Pembangunan kesadaran dan kepedulian terhadap Keamanan Siber



Peran TTIS

[redacted]

Menjadi Pusat Koordinasi Insiden

- Menerima laporan insiden dari OPD
- Menentukan tingkat keparahan & prioritas

[redacted]

Melakukan Analisis Teknis

- Investigasi penyebab insiden
- Mengidentifikasi dampak & potensi penyebaran

[redacted]

Mengendalikan & Memulihkan Sistem

- Membantu containment (mencegah meluas)
- Mendukung eradikasi malware & recovery layanan

[redacted]

Memberikan Rekomendasi Pencegahan

- Menyusun lesson learned setelah insiden
- Memberi advis keamanan ke OPD (patch, awareness, SOP)

[redacted]

Menjadi Jembatan ke BSSN/CSIRT Lain

- Eskalasi insiden besar ke level nasional
- Berkolaborasi lintas sektor jika perlu

Peran OPD



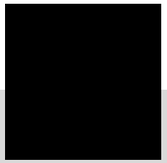
Menjadi Mata & Telinga Awal

- OPD adalah pihak pertama yang tahu ada gangguan di aplikasi/sistemnya.
- Peran: mendeteksi gejala insiden (website error, data hilang, login mencurigakan).



Melaporkan Segera ke TTIS

- Jangan diam atau mencoba perbaiki sendiri tanpa koordinasi.
- Gunakan kanal resmi pelaporan TTIS.



Menjaga Bukti Insiden

- Jangan hapus log atau jejak insiden.
- Biarkan TTI melakukan analisis forensik.



Mendukung Respons & Pemulihan

- Menyediakan akses/sumber daya yang diperlukan TTIS.
- Bekerjasama dalam mengembalikan layanan.



Membangun Budaya Aman di OPD

- Edukasi pegawai soal phishing, password kuat, dan pelaporan insiden.
- Menjadi garda depan pencegahan.

Alur Kerja TTIS dan OPD

1 Deteksi di OPD

OPD menemukan indikasi insiden (website error, login janggal, data hilang, email phishing, alert aneh).

2 Pelaporan Cepat ke TTIS

OPD melaporkan lewat kanal resmi (email, hotline, form pelaporan, dsb).

3 Tindakan Awal OPD

- Jaga bukti (jangan hapus log/file).
- Isolasi perangkat terdampak bila memungkinkan.

4 Tindak Lanjut oleh TTIS

- TTIS menerima laporan → analisis → menentukan level eskalasi.
- Jika insiden besar, bisa diteruskan ke BSSN atau TTIS sektoral terkait.

5 Komunikasi Balik ke OPD

- TTIS memberikan update status & rekomendasi.
- OPD mendukung pemulihan layanan.

Matriks Konsep: Respon vs. Penanganan

Respons Insiden (Incident Response)	Penanganan Insiden (Incident Handling)
Fokus: Taktis & Reaktif.	**Fokus:** Strategis & Holistik.
Definisi: Proses menanggapi insiden untuk meminimalkan dampak langsung.	**Definisi:** Proses menyeluruh dari awal hingga akhir siklus.
Tujuan Utama: Melindungi aset organisasi dan memulihkan operasi secepat mungkin (memadamkan api). 	**Tujuan Utama:** Mengidentifikasi, mengendalikan, menyelidiki, melaporkan, merespons, hingga mempelajari insiden untuk mencegah kejadian serupa di masa depan. 

Gemini Notebook

RESPON VS PENANGANAN INSIDEN



PENANGANAN INSIDEN

- Memulihkan data yang hilang akibat ransomware

RESPONS INSIDEN

- Mengisolasi sistem yang terinfeksi malware

RESPONS INSIDEN

- Mengubah password akun yang disusupi

PENANGANAN INSIDEN

- Mengidentifikasi dan menambal kerentanan yang dieksploitasi dalam serangan siber

PENANGANAN INSIDEN

- Melatih karyawan tentang kesadaran dan respon insiden

PENANGANAN INSIDEN

- Memblokir alamat IP yang berbahaya

RESPONS INSIDEN

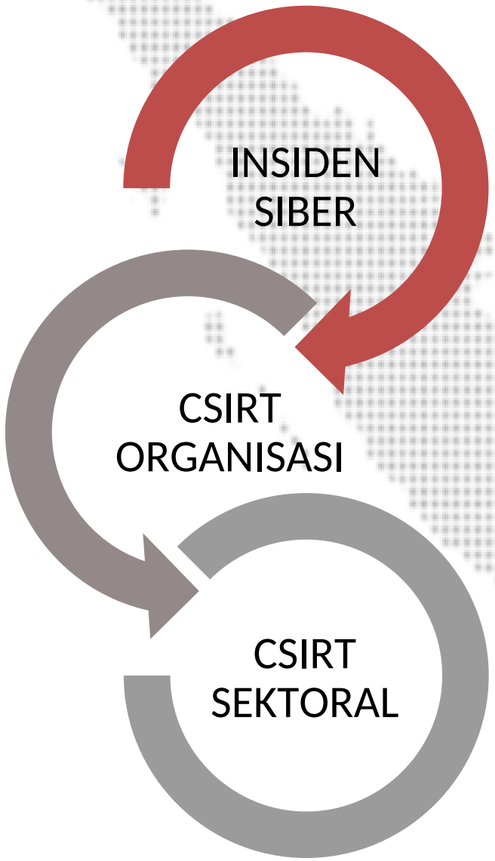




ESKALASI

PENANGANAN

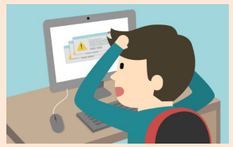
PELAPORAN DAN PENANGANAN INSIDEN SIBER



1 Terjadi Insiden Siber

Insiden Siber dapat berupa kejadian berikut:

- *Web Defacement*
- *SQL Injection*
- *Malware*
- *Ransomware*
- *DDoS*
- *Ilegal Access*



2 Melapor kepada CSIRT Organisasi (Internal)

Melaporkan insiden siber yang terjadi kepada CSIRT Organisasi melalui kontak resmi CSIRT Organisasi, misalnya melalui:

- *Telepon*
- *Email*
- *Chat Messenger*
- *dsb*



3 Penanganan Insiden oleh CSIRT Organisasi

- *POC memverifikasi apakah hal tsb insiden atau hanya kesalahan konfigurasi*
- *Jika merupakan insiden siber, maka tim CSIRT Organisasi akan melakukan penanganan insiden siber sesuai SOP yang berlaku*



4 CSIRT Organisasi meminta bantuan CSIRT Sektoral

Jika insiden tidak dapat tertangani, tim CSIRT Organisasi dapat meminta bantuan CSIRT Sektoral, dengan cara sbb:

- *Melakukan pengumpulan bukti insiden, misal: foto, screenshot, dan log insiden*
- *Menghubungi CSIRT Sektoral melalui kontrak resmi CSIRT Sektoral. Misal: BSSN*



5 Penanganan Insiden bersama CSIRT Sektoral

- *CSIRT Sektoral bersama CSIRT Organisasi berkolaborasi dalam penanganan insiden siber.*
- *Kontak resmi CSIRT Sektoral BSSN*

[redacted] **Telegram id: @GovCSIRT_ID**

WhatsApp: +62 85 123 123 940

[redacted] **Mail to: govcsirt@bssn[.]go[.]id**

[redacted] **Website: https[:]//bssn[.]go[.]id/gov-csirt/**

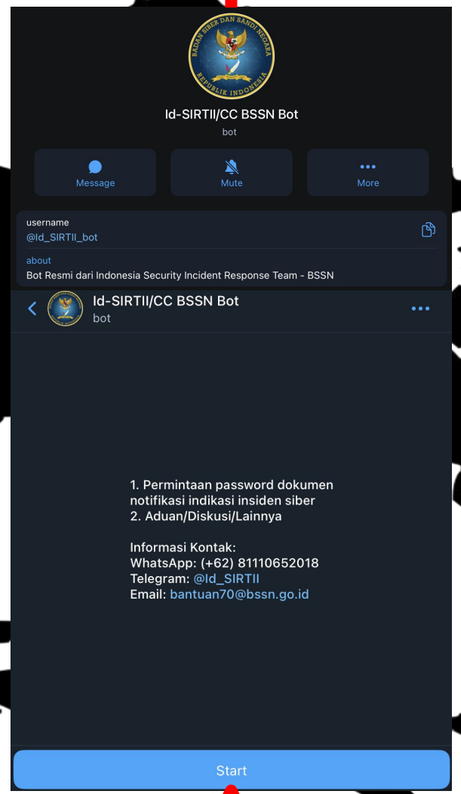
PENGELOLAAN NOTIFIKASI INSIDEN SIBER

1

PEMDA MENERIMA NOTIFIKASI INDIKASI INSIDEN DARI EMAIL bantuan70@bssn[.]go[.]id

2

PEMDA MEMINTA PASSWORD VIA BOT UNTUK MEMBUKA DOKUMEN bantuan70@bssn[.]go[.]id



3

PEMDA MELAKUKAN VALIDASI INDIKASI INSIDEN

4

PEMDA MENGIRIMKAN FORM VALIDASI INDIKASI INSIDEN KE EMAIL bantuan70@bssn[.]go[.]id

5

VALID

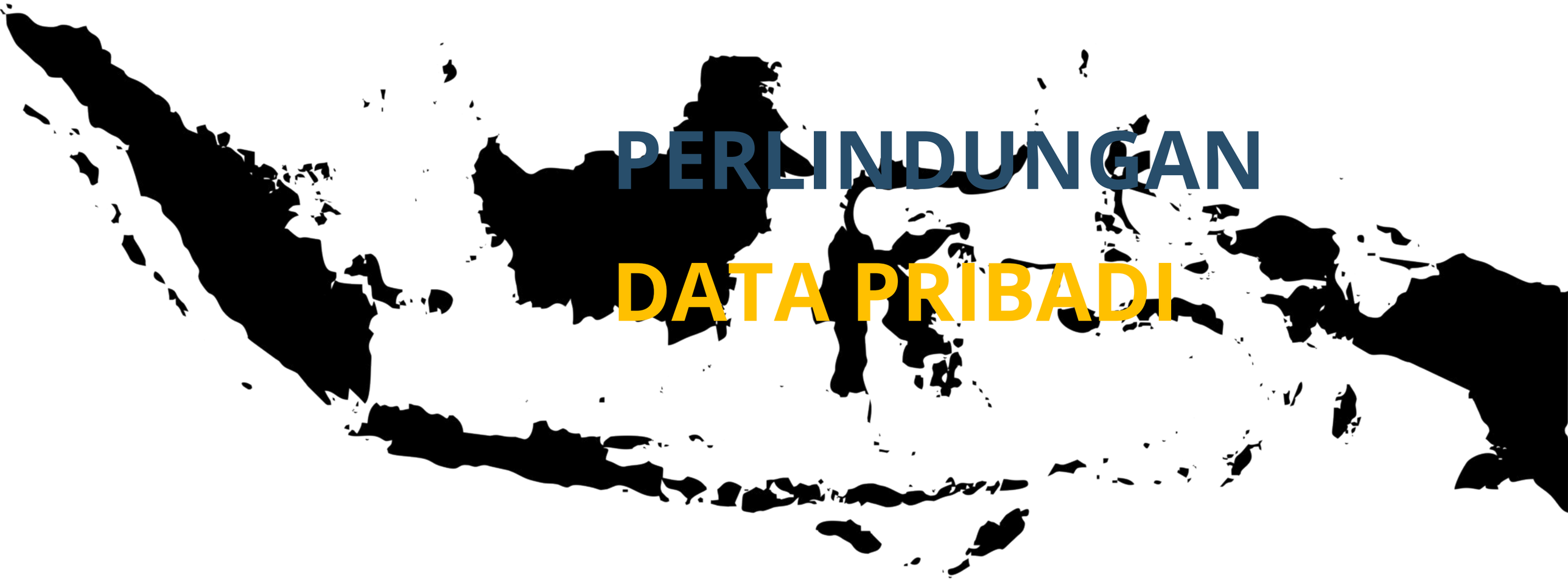
Pemda melakukan tahapan mitigasi dan perbaikan sistem secara mandiri. Jika insiden belum dapat ditangani mandiri, lakukan permohonan asistensi kepada Gov-CSIRT.

TIDAK VALID

Pemda tetap mengirimkan form validasi dan sampaikan hasil validasinya. Tetap waspada dan memeriksa sistem lain.

6

Lesson Learned untuk OPD Lain atau Pemda Lain Jika Insiden Benar Terjadi



PERLINDUNGAN

DATA PRIBADI

Anatomi Data Pribadi Menurut UU PDP



Berlaku untuk pemrosesan melalui sistem elektronik maupun nonelektronik (Pasal 1).

Klasifikasi Data & Beban Kepatuhan (Pasal 4)

Data Bersifat Umum

- Contoh: Nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, data kombinasi pengidentifikasi (seperti IP Address/No. HP).

Risk Score: Menengah (Standard Compliance)

Data Bersifat Spesifik

- Contoh: Data & informasi kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi.

Risk Score: Tinggi (Elevated Compliance Weight)

PROTOKOL DARURAT:
KEGAGALAN PELINDUNGAN DATA LEMBAGA

Apa yang harus dilakukan Badan/Dinas/Lembaga ketika Data Penduduk/Pegawai bocor?

“Kegagalan melindungi kerahasiaan, integritas, dan ketersediaan Data Pribadi, baik disengaja maupun tidak.”

Batas Waktu Kritis 3x24 Jam (Pasal 46)

T = 0 Jam

Insiden Kebocoran /
Kegagalan Data Instansi Ditemukan

T < 72 Jam

Batas Akhir: Wajib menyampaikan pemberitahuan tertulis

Siapa yang Wajib Diberitahu oleh Instansi?

1. **Subjek** Data Pribadi (Warga/Pengguna Layanan).
2. **Lembaga** (Otoritas PDP).
3. **Masyarakat** (Publik) — Khusus jika mengganggu pelayanan publik atau berdampak serius.

3 Elemen Wajib Pemberitahuan Insiden Bagi Instansi Pemerintah

Unit Keamanan Informasi Pemerintah

1. Identifikasi Data

Data Pribadi Warga apa saja yang terungkap? (Contoh: NIK, Nama, Alamat, Nomor HP).

→

2. Kronologi Insiden

Kapan dan bagaimana Data Pribadi tersebut bisa terungkap ke publik?

→

3. Tindakan Mitigasi

Upaya penanganan dan pemulihan apa yang sedang/telah dilakukan oleh Instansi Pemerintah?

Pemberitahuan ini merupakan kewajiban hukum mutlak seluruh Instansi Pemerintah.

Sesuai regulasi PDP terbaru dan protokol keamanan siber pemerintah.

SIMPDP
Sistem Informasi
Pengawasan Pelindungan Data Pribadi
Kementerian Komdigi

Kewajiban Pelaporan Kegagalan Pelindungan Data Pribadi (PDP)

Khusus Penyelenggara Sistem Elektronik (PSE)

pengawasanpdp.id

Portal resmi Sistem Informasi Pengawasan Pelindungan Data Pribadi (SIMPDP) Kementerian Komdigi menyediakan saluran wajib bagi PSE untuk melaporkan insiden dugaan kebocoran data.

Langkah 1: Akses Portal

Buka situs **pengawasanpdp.id** dan pilih menu **Lapor Gagal PDP**.

Langkah 2: Isi Formulir

Lengkapi Formulir Laporan Dugaan Kebocoran Data Pribadi. Pastikan detail informasi mencerminkan keadaan sebenarnya secara akurat.

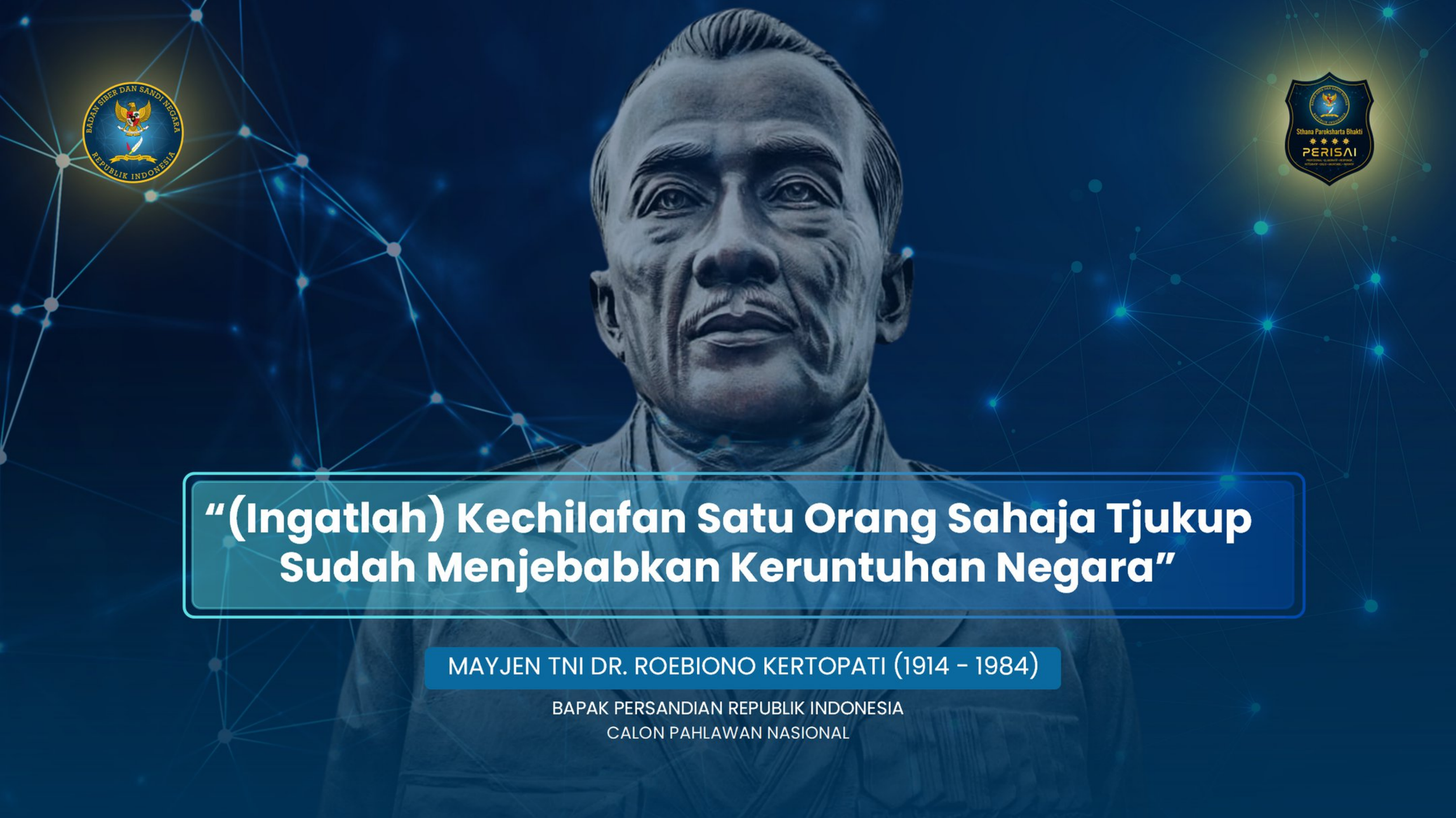
Langkah 3: Unduh Berkas

Simpan (unduh) formulir pelaporan yang telah diisi secara lengkap dari sistem.

Langkah 4: Kirim via Email

Kirimkan formulir yang telah diunduh tersebut ke email resmi pengawasan: **pengendalianaptika@kominfo.go.id**

Disclaimer: *Pastikan laporan diisi oleh pihak yang berwenang dari PSE dengan data faktual terkait insiden.*


BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Sthana Paroksharta Bhakti
PERISAI
“(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”
MAYJEN TNI DR. ROEBIONO KERTOPATI (1914 - 1984)
BAPAK PERSANDIAN REPUBLIK INDONESIA
CALON PAHLAWAN NASIONAL