 # Jaga Ruang Siber

STANDAR OPERASIONAL PROSEDUR
KEMANAN INFORMASI
(SOP KARI)

Nomor Dokumen	: SOP-KOMINFOPERSTATIK/001/2025
Versi	: 1.0
Tanggal Berlaku	: 20 Mei 2025
Disusun Oleh	: Zaenal Fanumbi, ST., M.Kom
Jabatan	: Bidang Persandian Dan Statistik
Disetujui Oleh	: Kepala Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Papua Barat

PEMERINTAH PROVINSI PAPUA BARAT
DINAS KOMUNIKASI INFORMATIKA PERSANDIAN DAN STATISTIK
Alamat : Kompleks Perkantoran Gubernur Papua Barat Arfai 2 Manokwari
Email : [Alamat Email]
Website : [Alamat Website]

LEMBAR PENGESAHAN
PEDOMAN TATA KELOLA KEAMANAN INFORMASI (PT KASI)

Disusun Oleh : Zaenal Fanumbi, ST, M.Kom & Team Penyusunan Pedoman Tata Kelola Keamanan Informasi (PT KARI)
Dinas Kominfo Persandian dan Statistik Provinsi Papua Barat.

Diperiksa Oleh : Nama : ZAENAL FANUMBI, ST,., M.Kom
NIP : 19810621 200909 1 001
Jabatan : Kepala Bidan Persandian dan Statistik
Tanda Tangan :

Disetujui oleh : Nama : FRANS P. ISTIA, S.Sos.,MM
NIP : 19690310 199103 1 017
Jabatan : Kepala Dinas Komuinkasi Informasika Persandian dan Statistik Provinsi Papua Barat

Tanda Tangan :

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga **Standar Operasional Prosedur (SOP) Keamanan Informasi** di lingkungan **Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat** dapat disusun dan diselesaikan dengan baik.

Perkembangan teknologi informasi yang semakin pesat telah membawa dampak signifikan terhadap pengelolaan data dan informasi pemerintahan. Dalam rangka menjaga kerahasiaan, keutuhan, dan ketersediaan informasi di lingkungan pemerintahan, diperlukan adanya pedoman yang jelas dan terstandarisasi mengenai pengelolaan keamanan informasi.

SOP Keamanan Informasi ini disusun sebagai acuan bagi seluruh pegawai dan pihak terkait di lingkungan Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat dalam melakukan pengelolaan informasi yang aman dan sesuai dengan ketentuan yang berlaku. Dokumen ini juga bertujuan untuk meningkatkan kesadaran dan tanggung jawab bersama dalam menjaga informasi pemerintahan dari berbagai ancaman, baik yang bersifat internal maupun eksternal.

Kami menyadari bahwa dalam penyusunan SOP ini masih terdapat kekurangan. Oleh karena itu, saran dan masukan yang bersifat membangun sangat kami harapkan demi penyempurnaan dan peningkatan kualitas SOP ini di masa yang akan datang.

Akhir kata, kami mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan SOP ini. Semoga SOP Keamanan Informasi ini dapat menjadi pedoman yang bermanfaat bagi kita semua dalam upaya mewujudkan tata kelola pemerintahan yang bersih, efektif, dan aman di Provinsi Papua Barat.

Manokwari, 31 Juni 2025

Kepala Dinas Komunikasi, Informatika, Persandian,dan Statistik
Provinsi Papua Barat

FRANS P. ISTIA, S.Sos, MM
Pembina Utama Madya/IVd
NIP. 19690310 199103 1 017

DAFTAR ISI

DAFTAR ISTILAH DAN SINGKATAN

ISTILAH/SINGKATAN	KETERANGAN
Keamanan Informasi	Perlindungan terhadap informasi dari berbagai ancaman guna menjamin kerahasiaan, keutuhan, dan ketersediaan informasi.
Informasi	Data atau kumpulan data yang memiliki arti, nilai, atau manfaat bagi organisasi.
Username	Identitas unik yang diberikan kepada pengguna untuk mengakses sistem informasi
Password	Kata sandi rahasia yang digunakan untuk mengautentikasi pengguna agar dapat mengakses sistem.
Aset Informasi	Segala bentuk informasi yang memiliki nilai bagi organisasi, termasuk sistem, aplikasi, data, perangkat keras, perangkat lunak, dan sumber daya manusia.
Insiden Keamanan Informasi	Kejadian yang tidak diinginkan atau tidak terduga yang mengganggu keamanan informasi, termasuk kebocoran data, akses tidak sah, atau serangan siber.
SOP	Standar Operasional Prosedur, pedoman baku dalam pelaksanaan tugas tertentu.
Data Sensitif	Informasi yang bersifat rahasia, strategis, atau penting yang jika disalahgunakan dapat merugikan pemerintah daerah maupun masyarakat.
Pemilik Informasi	Pihak atau unit kerja yang bertanggung jawab atas pengelolaan dan perlindungan informasi.
Pengguna Informasi	Pegawai atau pihak yang berhak mengakses dan menggunakan informasi sesuai otorisasi.
Router	Perangkat jaringan yang berfungsi untuk mentransmisikan paket data dari jaringan internet ke perangkat lain melalui proses routing
Switch	Komponen jaringan yang berfungsi untuk menghubungkan beberapa perangkat komputer dalam sebuah jaringan
Server	Pusat pengelola data dan layanan yang diakses oleh perangkat client seperti komputer, smartphone, atau perangkat lainnya.
Backup	Proses menyalin data/informasi untuk tujuan pemulihan jika terjadi kerusakan atau kehilangan data.
Disaster Recovery	Prosedur pemulihan layanan dan data penting pasca insiden atau bencana.
Firewall	Sistem pengamanan jaringan yang mengatur lalu lintas data keluar masuk jaringan.
Audit Keamanan Informasi	Proses pemeriksaan sistematis terhadap pengelolaan keamanan informasi untuk memastikan kepatuhan dan efektivitas.
Log	Catatan digital yang merekam berbagai aktivitas, peristiwa, atau transaksi yang terjadi dalam suatu sistem, aplikasi, jaringan atau perangkat.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini telah memberikan berbagai kemudahan dalam pengelolaan data dan pelayanan publik. Namun, di sisi lain, perkembangan tersebut juga meningkatkan risiko ancaman terhadap keamanan informasi, baik yang bersifat teknis maupun non-teknis.

Sebagai instansi pemerintah yang bertugas mengelola data, informasi, serta layanan komunikasi dan persandian, **Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Papua Barat** memiliki tanggung jawab untuk memastikan keamanan informasi agar terhindar dari ancaman kerusakan, kehilangan, penyalahgunaan, maupun kebocoran informasi yang dapat merugikan instansi maupun masyarakat.

Oleh karena itu, diperlukan sebuah pedoman dalam bentuk **Standar Operasional Prosedur (SOP) Keamanan Informasi** guna menjamin kerahasiaan, keutuhan dan ketersediaan informasi di lingkungan dinas.

1.2 Maksud dan Tujuan

a. Maksud

Penyusunan SOP Keamanan Informasi ini dimaksudkan sebagai pedoman resmi bagi seluruh pegawai dan pihak terkait dalam pengelolaan informasi agar berjalan secara aman, efektif, dan sesuai dengan standar serta peraturan yang berlaku.

b. Tujuan

1. Memberikan panduan standar dalam pengamanan informasi di lingkungan Dinas Kominfo Papua Barat.
2. Menjamin kerahasiaan, keutuhan, dan ketersediaan informasi dari berbagai ancaman.
3. Meningkatkan kesadaran, kewaspadaan, dan tanggung jawab pegawai dalam menjaga keamanan informasi.
4. Mencegah terjadinya kebocoran, penyalahgunaan, atau kehilangan informasi penting.
5. Mendukung kelancaran penyelenggaraan pemerintahan berbasis elektronik dan pelayanan publik.

1.3 Ruang Lingkup

SOP ini berlaku untuk :

1. Seluruh pegawai dan pihak ketiga yang terkait dalam pengelolaan, penggunaan, dan penyimpanan informasi di lingkungan Dinas Kominfo Papua Barat.
2. Seluruh data, dokumen, sistem informasi, perangkat keras, perangkat lunak, dan jaringan yang digunakan dalam aktivitas kedinasan.
3. Prosedur pengamanan informasi secara fisik maupun digital.

1.4 Dasar Hukum

SOP Keamanan Informasi ini disusun berdasarkan ketentuan peraturan perundang-undangan yang berlaku, di antaranya :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
4. Peraturan Presiden Nomor 82 Nomor 2023 tentang Percepatan Transformasi Digital dan Sistem Pemerintahan Berbasis Elektronik (SPBE).
5. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional.
6. Peraturan Menteri PAN-RB RI Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE Nasional.
7. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016, tentang Sistem Manajemen Pengamanan Informasi.
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik, Standar Teknis dan Prosedur Keamanan Pemerintahan Berbasis Elektronik.
9. Peraturan Gubernur Provinsi Papua Barat Nomor 33 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah.
10. Peraturan Gubernur Provinsi Papua Barat Nomor 18 Tahun 2018 tentang uraian tugas dan fungsi Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat.

BAB II
KEBIJAKAN UMUM KEAMANAN INFORMASI

2.1 Tujuan Kebijakan

Kebijakan Umum Keamanan Informasi ini bertujuan untuk memberikan landasan dan arah yang jelas dalam upaya perlindungan terhadap informasi yang dikelola oleh **Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat**, guna menjamin kerahasiaan, keutuhan, dan ketersediaan informasi serta mendukung tata kelola pemerintahan yang baik berbasis teknologi informasi.

2.2 Prinsip-Prinsip Keamanan Informasi

Dalam penyelenggaraan pengelolaan informasi, prinsip-prinsip berikut wajib diterapkan:

1. **Kerahasiaan (Confidentiality)** : Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
2. **Keutuhan (Integrity) :** Menjamin bahwa informasi tetap lengkap, benar, dan tidak mengalami perubahan tanpa otorisasi.
3. **Ketersediaan (Availability) :** Menjamin bahwa informasi tersedia dan dapat diakses sesuai kebutuhan oleh pihak yang berwenang.

2.3 Ruang Lingkup Kebijakan

Kebijakan ini berlaku bagi :

a. Seluruh pegawai di lingkungan Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Papua Barat.
b. Pihak ketiga yang memiliki hubungan kerja sama atau kontrak kerja dengan dinas terkait pengelolaan, penyimpanan dan akses informasi.
c. Seluruh sistem informasi, infrastruktur jaringan, perangkat keras, perangkat lunak, media penyimpanan dan dokumen baik cetak maupun elektronik yang digunakan dalam aktivitas kedinasan.

2.4 Strategi Penerapan Keamanan Informasi

Untuk menerapkan kebijakan keamanan informasi secara efektif, langkah-langkah strategis berikut dilakukan :

1. **Penetapan Standar dan Prosedur**

   Menyusun dan menerapkan standar serta prosedur keamanan informasi yang selaras dengan peraturan perundang-undangan.

2. **Peningkatan Kesadaran dan Pelatihan**

   Melakukan sosialisasi dan pelatihan rutin kepada pegawai mengenai pentingnya keamanan informasi dan tindakan pengamanannya.
3. **Pengendalian Akses Informasi**

   Mengatur hak akses informasi berdasarkan peran, fungsi, dan tingkat otorisasi pengguna.
4. **Penanganan Insiden Keamanan Informasi**

   Menyusun mekanisme pelaporan, penanganan, dan dokumentasi terhadap insiden keamanan informasi yang terjadi.
5. **Pemantauan dan Evaluasi Berkala**

   Melakukan pemantauan terhadap keamanan informasi serta evaluasi berkala untuk memastikan efektivitas penerapan kebijakan.

2.5 Tanggung Jawab Pengelolaan Keamanan Informasi

Seluruh pihak yang terlibat wajib mematuhi kebijakan ini dengan pembagian tanggung jawab sebagai berikut :

1. **Pimpinan Dinas**

   Bertanggung jawab atas penerapan dan pengawasan kebijakan keamanan informasi di lingkungan dinas.
2. **Unit Kerja Terkait**

   Melaksanakan pengamanan informasi sesuai SOP dan petunjuk teknis.
3. **Pegawai**

   Menjaga kerahasiaan, keutuhan dan ketersediaan informasi sesuai perannya masing-masing.
4. **Pihak Ketiga**

   Mematuhi ketentuan keamanan informasi sebagaimana tertuang dalam perjanjian kerja sama atau kontrak kerja.

BAB III
ORGANISASI PENGELOLAAN KEAMANAN INFORMASI

3.1 Struktur Organisasi Keamanan Informasi

Untuk memastikan penerapan keamanan informasi berjalan efektif dan terkoordinasi, **Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Papua Barat** membentuk **Tim Pengelola Keamanan Informasi** dengan susunan sebagai berikut :

a. **Penanggung Jawab:** Kepala Dinas
b. **Ketua:** Sekretaris Dinas
c. **Koordinator Teknis:** Kepala Bidang Persandian dan Statistik
d. **Anggota:**
    - Kepala Bidang Infrastruktu TIK
    - Kepala seksi Bidang Persandian dan Statistik
    - Kepala Seksi Bidang Infrastruktur TIK
    - Petugas Pengelola Data dan Informasi
    - Pegawai yang ditunjuk sesuai kebutuhan

Susunan ini dapat disesuaikan berdasarkan kebutuhan organisasi dan perkembangan teknologi informasi.

3.2 Tugas dan Tanggung Jawab

a. Kepala Dinas

- Menetapkan kebijakan keamanan informasi.
- Memberikan persetujuan terhadap SOP, standar dan prosedur keamanan informasi.
- Mengawasi pelaksanaan keamanan informasi secara menyeluruh.

b. Sekretaris Dinas

- Mengkoordinasikan kegiatan pengelolaan keamanan informasi antar bidang.
- Melaporkan pelaksanaan dan insiden keamanan informasi kepada Kepala Dinas.

c. Kepala Bidang Persandian dan Statistik

- Menyusun pedoman teknis dan SOP pengelolaan keamanan informasi.
- Melaksanakan evaluasi dan pemantauan keamanan informasi.
- Mengkoordinasikan tindak lanjut insiden keamanan informasi.

d. Kepala Seksi Bidang Persandian dan Statistik

- Melaksanakan pengamanan teknis sistem persandian dan komunikasi.
- Menangani pelaporan insiden keamanan informasi.
- Menjamin keamanan informasi statistik strategis yang dikelola dinas.

e. Kepala Bidang Infrastruktur TIK

- Menjamin keamanan perangkat keras, perangkat lunak, jaringan, dan sistem informasi.
- Melaksanakan evaluasi dan pemantauan perangkat keras, perangkat lunak, jaringan, dan sistem informasi.
- Mengkoordinasikan tindak lanjut insiden perangkat keras, perangkat lunak, jaringan, dan sistem informasi.

f. Kepala Seksi Infrastruktur TIK

- Melaksanakan pengamanan perangkat keras, perangkat lunak, jaringan, dan sistem informasi.

g. Petugas Pengelola Data dan Informasi

- Mengelola informasi sesuai klasifikasi dan ketentuan keamanan informasi.
- Melaporkan potensi ancaman atau insiden.

h. Pihak Ketiga/Pegawai yang Ditunjuk

- Mematuhi seluruh kebijakan dan prosedur keamanan informasi yang berlaku.

3.3 Mekanisme Kerja Organisasi Keamanan Informasi

1. **Rapat Koordinasi Keamanan Informasi**

   Dilaksanakan minimal sekali dalam 3 bulan atau sewaktu-waktu jika diperlukan untuk membahas isu keamanan informasi dan evaluasi pelaksanaannya.

2. **Pelaporan Insiden**

   Seluruh pegawai wajib melaporkan insiden keamanan informasi kepada petugas atau atasan langsung dalam waktu maksimal 1×24 jam setelah kejadian.

3. **Evaluasi Berkala**

   Tim Pengelola Keamanan Informasi melakukan evaluasi sistem, prosedur, dan insiden keamanan informasi secara berkala untuk perbaikan berkelanjutan.

4. **Sosialisasi dan Pelatihan**

   Mengadakan sosialisasi dan pelatihan keamanan informasi secara rutin untuk seluruh pegawai.

BAB IV
PROSEDUR KEAMANAN INFORMASI

4.1 Klasifikasi Informasi

1. Tujuan

Menetapkan prosedur pengklasifikasian informasi untuk menjamin keamanan, kerahasiaan, dan integritas data/informasi yang dikelola oleh Dinas Kominfo Persandian dan Statistik.

2. **Ruang Lingkup**

Prosedur ini berlaku untuk seluruh informasi yang dikelola, disimpan, dan disampaikan oleh Dinas Kominfo Persandian dan Statistik, baik dalam bentuk digital maupun fisik.

3. **Definisi**

a. **Informasi :** Data atau fakta yang telah diolah yang memiliki nilai bagi organisasi.

b. **Klasifikasi Informasi :** Proses penentuan tingkat sensitivitas dan perlakuan terhadap informasi.

c. **Kategori Klasifikasi :**

- ☑ **Sangat Rahasia :** Informasi yang jika bocor dapat menyebabkan kerugian besar bagi organisasi atau pihak lain.
- ☑ **Rahasia :** Informasi yang perlu dijaga kerahasiaannya karena dapat menimbulkan kerugian jika tersebar.
- ☑ **Terbatas :** Informasi yang hanya boleh diakses oleh pihak tertentu dalam organisasi.
- ☑ **Publik :** Informasi yang dapat diakses dan diketahui oleh umum tanpa pembatasan.

4. Prosedur

4.1 Identifikasi Informasi

a. Setiap unit kerja menginventarisasi informasi yang dimiliki dan mengkategorikan secara umum berdasarkan jenis dan fungsi.

4.2 Penentuan Klasifikasi

a. Pemilik informasi (information owner) bertanggung jawab menentukan klasifikasi awal berdasarkan dampak kerugian yang mungkin terjadi jika informasi tersebut bocor, dimanipulasi atau hilang.

b. Klasifikasi dilakukan dengan mempertimbangkan aspek kerahasiaan, integritas dan ketersediaan.

4.3 Penandaan Informasi

a. Setelah diklasifikasikan, informasi harus diberi label yang jelas sesuai kategori klasifikasi (misal: **Sangat Rahasia**, **Rahasia**, dll).
b. Label dapat berupa watermark, header/footer pada dokumen, atau metadata pada file digital.

4.4 Pengendalian Akses

a. Akses terhadap informasi diberikan sesuai dengan klasifikasinya dan kebutuhan tugas.
b. Informasi berklasifikasi tinggi hanya boleh diakses oleh personel yang memiliki hak dan kewenangan.
c. Penggunaan mekanisme keamanan seperti password, enkripsi, dan izin akses khusus harus diterapkan.

4.5 Peninjauan dan Re-Klasifikasi

a. Klasifikasi informasi harus ditinjau secara berkala (misal tiap 6 bulan atau setahun sekali) atau ketika ada perubahan kondisi.
b. Bila diperlukan, dilakukan re-klasifikasi agar sesuai dengan kondisi terbaru.

4.6 Pelaporan dan Penanganan Pelanggaran

a. Setiap indikasi kebocoran atau penyalahgunaan informasi harus segera dilaporkan ke tim keamanan informasi.
b. Tindakan penanganan pelanggaran dilakukan sesuai dengan prosedur keamanan informasi yang berlaku.

5. Tanggung Jawab

Pemilik Informasi	Menentukan dan memastikan klasifikasi informasi yang dikelola
Pengelola Sistem Informasi	Mengimplementasikan kontrol akses dan perlindungan sesuai klasifikasi.
Tim Keamanan Informasi	Mematuhi aturan penggunaan dan menjaga kerahasiaan informasi sesuai klasifikasinya.

Pengguna Informasi	Memantau, mengevaluasi, dan mengawasi pelaksanaan klasifikasi informasi

6. Dokumen Terkait

a. Kebijakan Keamanan Informasi
b. Prosedur Pengelolaan Akses Informasi
c. Pedoman Penanganan Insiden Keamanan Informasi.

4.2 Pengendalian Akses Informasi

Akses informasi diatur sesuai prinsip **need to know** dan **need to use**.

1. Tujuan

Menetapkan tata cara pengendalian akses terhadap informasi yang dikelola Dinas Kominfo Persandian dan Statistik untuk menjamin keamanan, kerahasiaan, integritas, dan ketersediaan informasi sesuai klasifikasinya.

2. Ruang Lingkup

Prosedur ini berlaku untuk seluruh sistem informasi, data, dan dokumen yang dikelola, baik berbentuk digital maupun fisik, yang berada di lingkungan Dinas Kominfo Persandian dan Statistik.

3. Definisi

a. **Akses Informasi :** Hak untuk menggunakan, melihat, mengubah, atau menghapus informasi sesuai kewenangan.
b. **Pemilik Informasi :** Unit atau pejabat yang bertanggung jawab atas suatu jenis informasi.
c. **Pengguna Informasi :** Personel yang memiliki hak akses terhadap informasi tertentu untuk keperluan tugasnya.

4. Prosedur

4.1 Penetapan Hak Akses

a. Hak akses ditentukan berdasarkan klasifikasi informasi dan kebutuhan kerja pengguna.
b. Pemilik informasi menetapkan siapa saja yang boleh mengakses informasi, jenis akses yang diperbolehkan (lihat, ubah, hapus, distribusi).
c. Semua hak akses harus dicatat dalam daftar kontrol akses.

4.2 Pengelolaan Hak Akses

a. Setiap permohonan akses harus diajukan secara formal melalui formulir permohonan akses informasi.
b. Akses diberikan setelah persetujuan dari pemilik informasi dan tim keamanan informasi.
c. Hak akses yang tidak diperlukan harus segera dicabut.

4.3 Autentikasi dan Otorisasi

a. Sistem informasi harus menerapkan autentikasi pengguna minimal menggunakan username dan password.
b. Untuk akses ke informasi berklasifikasi **Rahasia** dan **Sangat Rahasia**, gunakan mekanisme autentikasi ganda (two-factor authentication).
c. Pengguna hanya dapat mengakses informasi sesuai otorisasi yang diberikan.

4.4 Pengendalian Fisik

a. Dokumen fisik berklasifikasi **Rahasia** dan **Sangat Rahasia** disimpan di ruang penyimpanan terkunci dengan akses terbatas.
b. Ruang server dan ruang penyimpanan data penting harus dibatasi aksesnya dengan sistem kontrol akses fisik seperti kunci, kartu akses, atau sidik jari.

4.5 Pemantauan dan Audit Akses

a. Setiap aktivitas akses terhadap sistem informasi yang memuat data penting wajib direkam dalam log aktivitas.
b. Tim keamanan informasi melakukan pemeriksaan log secara berkala untuk mendeteksi adanya akses yang tidak sah atau mencurigakan.

4.6 Peninjauan Hak Akses

a. Hak akses pengguna harus ditinjau minimal setiap 6 bulan sekali atau saat terjadi perubahan jabatan, tugas, atau keluar masuk pegawai.
b. Hak akses yang tidak sesuai harus segera diperbaiki.

4.7 Penanganan Pelanggaran Akses

a. Pelanggaran terhadap pengendalian akses harus segera dilaporkan ke Tim Keamanan Informasi.
b. Tindakan penanganan dilakukan sesuai dengan prosedur penanganan insiden keamanan informasi.

5. Tanggung Jawab

Pemilik Informasi	Menetapkan hak akses sesuai klasifikasi
Pengelola Sistem Informasi	Mengimplementasikan dan memelihara kontrol akses di sistem.
Tim Keamanan Informasi	Melakukan pengawasan, audit, dan penanganan insiden akses.
Pengguna Informasi	Menggunakan informasi sesuai kewenangan dan tidak menyebarkan tanpa izin.

6. Dokumen Terkait

a. Prosedur Klasifikasi Informasi
b. Prosedur Penanganan Insiden Keamanan Informasi
c. Formulir Permohonan Akses Informasi

4.3 Pengelolaan Akses Sistem

1. Tujuan

Menjamin bahwa hak akses ke sistem informasi hanya diberikan kepada personel yang berwenang sesuai tugas dan tanggung jawabnya, guna menjaga kerahasiaan, integritas, dan ketersediaan data.

2. Ruang Lingkup

Prosedur **Pengelolaan Akses Sistem** ini berlaku untuk seluruh sistem informasi, infrastruktur teknologi informasi, dan layanan jaringan yang digunakan di lingkungan Dinas Komunikasi, Informatika, Persandian, dan Statistik, baik yang dikelola secara internal maupun oleh pihak ketiga

3. Prosedur :

3.1 Permohonan Akses

a. Pegawai atau pihak terkait yang membutuhkan akses sistem wajib mengisi **Formulir Permohonan Akses Sistem Informasi**.
b. Formulir harus mendapat persetujuan dari :
   ☑ Atasan Langsung
   ☑ Kepala Bidang TIK
   ☑ Admin Sistem

3.2 Pemberian Akses

a. Admin Sistem memberikan hak akses sesuai dengan permohonan yang telah disetujui.
b. Akses diberikan berdasarkan prinsip **least privilege** (akses minimum sesuai kebutuhan).
c. Setiap aktivitas pemberian akses dicatat dalam **Log Pemberian Akses Sistem**.

3.3 Perubahan Hak Akses

a. Perubahan hak akses dilakukan apabila :
   ☑ Ada perubahan jabatan atau tugas
   ☑ Permintaan resmi dari atasan langsung
b. Perubahan dicatat dalam **Log Perubahan Akses**.

3.4 Penonaktifan dan Penghapusan Akses

a. Akses pengguna wajib dinonaktifkan apabila :
   ☑ Pegawai resign, mutasi, atau pension
   ☑ Tidak lagi membutuhkan akses
   ☑ Terjadi pelanggaran keamanan
b. Proses penonaktifan dilakukan maksimal **1x24 jam** setelah keputusan berlaku.
c. Setiap aktivitas penonaktifan dicatat dalam **Log Penonaktifan Akses**.

3.5 Reset Password

a. Permintaan reset password hanya dilakukan oleh pemilik akun dengan verifikasi identitas.
b. Reset dilakukan oleh Admin TI dan dicatat di log reset password.

3.4 Audit Akses

a. Audit terhadap seluruh hak akses sistem dilakukan **minimal setiap 6 bulan sekali**.
b. Hak akses yang tidak aktif lebih dari 3 bulan tanpa alasan jelas akan dinonaktifkan sementara hingga dilakukan verifikasi ulang.

4. Tanggung Jawab

Kepala Bidang TIK	Menyetujui dan mengawasi proses pengelolaan akses sistem

Admin Sistem	Memberikan, mengubah, menonaktifkan, dan mencatat hak akses sistem
Atasan Langsung	Memberikan persetujuan terhadap permohonan akses bawahannya
Seluruh Pegawai	Menggunakan akses sesuai kewenangan dan menjaga kerahasiaan akun

5. Formulir dan Log Terkait

a. Formulir Permohonan Akses Sistem Informasi
b. Log Pemberian Akses Sistem
c. Log Perubahan Akses
d. Log Penonaktifan Akses
e. Log Reset Password

4.4 Backup dan Restore Data

1. **Tujuan**

Menjamin ketersediaan dan keamanan data penting dengan melakukan backup secara rutin dan restore data apabila terjadi gangguan, kerusakan, atau kebutuhan pemulihan data.

2. **Ruang Lingkup**

Prosedur ini mencakup seluruh aktivitas yang berkaitan dengan proses **pencadangan (backup)** dan **pemulihan (restore)** data serta sistem informasi yang dikelola oleh Dinas Komunikasi, Informatika, Persandian, dan Statistik,

3. **Prosedur**

3.1 Backup Data

a. **Jadwal Backup**

☑ Backup dilakukan secara:

- **Harian** untuk data operasional penting
- **Mingguan** untuk data aplikasi system
- **Bulanan** untuk seluruh data server dan database

b. **Media Backup**

☑ Backup disimpan ke media berikut:

- Harddisk eksternal
- Server Cadangan
- Cloud storage

☑ Media backup wajib terenkripsi.

c. **Proses Backup**

☑ Admin TI melakukan backup sesuai jadwal.

☑ Backup dilakukan di luar jam operasional untuk menghindari gangguan sistem.

☑ Hasil backup dicatat di **Log Backup Data**.

d. **Penyimpanan Media Backup**

☑ Media backup disimpan di ruang penyimpanan aman dan terbatas aksesnya.

☑ Setiap media backup diberi label tanggal dan keterangan isi data.

3.2 Restore Data

a. **Permohonan Restore**

☑ Pengguna yang memerlukan restore data wajib mengisi **Formulir Permohonan Backup & Restore Data**.

☑ Permohonan disetujui oleh :

- Atasan langsung
- Kepala Bidang TIK

b. **Proses Restore**

☑ Admin TI melakukan restore data sesuai permohonan.

☑ Restore dilakukan dari media backup terakhir atau sesuai tanggal yang diminta.

☑ Hasil restore dicatat di **Log Restore Data**.

c. **Konfirmasi Pengguna**

☑ Setelah proses restore selesai, pengguna wajib melakukan pengecekan data dan memberikan konfirmasi.

4. Penanggung Jawab

Kepala Bidang TIK	Menyetujui permohonan restore dan mengawasi pelaksanaan backup
Admin Sistem	Melaksanakan backup, restore, dan pencatatan log
Pengguna	Mengajukan permohonan restore dan melakukan verifikasi data

5. **Formulir dan Log Terkait**
    - Formulir Permohonan Backup & Restore Data
    - Log Backup Data
    - Log Restore Data

4.5 Penanganan Insiden Keamanan Informasi

1. **Tujuan**

   Menangani setiap insiden keamanan informasi secara cepat, tepat, dan terkoordinasi untuk meminimalkan dampak terhadap operasional dan kerahasiaan data.

2. Prosedur ini mencakup seluruh aktivitas yang berkaitan dengan **deteksi, pelaporan, analisis, penanganan, dan mitigasi insiden keamanan informasi** yang terjadi pada sistem informasi, jaringan, perangkat, serta data yang berada di lingkungan Dinas Komunikasi Informatika Persandian dan Statistik.

3. **Prosedur**

   3.1 Identifikasi Insiden

   a. Setiap pegawai wajib melaporkan insiden keamanan informasi, seperti:
      ☑ Virus/malware
      ☑ Kebocoran data
      ☑ Akses ilegal
      ☑ Gangguan sistem
   b. Insiden dilaporkan melalui :
      ☑ Lisan langsung ke Admin TI
      ☑ Mengisi **Formulir Laporan Insiden Keamanan Informasi**

   3.2 Pencatatan Insiden

   a. Admin TI mencatat insiden ke dalam **Log Insiden Keamanan Informasi** dengan detail :
      ☑ Tanggal kejadian
      ☑ Waktu
      ☑ Jenis insiden
      ☑ Lokasi
      ☑ Sistem/Perangkat terdampak
      ☑ Pelapor

☑ Dampak awal

3.3 Analisis dan Klasifikasi Insiden

a. Admin TI bersama Kepala Bidang TIK melakukan analisis awal.
b. Menentukan klasifikasi insiden :
   ☑ **Rendah** : Tidak berdampak signifikan
   ☑ **Sedang** : Mengganggu sebagian layanan
   ☑ **Tinggi** : Menghentikan layanan atau menyebabkan kerugian data besar

3.4 Penanganan dan Mitigasi

a. Melakukan tindakan sesuai tingkat insiden :
   ☑ Isolasi sistem/perangkat terdampak
   ☑ Pembersihan virus/malware
   ☑ Perubahan password
   ☑ Restore data dari backup
   ☑ Blokir akses tidak sah

3.5 Pelaporan Insiden

a. Insiden dilaporkan ke atasan langsung dan Kepala Bidang TIK **maksimal 1x24 jam** setelah kejadian.
b. Jika berdampak besar, laporan diteruskan ke Kepala Dinas.

3.6 Penyusunan Laporan Akhir

a. Admin TI membuat laporan insiden berisi :
   ☑ Kronologi kejadian
   ☑ Dampak
   ☑ Tindakan mitigasi
   ☑ Rekomendasi pencegahan ke depan
b. Laporan disimpan dalam **Arsip Insiden Keamanan Informasi**.

3.7 Evaluasi dan Tindak Lanjut

a. Dilakukan evaluasi rutin setiap **6 bulan** terhadap insiden yang pernah terjadi.
b. Menyusun rekomendasi perbaikan SOP atau penguatan sistem.

4. Penanggung Jawab

Kepala Bidang TIK	Menyetujui dan mengawasi proses penanganan insiden

Admin Sistem	Mencatat, menganalisis, menangani dan menyusun laporan insiden.
Pengguna	Melaporkan insiden yang terjadi

5. Formulir dan Log Terkait

a. Formulir Laporan Insiden Keamanan Informasi
b. Log Insiden Keamanan Informasi
c. Laporan Akhir Insiden

4.6 Pengelolaan Perangkat TI dan Jaringan

1. Tujuan

Memberikan pedoman pengelolaan perangkat teknologi informasi (TI) dan jaringan agar operasional sistem informasi berjalan aman, efisien dan terkontrol serta meminimalisir risiko ancaman terhadap keamanan informasi.

2. Ruang Lingkup

Prosedur ini mencakup seluruh aktivitas yang berkaitan dengan **pengelolaan, pengamanan, pemeliharaan, dan pengawasan terhadap perangkat teknologi informasi (TI) serta infrastruktur jaringan** yang digunakan di lingkungan Dinas Komunikasi Informatika Persandian dan Statistik.

3. Prosedur

3.1 Inventarisasi Perangkat

☑ Setiap perangkat TI wajib dicatat dalam **Daftar Inventaris TI**.
☑ Inventarisasi meliputi jenis perangkat, spesifikasi, nomor seri, lokasi dan penanggung jawab.
☑ Update inventaris dilakukan setiap ada penambahan, mutasi atau penghapusan perangkat.

3.2 Instalasi & Konfigurasi

☑ Instalasi perangkat hanya boleh dilakukan oleh petugas TI yang berwenang.
☑ Setiap instalasi wajib mengikuti standar keamanan (password default diganti, antivirus terpasang, firewall diaktifkan).
☑ Dokumentasi konfigurasi jaringan dan perangkat harus tersimpan di pusat data Dinas.

3.3 Pengelolaan Akses

- ☑ Hak akses ke perangkat jaringan (router, switch, firewall, server) hanya diberikan kepada personel yang berwenang.
- ☑ Akses administratif dicatat dan dievaluasi secara berkala.
- ☑ Password admin minimal 8 karakter, kombinasi huruf besar, kecil, angka dan simbol, serta diganti minimal 3 bulan sekali.

3.4 Monitoring & Maintenance

- ☑ Monitoring aktivitas jaringan dilakukan setiap hari menggunakan tools monitoring (jika ada).
- ☑ Pengecekan antivirus, patch system dan log keamanan dilakukan secara rutin.
- ☑ Maintenance perangkat dilakukan minimal setiap 6 bulan atau sesuai kebutuhan.

3.5 Backup Konfigurasi

- ☑ Konfigurasi penting perangkat jaringan disimpan di lokasi aman, terenkripsi, dan dilakukan backup rutin minimal setiap perubahan konfigurasi.

3.6 Pengamanan Fisik

- ☑ Ruang server dan perangkat jaringan harus dalam area terbatas, dilengkapi akses kontrol fisik (kunci/pin/card access).
- ☑ Hanya petugas berwenang yang boleh memasuki ruang server.
- ☑ CCTV aktif memantau area server selama 24 jam.

3.7 Penghapusan & Pemutakhiran

- ☑ Perangkat yang rusak atau tidak layak pakai harus dinonaktifkan, dicatat, dan dihapus dari daftar inventaris.
- ☑ Data pada perangkat yang akan dilepas/dihapus harus dibersihkan secara permanen (secure wipe).
- ☑ Pemutakhiran perangkat dilakukan sesuai siklus anggaran atau kebutuhan operasional.

C. Penanggung Jawab

Kepala Bidang TIK	Pengawasan keseluruhan proses pengelolaan perangkat dan jaringan

Admin Sistem	Instalasi, maintenance, backup, monitoring, pengamanan perangkat TI
Seluruh Pegawai	Menggunakan perangkat TI sesuai ketentuan, tidak melakukan instalasi tanpa izin

4.7 Penghapusan Data

1. Tujuan

Menjamin bahwa data yang sudah tidak diperlukan atau memiliki risiko keamanan bila tetap disimpan dapat dihapus secara aman, permanen dan terdokumentasi sesuai prosedur.

2. Ruang Lingkup

Prosedur ini mencakup seluruh aktivitas yang berkaitan dengan **penghapusan, pemusnahan, dan pembersihan data digital maupun fisik** yang tersimpan dalam sistem informasi, perangkat penyimpanan, dan media elektronik lainnya di lingkungan Dinas Komunikasi Informatika Persandian dan Statistik.

3. Prosedur

3.1 Identifikasi Data yang Akan Dihapus

a. Admin Sistem melakukan inventarisasi data yang :
   - ☑ Tidak lagi digunakan
   - ☑ Kadaluarsa sesuai ketentuan penyimpanan data
   - ☑ Tidak relevan terhadap kebutuhan operasional

3.2 Permohonan Penghapusan

a. Unit kerja yang memiliki data mengajukan permohonan penghapusan menggunakan **Formulir Permohonan Penghapusan Data**.
b. Permohonan disetujui oleh :
   - ☑ Atasan langsung
   - ☑ Kepala Bidang TIK

3.3 Metode Penghapusan

a. Data dihapus menggunakan metode **secure delete** agar tidak dapat dipulihkan, contoh :
   - ☑ Overwrite data minimal 3 kali
   - ☑ Menggunakan software secure erasure tools
b. Untuk media penyimpanan fisik (harddisk, flashdisk), dilakukan :

☑ **Physical destruction** (penghancuran fisik) bila diperlukan

3.4 Pencatatan Penghapusan

a. Setiap proses penghapusan wajib dicatat dalam **Berita Acara Penghapusan Data** yang memuat :
   - ☑ Jenis data
   - ☑ Lokasi penyimpanan
   - ☑ Tanggal penghapusan
   - ☑ Metode penghapusan
   - ☑ Pihak yang melakukan
   - ☑ Persetujuan atasan

3.5 Pelaporan

a. Berita Acara Penghapusan diserahkan kepada Kepala Bidang TIK dan disimpan sebagai arsip.

6. Penanggung Jawab

Kepala Bidang TIK	Menyetujui penghapusan data dan mengawasi pelaksanaannya
Admin Sistem	Melakukan penghapusan data dan mencatat dalam berita acara
Unit Pemilik Data	Mengajukan permohonan penghapusan data dan memastikan data tak diperlukan

7. Formulir dan Dokumen Terkait

a. Formulir Permohonan Penghapusan Data
b. Berita Acara Penghapusan Data

4.8 Pengelolaan Risiko Keamanan Informasi

1. Tujuan

Memberikan pedoman dalam melakukan identifikasi, analisis, evaluasi, dan pengendalian risiko terhadap keamanan informasi guna melindungi data, sistem, dan layanan informasi yang dikelola oleh Dinas Kominfo Persandian dan Statistik Provinsi Papua Barat.

2. Ruang Lingkup

Prosedur ini berlaku untuk seluruh aktivitas pengelolaan keamanan informasi yang berkaitan dengan :

a. Sistem informasi dinas.
b. Data layanan publik, statistik sectoral dan persandian.
c. Infrastruktur jaringan dan perangkat TI.
d. Data pribadi dan data rahasia milik pemerintah daerah.
e. Akses pihak ketiga terhadap sistem dan data dinas.

3. Prosedur

3.1 Identifikasi Risiko

a. Mengidentifikasi potensi ancaman terhadap keamanan informasi, baik dari internal maupun eksternal.
b. Mengidentifikasi kerentanan pada sistem, perangkat, aplikasi, data, dan proses kerja.
c. Mengelompokkan risiko berdasarkan kategori :
   ☑ Ancaman fisik
   ☑ Ancaman teknis
   ☑ Ancaman administrative
   ☑ Ancaman pihak ketiga

3.2 Analisis Risiko

a. Menganalisis potensi dampak dari setiap risiko terhadap:
   ☑ Kerahasiaan informasi.
   ☑ Integritas data.
   ☑ Ketersediaan layanan.
b. Menentukan tingkat risiko berdasarkan kemungkinan kejadian dan dampak yang ditimbulkan.

3.3 Evaluasi Risiko

a. Menentukan risiko yang dapat diterima dan yang harus segera dikendalikan.
b. Mengelompokkan risiko ke dalam :
   ☑ Risiko rendah (diterima).
   ☑ Risiko sedang (dipantau dan dikendalikan).
   ☑ Risiko tinggi (ditangani segera dengan tindakan pengendalian).

3.4 Pengendalian Risiko

a. Menyusun dan menerapkan langkah-langkah pengendalian untuk mengurangi kemungkinan dan dampak risiko.
b. Tindakan pengendalian :

- ☑ Penerapan firewall, antivirus, dan endpoint protection.
- ☑ Backup data berkala.
- ☑ Pengaturan hak akses sesuai prinsip least privilege.
- ☑ Pelatihan keamanan informasi bagi pegawai.
- ☑ Peningkatan pengamanan fisik ruang server.

3.5 Monitoring dan Tinjauan Risiko

a. Melakukan pemantauan berkala terhadap risiko dan efektivitas pengendalian yang diterapkan.
b. Melakukan review risiko minimal **setahun sekali** atau saat terjadi insiden keamanan.
c. Melaporkan hasil monitoring kepada pimpinan dinas.

4. Dokumentasi

a. Semua proses pengelolaan risiko wajib didokumentasikan dalam :
   - ☑ Formulir Identifikasi Risiko
   - ☑ Matriks Analisis Risiko
   - ☑ Rencana Pengendalian Risiko
   - ☑ Laporan Monitoring dan Review Risiko

5. Tanggung Jawab

Kepala Dinas	Bertanggung jawab atas pengesahan kebijakan dan pengendalian risiko strategis.
Tim Pengelola Keamanan Informasi	Bertanggung jawab atas pelaksanaan
Seluruh Pegawai	Wajib melaporkan potensi risiko atau insiden keamanan informasi yang ditemukan

6. Formulir dan Dokumen Terkait

a. Formulir Identifikasi Risiko Keamanan Informasi.
b. Matriks Analisis Risiko

BAB V
HAK DAN KEWAJIBAN PENGGUNA INFORMASI

5.1 Hak Pengguna Informasi

Setiap pegawai, pejabat, dan pihak ketiga yang diberikan akses terhadap informasi di lingkungan **Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Papua Barat** memiliki hak sebagai berikut :

1. **Mengakses informasi** sesuai dengan tugas, wewenang dan hak akses yang telah ditetapkan.
2. **Mendapatkan informasi yang akurat, tepat waktu dan sesuai kebutuhan** tugas kedinasan.
3. **Mendapatkan fasilitas keamanan informasi** yang memadai dalam melaksanakan tugas, baik berupa infrastruktur fisik maupun sistem teknologi informasi.
4. **Melaporkan insiden atau ancaman keamanan informasi** tanpa takut dikenai sanksi selama laporan dilakukan dengan itikad baik.
5. **Mengikuti pelatihan atau sosialisasi** terkait kebijakan dan prosedur keamanan informasi yang diselenggarakan oleh dinas.

5.2 Kewajiban Pengguna Informasi

Setiap pengguna informasi di lingkungan **Dinas Kominfo Papua Barat** wajib:

1. **Menjaga kerahasiaan, keutuhan dan ketersediaan informasi** sesuai klasifikasi dan ketentuan yang berlaku.
2. **Mematuhi seluruh kebijakan, SOP dan ketentuan pengelolaan informasi** yang ditetapkan.
3. **Menggunakan informasi dan fasilitas teknologi informasi hanya untuk keperluan kedinasan** sesuai tugas dan wewenangnya.
4. **Tidak menyalahgunakan hak akses informasi** untuk kepentingan pribadi, kelompok atau pihak lain.
5. **Melaporkan setiap insiden, ancaman, atau penyalahgunaan informasi** yang diketahuinya kepada petugas atau atasan langsung.
6. **Mengikuti pelatihan, sosialisasi dan uji pemahaman** terkait keamanan informasi.
7. **Mengamankan akun, password, media penyimpanan dan perangkat kerja** agar tidak disalahgunakan pihak yang tidak berwenang.

8. **Tidak menyebarluaskan informasi yang bersifat rahasia atau terbatas** tanpa izin resmi dari pejabat yang berwenang.
9. **Mematuhi ketentuan hukum dan peraturan perundang-undangan** terkait informasi dan transaksi elektronik.

5.3 Sanksi Pelanggaran

Setiap pelanggaran terhadap ketentuan hak dan kewajiban pengguna informasi akan dikenakan sanksi sesuai peraturan perundang-undangan dan ketentuan disiplin pegawai yang berlaku di lingkungan Dinas Kominfo Persandian dan Statistik Provinsi Papua Barat, antara lain :

1. Teguran lisan atau tertulis.
2. Pembatasan atau pencabutan hak akses.
3. Tindakan administratif sesuai Peraturan Pemerintah Nomor 94 Tahun 2021 tentang Disiplin PNS.
4. Pelaporan kepada aparat penegak hukum apabila terdapat unsur pidana

BAB VI
AUDIT DAN EVALUASI KEAMANAN INFORMASI

6.1 Tujuan Audit dan Evaluasi

Audit dan evaluasi keamanan informasi dilakukan untuk :

1. Menilai kesesuaian penerapan kebijakan dan prosedur keamanan informasi dengan standar, SOP dan ketentuan yang berlaku.
2. Mengidentifikasi potensi kelemahan, pelanggaran dan celah keamanan dalam pengelolaan informasi.
3. Memberikan rekomendasi perbaikan untuk peningkatan keamanan informasi secara berkelanjutan.
4. Memastikan efektivitas tindakan pengamanan dan kontinuitas layanan informasi.

6.2 Pelaksanaan Audit Keamanan Informasi

☒ ***Prosedur :***

1. Audit keamanan informasi dilakukan oleh Tim Pengelola Keamanan Informasi atau auditor internal yang ditunjuk secara berkala minimal **1 (satu) kali dalam setahun** atau sewaktu-waktu jika terdapat insiden besar.
2. Ruang lingkup audit meliputi :
   - ✓ Kebijakan dan prosedur keamanan informasi
   - ✓ Pengendalian akses informasi
   - ✓ Pengamanan fisik dan lingkungan
   - ✓ Pengelolaan media penyimpanan
   - ✓ Pengamanan jaringan
   - ✓ Penanganan insiden
   - ✓ Pengelolaan risiko
3. Audit dilaksanakan berdasarkan checklist standar keamanan informasi yang telah ditetapkan.
4. Hasil audit disusun dalam bentuk laporan yang memuat temuan, analisis, dan rekomendasi tindak lanjut.

6.3 Evaluasi Keamanan Informasi

☒ ***Prosedur :***

1. Evaluasi keamanan informasi dilakukan secara rutin untuk menilai efektivitas penerapan kebijakan, prosedur, dan pengamanan informasi.
2. Evaluasi dilakukan berdasarkan hasil audit, laporan insiden, hasil pemantauan keamanan jaringan, serta masukan dari pegawai.
3. Hasil evaluasi menjadi dasar perbaikan SOP, pembaruan kebijakan, atau peningkatan kapasitas sumber daya keamanan informasi.

6.4 Tindak Lanjut Hasil Audit dan Evaluasi

☒ **Prosedur :**

1. Tim Pengelola Keamanan Informasi menyusun rekomendasi tindak lanjut dari hasil audit dan evaluasi.
2. Tindak lanjut dapat berupa :
   - Penyempurnaan kebijakan dan SOP
   - Penguatan pengendalian akses
   - Perbaikan sistem dan jaringan
   - Peningkatan kesadaran dan pelatihan pegawai
3. Pelaksanaan tindak lanjut dilakukan oleh unit kerja terkait sesuai tugas dan kewenangannya.
4. Tim Pengelola Keamanan Informasi memantau dan mengevaluasi pelaksanaan tindak lanjut untuk memastikan perbaikan berjalan efektif

BAB VII
SANKSI DAN TINDAKAN PELANGGARAN

7.1 Prinsip Penegakan Sanksi

Penegakan sanksi terhadap pelanggaran keamanan informasi dilakukan secara adil, objektif, dan proporsional sesuai dengan tingkat pelanggaran yang terjadi. Sanksi bertujuan untuk mencegah terulangnya pelanggaran dan menjaga integritas sistem keamanan informasi.

7.2 Jenis Pelanggaran

Pelaksanaan keamanan informasi dapat mengalami pelanggaran berupa:

1. **Pelanggaran Ringan**

   Contoh : kelalaian dalam menjaga kerahasiaan password, terlambat melaporkan insiden tanpa dampak signifikan.
2. **Pelanggaran Sedang**

   Contoh : penyalahgunaan akses informasi untuk kepentingan pribadi, mengabaikan prosedur pengamanan data.
3. **Pelanggaran Berat**
4. Contoh : pembocoran informasi rahasia dengan sengaja, sabotase sistem, atau pelanggaran yang menyebabkan kerugian besar.

7.3 Sanksi atas Pelanggaran

Berdasarkan tingkat pelanggaran, sanksi yang dapat dikenakan meliputi:

1. **Teguran Lisan atau Tertulis** Diberikan untuk pelanggaran ringan sebagai peringatan dan edukasi.
2. **Pembatasan atau Pencabutan Hak Akses** Diberikan apabila pelanggaran berulang atau memiliki potensi merugikan sistem.
3. **Sanksi Administratif** Sesuai Peraturan Pemerintah dan peraturan internal, seperti penurunan pangkat, skorsing, atau pemberhentian sementara.
4. **Tindakan Hukum** Dilakukan apabila pelanggaran mengandung unsur pidana atau merugikan negara, termasuk pelaporan ke aparat penegak hukum.

7.4 Prosedur Penanganan Pelanggaran

1. Pelanggaran dilaporkan kepada Tim Pengelola Keamanan Informasi dan pimpinan terkait.
2. Dilakukan investigasi untuk memastikan fakta dan tingkat pelanggaran.
3. Berdasarkan hasil investigasi, dilakukan penetapan sanksi sesuai ketentuan.

4. Pihak yang dikenakan sanksi diberikan kesempatan untuk memberikan klarifikasi atau pembelaan.
5. Pelaksanaan sanksi didokumentasikan dan diawasi oleh Tim Pengelola Keamanan Informasi.

7.5 Perlindungan Pelapor

Dinas memberikan perlindungan kepada pegawai atau pihak lain yang melaporkan pelanggaran keamanan informasi secara jujur dan bertanggung jawab agar terhindar dari tindakan pembalasan (whistleblower protection).

BAB VIII
PENUTUP

8.1 Kesimpulan

SOP Keamanan Informasi ini disusun sebagai pedoman resmi untuk memastikan pengelolaan dan perlindungan informasi di lingkungan **Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat** berjalan efektif, aman, dan sesuai dengan standar yang berlaku.

Implementasi SOP ini merupakan tanggung jawab bersama seluruh pegawai dan pihak terkait untuk menjaga kerahasiaan, integritas dan ketersediaan informasi demi tercapainya pelayanan publik yang optimal.

8.2 Evaluasi dan Revisi

SOP ini akan dievaluasi secara berkala dan direvisi sesuai kebutuhan agar tetap relevan dengan perkembangan teknologi, kebijakan, serta kondisi organisasi.

8.3 Penutup

Demikian SOP Keamanan Informasi ini disusun untuk dipatuhi dan dilaksanakan secara konsisten oleh seluruh jajaran Dinas Kominfo Provinsi Papua Barat. Semoga SOP ini dapat mendukung terciptanya tata kelola keamanan informasi yang handal dan terpercaya.

LAMPIRAN

Lampiran 1 :

a. Formulir Permohonan Akses Sistem Informasi
b. Formulir Permohonan Akses Informasi
c. Formulir Permohonan Backup & Restore Data
d. Formulir Laporan Insiden Keamanan Informasi
e. Formulir Permohonan Penghapusan Data
f. Formulir Identifikasi Risiko Keamanan Informasi.

Lampiran 2 :

a. Log Pemberian Akses Sistem
b. Log Perubahan Akses
c. Log Penonaktifan Akses
d. Log Reset Password
e. Log Backup Data
f. Log Restore Data
g. Log Insiden Keamanan Informasi

Lampiran 3 :

a. Berita Acara Penghapusan Data
b. Laporan Akhir Insiden
c. Matriks Analisis Risiko

LAMPIRAN I

a. Formulir Permohonan Akses Sistem Informasi
b. Formulir Permohonan Akses Informasi
c. Formulir Permohonan Backup & Restore Data
d. Formulir Laporan Insiden Keamanan Informasi
e. Formulir Permohonan Penghapusan Data
f. Formulir Identifikasi Risiko Keamanan Informasi.

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR PERMOHONAN AKSES SISTEM INFORMASI

Nomor : ……
Hari/Tanggal : ……/……/… ../……..

A. Data Pemohon

No	Uraian	Isi
1.	Nama Lengkap	
2.	NIP/NIK	
3.	Jabatan	
4.	Unit Kerja	
5.	No. HP/Email	

B. Data Sistem/Aplikasi yang Dimohonkan

No	Nama Sistem/Aplikasi	Level Akses yang Dimohonkan (Admin/User/Viewer)	Keterangan
1.			
2.			

C. Alasan Permohonan

……
……
……

D. Persetujuan

No	Nama	Jabatan	Tanggal	Tanda Tangan
1		Atasan Langsung		
2		Kepala Bidang TIK		

A. Tindak Lanjut Admin Sistem

No	Tindakan	Tanggal	Nama Admin	Tanda Tangan
1	Akses Diberikan			
2	Akses Ditolak (alasan)			

Catatan :
- Formulir ini wajib diarsipkan oleh Admin Sistem setelah proses selesai.

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR PERMOHONAN AKSES INFORMASI

Nomor Formulir : …….

Hari/Tanggal Permohonan : ……. / ….. / ……../……

a. Data Pemohon

No.	Keterangan	Isi
1.	Nama Lengkap	
2.	NIP (jika ASN) / No. Identitas	
3.	Jabatan/Instansi/Unit Kerja	
4.	Alamat Email	
5.	Nomor Telepon/HP	

b. Informasi yang Dimohonkan

No.	Keterangan	Isi
1.	Jenis Informasi yang Dimohonkan	
2.	Tujuan Penggunaan Informasi	
3.	Sistem/Unit/Divisi yang Mengelola Informasi	

.

c. Persetujuan

No.	Keterangan	Paraf / Tanda Tangan
1	Atasan Langsung	
2	Tim Pengelola Keamanan Informasi	
3	Verifikasi Kepala Bidang	

d. **Catatan Tambahan (jika ada):**

……..

Tanda Tangan Pemohon

(……..)

Nama Lengkap

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR PERMOHONAN BACKUP & RESTORE DATA

Nomor : .....
Hari/Tanggal : ...../...../...../.....

A. Data Pemohon

No	Keterangan	Isi
1.	Nama Lengkap	
2.	NIP	
3.	Jabatan	
4.	Unit Kerja	
5.	No. HP/Email	

B. Jenis Permohonan

☐ Backup Data

☐ Restore Data

Sistem/Aplikasi : .....
Jenis Data : .....
Lokasi Penyimpanan : .....

C. Alasan Permohonan

.....
.....

D. Persetujuan

No	Nama Pejabat	Jabatan	Tanda Tangan & Tanggal
1.		Atasan Langsung	
2.		Kepala Bidang TIK	

E. Tindak Lanjut Admin Sistem

No	Tindakan	Tanggal	Nama Admin	Tanda Tangan
1	Backup/Restore Dilakukan			
2	Backup/Restore Ditolak (alasan)			

Catatan :

- Formulir ini wajib diarsipkan oleh Admin Sistem setelah proses selesa

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR LAPORAN INSIDEN KEAMANAN INFORMASI

Nomor Laporan : ……

Hari/Tanggal Kejadian : ……/……/……/……

A. Data Pelapor

No	Keterangan	Isi
1.	Nama Lengkap	
2.	NIP/NIK	
3.	Jabatan	
4.	Unit Kerja	
5.	No. HP/Email	

B. Detail Insiden

No	Keterangan	Isi
1.	Tanggal & Waktu Kejadian	
2.	Lokasi/Unit Sistem Terkait	
3.	Jenis Insiden	☐ Virus/Malware ☐ Akses Ilegal ☐ Kebocoran Data ☐ Gangguan Sistem ☐ Lainnya : ……
4.	Deskripsi Singkat Insiden	
5.	Dampak yang Ditimbulkan	

C. Tindakan Awal yang Diambil

……

……

D. Rekomendasi atau Permintaan Tindakan Lanjutan

……

……

E. Tindak Lanjut Tim TIK

No	Tindakan	Dilaksanakan Oleh	Tanggal	Keterangan
1.				
2.				

Dokumentasi Tambahan (Jika Ada) :

☐ Log Sistem ☐ Screenshot Bukti ☐ File Terkait

Catatan:

*- Formulir ini wajib dilaporkan maksimal **1×24 jam** sejak kejadian insiden, ditandatangani pelapor, atasan langsung, dan diserahkan ke Kepala Seksi Infrastruktur Dasar TIK untuk penanganan.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR LAPORAN INSIDEN KEAMANAN INFORMASI

Nomor Laporan : .....
Hari/Tanggal Kejadian : ...../...../...../.....

A. Data Pelapor

No	Keterangan	Isi
1.	Nama Lengkap	
2.	NIP/NIK	
3.	Jabatan	
4.	Unit Kerja	
5.	No. HP/Email	

B. Detail Insiden

No	Keterangan	Isi
1.	Tanggal & Waktu Kejadian	
2.	Lokasi/Unit Sistem Terkait	
3.	Jenis Insiden	☐ Virus/Malware ☐ Akses Ilegal ☐ Kebocoran Data ☐ Gangguan Sistem ☐ Lainnya : .....
4.	Deskripsi Singkat Insiden	
5.	Dampak yang Ditimbulkan	

C. Tindakan Awal yang Diambil

.....
.....

D. Rekomendasi atau Permintaan Tindakan Lanjutan

.....
.....

E. Tindak Lanjut Tim TIK

No	Tindakan	Dilaksanakan Oleh	Tanggal	Keterangan
1.				
2.				

Dokumentasi Tambahan (Jika Ada) :

☐ Log Sistem ☐ Screenshot Bukti ☐ File Terkait

Catatan:

*- Formulir ini wajib dilaporkan maksimal **1×24 jam** sejak kejadian insiden, ditandatangani pelapor, atasan langsung, dan diserahkan ke Kepala Seksi Infrastruktur Dasar TIK untuk penanganan.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR PERMOHONAN PENGHAPUSAN DATA

Nomor : .....

Tanggal : ...../...../...../.....

A. Data Pemohon

No.	Keterangan	Isi
1.	Nama Lengkap	
2.	NIP/NIK	
3.	Jabatan	
4.	Unit Kerja	
5.	No. HP/Email	

B. Detail Data yang Akan Dihapus

No.	Keterangan	Isi
1.	Nama Sistem/Aplikasi	
2.	Jenis Data	
3.	Lokasi Penyimpanan Data	
4.	Alasan Penghapusan Data	

C. Persetujuan

No	Nama	Jabatan	Tanda Tangan & Tanggal
1.		Atasan Langsung	
2.		Kepala Bidang TIK	

D. Tindak Lanjut Admin Sistem

No.	Tindakan Penghapusan	Tanggal Pelaksanaan	Nama Admin	Tanda Tangan
1.	Penghapusan Data Dilakukan			
2.	Penghapusan Ditolak (Alasan)			

Catatan:

- *Penghapusan data penting wajib melalui persetujuan atasan dan didokumentasikan.*
- *Data yang sudah dihapus tidak dapat dikembalikan.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

FORMULIR IDENTIFIKASI RISIKO KEAMANAN INFORMASI

Nomor Formulir : .....
Hari/Tanggal Identifikasi : ..... / ..... / ...../.....

A. Data Pengidentifikas

No.	Keterangan	Isi
1.	Nama Pengidentifikasi	
2.	Jabatan	
3.	Unit Kerja	

B. Informasi Risiko

No.	Keterangan	Isi
1.	Area/Kegiatan yang Dianalisis	
2.	Deskripsi Potensi Risiko	
3.	Sumber Ancaman	Internal / Eksternal / Teknis / Fisik
4.	Kerentanan (Vulnerability)	
5.	Dampak Potensial	Kerahasiaan / Integritas / Ketersediaan
6.	Tingkat Kemungkinan (Low/Medium/High)	
7.	Tingkat Dampak (Low/Medium/High)	
8.	Level Risiko (Dari Matriks Risiko)	Rendah / Sedang / Tinggi

C. Rencana Pengendalian Risiko

No.	Keterangan	Isi
1.	Rekomendasi Tindakan Pengendalian	
2.	Penanggung Jawab	
3.	Tindak Lanjut yang Dilakukan	
4.	Tanggal Rencana Tindak Lanjut	

D. Verifikasi

No.	Keterangan	Tanda Tangan
1.	Tim Pengelola Keamanan Informasi	
2.	Kepala Bidang Persandian dan Statistik	

E. Catatan Tambahan :

……
……

Tanda Tangan Pengidentifikasi

(……..)

Nama Lengkap

Keterangan :

- ☒ *Level Risiko dihitung berdasarkan Matriks Risiko (Likelihood x Impact).*
- ☒ *Formulir ini wajib diarsipkan sebagai bagian dari dokumentasi pengelolaan risiko keamanan informasi.*

LAMPIRAN II

a. Log Pemberian Akses Sistem
b. Log Perubahan Akses
c. Log Penonaktifan Akses
d. Log Reset Password
e. Log Backup Data
f. Log Restore Data
g. Log Insiden Keamanan Informasi

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG PEMBERIAN AKSES SISTEM

No	Tanggal	Nama Pengguna	NIP	Unit Kerja	Sistem/Aplikasi	Level Akses	Disetujui Oleh	Diberikan Oleh	Keterangan
1.									
2.									
3.									
4.									
dst.									

Keterangan Kolom :

- ☑ ***No*** *: Nomor urut log*
- ☑ ***Tanggal*** *: Tanggal akses diberikan*
- ☑ ***Nama Pengguna*** *: Nama lengkap pengguna yang diberi akses*
- ☑ ***NIP*** *: Nomor induk pegawai*
- ☑ ***Unit Kerja*** *: Unit kerja asal pengguna*
- ☑ ***Sistem/Aplikasi*** *: Nama sistem atau aplikasi yang diakses*
- ☑ ***Level Akses*** *: Hak akses yang diberikan (Admin, User, Viewer, dll.)*
- ☑ ***Disetujui Oleh*** *: Pejabat yang menyetujui akses*
- ☑ ***Diberikan Oleh*** *: Admin sistem yang memberikan akses*
- ☑ ***Keterangan*** *: Misalnya Baru, Ubah Akses, Nonaktif, dll.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG PERUBAHAN AKSES

No	Tanggal	Nama Pengguna	NIP	Sistem/ Aplikasi	Perubahan Akses (Sebelum)	Perubahan Akses (Sesudah)	Disetujui Oleh	Disetujui Oleh	Keterangan
1.									
2.									
3.									
4.									
dst.									

Keterangan Kolom :

- ☑ ***No*** *: Nomor urut pencatatan*
- ☑ ***Tanggal*** *: Tanggal perubahan akses dilakukan*
- ☑ ***Nama Pengguna*** *: Nama pegawai yang aksesnya diubah*
- ☑ ***NIP*** *: Nomor induk pegawai*
- ☑ ***Sistem/Aplikasi*** *: Nama sistem/aplikasi yang diubah aksesnya*
- ☑ ***Perubahan Akses (Sebelum)*** *: Level akses sebelum perubahan*
- ☑ ***Perubahan Akses (Sesudah)*** *: Level akses setelah perubahan*
- ☑ ***Disetujui Oleh*** *: Pejabat yang menyetujui perubahan*
- ☑ ***Diperbarui Oleh*** *: Admin sistem yang melakukan perubahan*
- ☑ ***Keterangan*** *: Misalnya Promosi jabatan, Penyesuaian tugas, Rotasi, dll.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG PENONAKTIFAN AKSES

No	Tanggal	Nama Pengguna	NIP	Sistem/Aplikasi	Alasan Penonaktifan	Disetujui Oleh	Dinonaktifkan Oleh	Keterangan
1								
2								
3								
4								
dst.								

Keterangan Kolom :

- ☑ ***No*** *: Nomor urut log*
- ☑ ***Tanggal*** *: Tanggal penonaktifan akses dilakukan*
- ☑ ***Nama Pengguna*** *: Nama pegawai yang aksesnya dinonaktifkan*
- ☑ ***NIP/NIK*** *: Nomor induk pegawai*
- ☑ ***Sistem/Aplikasi*** *: Nama sistem/aplikasi yang aksesnya dinonaktifkan*
- ☑ ***Alasan Penonaktifan*** *: Misalnya Pindah tugas, Pensiun, Cuti panjang, Pelanggaran, dll.*
- ☑ ***Disetujui Oleh*** *: Pejabat yang menyetujui penonaktifan*
- ☑ ***Dinonaktifkan Oleh*** *: Admin sistem yang melakukan penonaktifan*
- ☑ ***Keterangan*** *: Misalnya Permanen, Sementara, Bisa aktif kembali, dll.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG RESET PASSWORD

No	Tanggal	Nama Pengguna	NIP	Sistem/Aplikasi	Alasan Reset	Diminta Oleh	Dilakukan Oleh	Keterangan
1								
2								
3								
4								
dst								

Keterangan Kolom :

- ☑ ***No*** *: Nomor urut log*
- ☑ ***Tanggal*** *: Tanggal reset password dilakukan*
- ☑ ***Nama Pengguna*** *: Nama pegawai yang password-nya di-reset*
- ☑ ***NIP/NIK*** *: Nomor induk pegawai*
- ☑ ***Sistem/Aplikasi*** *: Nama sistem/aplikasi yang password-nya di-reset*
- ☑ ***Alasan Reset*** *: Misalnya Lupa password, Akun terkunci, Permintaan rutin, Kompromi akun, dll.*
- ☑ ***Diminta Oleh*** *: Nama pegawai/atasan yang mengajukan permohonan reset*
- ☑ ***Dilakukan Oleh*** *: Admin sistem yang melakukan reset password*
- ☑ ***Keterangan*** *: Misalnya Password default, Password sementara, Diminta ganti saat login, dll.*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG BACKUP DATA

No	Tanggal Backup	Nama Sistem/Aplikasi	Jenis Data	Media Penyimpanan	Lokasi Penyimpanan	Dilakukan Oleh	Status Backup	Keterangan
1.								
2.								
3.								
4.								
dst								

Keterangan Kolom :

- ☑ ***No*** *: Nomor urut log*
- ☑ ***Tanggal Backup*** *: Tanggal backup dilakukan*
- ☑ ***Nama Sistem/Aplikasi*** *: Nama sistem/aplikasi yang datanya dibackup*
- ☑ ***Jenis Data*** *: Jenis data yang dibackup (Database, Dokumen, Media, dll.)*
- ☑ ***Media Penyimpanan*** *: Media tempat data backup disimpan (Harddisk Eksternal, Cloud, Tape, Server Cadangan, dll.)*
- ☑ ***Lokasi Penyimpanan*** *: Lokasi fisik/virtual media penyimpanan*
- ☑ ***Dilakukan Oleh*** *: Nama admin yang melakukan backup*
- ☑ ***Status Backup*** *: Berhasil atau Gagal*
- ☑ ***Keterangan*** *: Tambahan informasi, misal backup harian/mingguan/bulanan atau catatan khusus*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG RESTORE DATA

No	Tanggal Restore	Nama Sistem/Aplikasi	Jenis Data	Permohonan Oleh	Disetujui Oleh	Dilakukan Oleh	Media Sumber	Status Restore	Keterangan
1.									
2.									
3.									
4.									
dst									

Keterangan Kolom :

- ☑ ***No*** *: Nomor urut log*
- ☑ ***Tanggal Restore*** *: Tanggal restore dilakukan*
- ☑ ***Nama Sistem/Aplikasi*** *: Nama sistem/aplikasi yang datanya direstore*
- ☑ ***Jenis Data*** *: Jenis data yang direstore (Database, Dokumen, Media, dll.)*
- ☑ ***Permohonan Oleh*** *: Nama pemohon restore data*
- ☑ ***Disetujui Oleh*** *: Pejabat yang menyetujui permohonan*
- ☑ ***Dilakukan Oleh*** *: Nama admin yang melakukan restore*
- ☑ ***Media Sumber*** *: Media tempat data restore diambil (Harddisk Eksternal, Cloud, Server Cadangan, dll.)*
- ☑ ***Status Restore*** *: Berhasil atau Gagal*
- ☑ ***Keterangan*** *: Keterangan tambahan misal alasan restore, versi data, atau catatan penting lainny*

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LOG INSIDEN KEAMANAN INFORMASI

No.	Tanggal & Waktu Kejadian	Pelapor	Jenis Insiden	Deskripsi Singkat Insiden	Dampak yang Ditimbulkan	Tindakan Awal	Tindak Lanjut	Status (Selesai /Proses)	PIC Penanganan	Ket
1.										
2.										
3.										
4.										
dst										

Keterangan Kolom :

- ☑ ***Tanggal & Waktu Kejadian*** *: Waktu saat insiden terjadi.*
- ☑ ***Pelapor*** *: Nama pegawai atau pihak yang melaporkan insiden.*
- ☑ ***Jenis Insiden*** *: Contoh: malware, phishing, kebocoran data, kerusakan sistem, dll.*
- ☑ ***Deskripsi Singkat Insiden*** *: Ringkasan kejadian.*
- ☑ ***Dampak yang Ditimbulkan*** *: Misal: gangguan layanan, kehilangan data, kerugian reputasi.*
- ☑ ***Tindakan Awal*** *: Langkah awal yang diambil untuk mitigasi.*
- ☑ ***Tindak Lanjut*** *: Langkah lanjutan untuk penyelesaian dan pencegahan berulang.*
- ☑ ***Status*** *: Selesai / Proses.*
- ☑ ***PIC Penanganan*** *: Nama personel yang bertanggung jawab menangani insiden.*
- ☑ ***Keterangan*** *: Catatan tambahan jika ada.*

LAMPIRAN III

a. Berita Acara Penghapusan Data
b. Laporan Akhir Insiden
c. Matriks Analisis Risiko Keamanan Informasi

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

BERITA ACARA PENGHAPUSAN DATA

Nomor : ……

Hari/Tanggal : ……/……/……/……/……

Pada hari …., tanggal……, bulan,……Tahun,…..kami yang bertanda tangan di bawah ini :

No.	Nama Lengkap	Jabatan	Unit Kerja	Tanda Tangan
1.				
2.				
3.				
dst				

Menyatakan bahwa:

1. Data berikut ini telah dilakukan penghapusan secara permanen sesuai dengan prosedur yang berlaku :

No.	Nama Sistem/Aplikasi	Jenis Data	Lokasi Penyimpanan Data	Metode Penghapusan
1.				
2.				
3.				
dst				

2. Penghapusan data dilakukan pada tanggal…… bulan…… tahun…… oleh…… (nama pelaksana penghapusan).
3. Proses penghapusan data ini telah disetujui oleh atasan langsung dan sesuai dengan ketentuan keamanan informasi yang berlaku.

Demikian berita acara ini dibuat untuk digunakan sebagaimana mestinya.

Pelaksana Penghapusan Data

1. Nama : ……
2. Jabatan : ……..
3. Tanggal : ……..
4. Tanda Tangan : ……..

Atasan Langsung

1. Nama : ……
2. Jabatan : ……..
3. Tanggal : ……..
4. Tanda Tangan : ……..

PEMERINTAH PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK

Alamat : Kompleks Perkantoran Gubernur Arfai

LAPORAN AKHIR INSIDEN KEAMANAN INFORMASI

Nomor Laporan : .....
Hari/Tanggal Laporan : ...../...../.....
Nomor Insiden : .....
Hari/Tanggal Kejadian : ...../...../...../...../.....

A. Informasi Umum Insiden

No	Keterangan	Isi
1.	Pelapor	
2.	Unit/Sistem Terkait	
3.	Jenis Insiden	
4.	Lokasi Kejadian	
5.	Dampak Insiden	

B. Kronologi Kejadian

.....
.....

C. Tindakan Penanganan

No	Tindakan	Pelaksana	Tanggal	Hasil / Status
1.				
2.				
3.				
dst				

D. Evaluasi dan Analisis

- Penyebab utama insiden : .....
- Kelemahan sistem/proses :.....
- Dampak jangka pendek dan jangka Panjang : .....

E. Rekomendasi Pencegahan dan Perbaikan

.....
.....

F. Pernyataan Penutupan

Dengan ini kami menyatakan insiden telah ditangani dan laporan ini menjadi dokumentasi resmi untuk tindak lanjut dan audit keamanan informasi.

Disusun Oleh :

Nama : .....
Jabatan : .....
Tanggal : .....
Tanda Tangan : .....

Diverifikasi Oleh :

Nama : .....
Jabatan : .....
Tanggal : .....
Tanda Tangan : .....

PEMERINTAH PROVINSI PAPUA BARAT
DINAS KOMUNIKASI INFORMATIKA PERSANDIAN & STATISTIK
Alamat : Kompleks Perkantoran Gubernur Arfai

MATRIKS ANALISIS RISIKO KEAMANAN INFORMASI

A. Kategori Tingkat Dampak (Impact)

Skor	Kategori	Keterangan
1.	Rendah	Kerugian ringan, tidak berdampak signifikan pada layanan atau data.
2.	Sedang	Mengganggu sebagian layanan atau berpotensi kebocoran data terbatas.
3.	Tinggi	Menghentikan layanan utama, kebocoran data penting, kerugian besar.

B. Kategori Tingkat Kemungkinan (Likelihood)

Skor	Kategori	Keterangan
1	Rendah	Jarang terjadi, kecil kemungkinan terjadi dalam 1 tahun.
2	Sedang	Mungkin terjadi 1–2 kali dalam 1 tahun.
3	Tinggi	Sering terjadi, lebih dari 2 kali dalam 1 tahun.

C. Matriks Risiko

Skor	Level Risiko	Tindakan Yang Diperlukan
1–2	Rendah	Diterima, cukup dipantau.
3–4	Sedang	Perlu tindakan pengendalian moderat dan monitoring berkala.
6–9	Tinggi	Perlu penanganan segera dan mitigasi prioritas tinggi.

D. Kategori Level Risiko

Skor	Level Risiko	Tindakan Yang Diperlukan
1–2	Rendah	Diterima, cukup dipantau.
3–4	Sedang	Perlu tindakan pengendalian moderat dan monitoring berkala.
6–9	Tinggi	Perlu penanganan segera dan mitigasi prioritas tinggi.

Contoh Penggunaan:

Jika suatu risiko memiliki:

- **Kemungkinan** : Tinggi (3)
- **Dampak** : Sedang (2)

Maka skor = **3 x 2 = 6** → **Tingkat Risiko: Tinggi**

Tindakan: Segera lakukan mitigasi dan monitoring intensif.