KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI PROVINSI PAPUA BARAT

DINAS KOMUNIKASI INFORMATIKA STATISTIK DAN PERSANDIAN
PEMERINTAH PROVINSI PAPUA BARAT | 2024

LEMBAR PENGESAHAN

Disusun Oleh : Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat

Diperiksa Oleh : Nama : Zaenal Fanumbi. ST, M.Kom.
NIP : 198106212009091002
Jabatan : Kepala Bidang Persandian dan Statistik
Tanda Tangan :

Disetujui Oleh : Nama : Frans P. Istia. S.Sos, M.M
NIP : 196903101991031017
Jabatan : Kepala Dinas Komunikasi Informatika, Persandian Dan Statistik
Tanda Tangan :

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH PROVINSI PAPUA BARAT

Pengarah:
Sekretaris Daerah Provinsi Papua Barat

Penanggung Jawab:
Kepala Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat

Tim Penyusun:
Dr. Eng. Ir. Yuyun, S.Kom., M.T.
Dr. Eng. Hazriani, S.Kom., M.T.
Dr. Ir. Abdul Latief Arda, M.Kom., M.Si.
Muhammad Risal, S.Kom., M.T.
Andy Lukman Affandy, S.Kom., M.T.

Tim Editor:
Nurfaedah, S.Pd., M.Hum.
Nur Adha, S.Kom.

Desain Sampul: Muhammad Ikbal Mursidin, S.Kom.

Diterbitkan oleh Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat
Jl. Abraham O. Atururi, Arfai. Kabupaten Manokwari, Provinsi Papua Barat Selatan, Indonesia
Website: https://diskominfoperstatik.papuabaratprov.go.id/

LOG MODIFIKASI

Versi	Oleh	Tanggal	Keterangan Modifikasi
1	Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat	2 Agustus 2024	Dokumen Versi I

DOKUMEN INI MERUPAKAN DOKUMEN YANG SENANTIASA DAPAT BERUBAH SESUAI DENGAN PERKEMBANGAN PROSES BISNIS DAN TEKNOLOGI, SEHINGGA PERLU DILAKUKAN REVIEW SEKURANG-KURANGNYA SETAHUN SEKALI

SAMBUTAN

KEPALA DINAS KOMUNIKASI INFORMATIKA, PERSANDIAN DAN STATISTIK PROVINSI PAPUA BARAT

Puji syukur kami panjatkan kehadirat Tuhan yang Maha Esa, atas berkat rahmat dan karunia-Nya, Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat, telah menyelesaikan kegiatan penyusunan buku Kebijakan Sistem Manajemen Keamanan Informasi sebagai bentuk tanggung jawab pengelolaan Keamanan Sistem Pemerintahan Berbasis Elektronik dalam lingkup Pemerintah Provinsi Papua Barat.

Kemajuan pesat serta potensi pemanfaatan teknologi informasi dan komunikasi (TIK) membuka peluang bagi pengaksesan, pengelolaan dan pendayagunaan informasi secara cepat dan akurat. Pemanfaatan TIK dalam pemerintahan yang secara nasional dikenal dengan Sistem Pemerintahan Berbasis Elektronik (SPBE) berperan meningkatkan efisiensi, efektifitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan. Namun di sisi lain, terdapat ancaman keamanan dalam penyelenggaraan SPBE yang dapat mengganggu ketersediaan dan kerahasiaan aset informasi yang bersifat merugikan, baik kerugian finansial, dampak sosial, masalah hukum, hingga penurunan reputasi organisasi. Gangguan tersebut dapat bersifat eksternal berupa ancaman privasi, pencurian informasi yang berorientasi profit, hingga ancaman keamanan nasional, serta ancaman dari dalam organisasi yang dilakukan oleh orang dalam di organisasi (*insider*) baik disengaja ataupun tidak disengaja. Selain itu, bencana alam (banjir, kebakaran, gempa bumi, gangguan hewan, dll) maupun ancaman kegagalan teknis (kesalahan penggunaan ataupun kegagalan perangkat keras/lunak) dapat pula menyebabkan hilangnya data, merusak perangkat TIK serta menghambat layanan informasi.

Mencermati besarnya resiko gangguan terhadap aset informasi, maka Pemerintah Provinsi Papua Barat melalui kewenangan Dinas Komunikasi Informatika, Persandian dan Statistik, menyusun buku panduan tentang **Kebijakan Sistem Manajemen Keamanan Informasi Pemerintah Provinsi Papua Barat**, yang diharapkan dapat menjadi solusi cerdas dalam mengelola aset informasi Pemerintah Provinsi Papua Barat. Dokumen ini disusun mengacu pada Standar Internasional ISO 27001:2013 yaitu standar yang mengatur tentang kerangka kerja untuk pendekatan sensitif terkait pengelolaan sistem keamanan informasi.

Akhir kata semoga kehadiran buku Pedoman SMKI ini dapat dimanfaatkan sebaik-baiknya dan menjadi acuan oleh seluruh elemen perangkat daerah, pegawai, maupun pihak ketiga dalam menjaga keamanan dan ketersediaan aset informasi Pemerintah Provinsi Papua Barat.

Manokwari, 31 Juli 2024

KADIS KOMINFOPERSTATIK
PROVINSI PAPUA BARAT

DAFTAR ISI

LEMBAR PENGESAHAN II
IDENTITAS PENYUSUN II
LOG MODIFIKASI IV
SAMBUTAN V
DAFTAR ISI VII
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Maksud dan Tujuan 1
1.3 Acuan Penyusunan 2
1.4 Ruang Lingkup 2
BAB II RUANG LINGKUP SISTEM MANAJEMEN KEAMANAN INFORMASI 6
2.1 Pengendalian Kebijakan Keamanan Informasi 6
2.2 Pengendalian Organisasi Keamanan Informasi 8
2.3 Pengendalian Sumber Daya Manusia 10
2.4 Pengelolaan Aset 12
2.5 Pengendalian Akses 16
2.6 Kriptografi 21
2.7 Keamanan Fisik dan Lingkungan 22
2.8 Komunikasi dan Manajemen Operasi 26
2.9 Keamanan Komunikasi 32
2.10 Akuisisi Sistem, Pengembangan dan Pemeliharaan 35
2.11 Hubungan dengan Pihak Ketiga atau Pemasok 39
2.12 Manajemen Insiden Keamanan Informasi 45
2.13 Keamanan Informasi dari Aspek Manajemen Kelangsungan Organisasi 49
2.14 Kepatuhan 51
BAB III PENUTUP 56
LAMPIRAN 57

Formulir 01 Revisi Dokumen *57*
Formulir 02 Daftar Distribusi Dokumen 58
Formulir 03 Rangkuman, Rencana & Verifikasi Perbaikan Hasil Audit Internal *59*
Formulir 04 Rencana Audit Internal *60*
Formulir 05 Rekapitulasi Temuan Audit Internal *61*
Formulir 06 Logbook Insiden Keamanan Informasi *62*
Formulir 07 Laporan Insiden Keamanan Informasi *63*
Formulir 08 Penilaian/Evaluasi Pihak Ketiga atau Pemasok *64*
Formulir 09 Permohonan User/Hak Akses Sistem/Aplikasi *65*
Formulir 10 Penyimpanan Aset Informasi *66*
Formulir 11 Penggunaan dan Pembagian Aset Informasi *67*
Formulir 12 Pengembalian Aset *68*
Formulir 13 Berita Acara Pemusnahan Dokumen dan Perangkat *69*
Formulir 14 Hak Akses Pengguna *70*
Formulir 15 Struktur Folder Untuk Akses Pengguna *71*
Formulir 16 Visitor Log Book Secure Area *72*
Formulir 17 Permohonan Peminjaman Fasilitas TI *73*
Formulir 18 Laporan Kerusakan Dan Perbaikan Perangkat Teknologi Informasi *74*
Formulir 19 Backup Checklist *75*
Formulir 20 Prosedur Pengelolaan Keamanan Jaringan *76*
Formulir 21 Komunikasi Eksternal *77*
Formulir 22 Komunikasi Internal *78*
Formulir 23 Log Book Kerusakan Dan Perbaikan Perangkat Teknologi Informasi *79*
Formulir 24 Permintaan Perubahan *80*
Formulir 25 Permohonan Pembuangan/Pemusnahan Aset *81*
Formulir 26 Validasi/Evaluasi Kelayakan Produk IT *82*
Formulir 27 Post Incident review *83*
Formulir 28 Evaluasi Kesesuaian Persyaratan Dan Peraturan Perundungan *84*

Formulir 29 Permohonan Penyimpanan Informasi/Data..... 85
Formulir 30 Prosedur Kesesuaian Terhadap Persyaratan 86

BAB I
PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan aset penting bagi sebuah organisasi, tidak terkecuali bagi organisasi perangkat daerah dalam lingkup Pemerintah Provinsi Papua Barat. Mencermati fakta tingginya kasus insiden kebocoran, kerusakan, serta gangguan lainnya terhadap ketersediaan informasi pada sistem pemerintahan berbasis elektronik (SPBE) yang dapat menyebabkan kerugian finansial maupun non finansial, perlu ditetapkan kebijakan atau aturan terkait pengamanan dan perlindungan informasi yang dikenal dengan Sistem Manajemen Keamanan Informasi (SMKI).

Kebijakan keamanan informasi memuat standar, prosedur, serta formulir untuk menjadi pedoman bagi setiap unsur dalam lingkup pemerintah Provinsi Papua Barat serta pihak ketiga dalam mengakses, mengelola dan melaksanakan tanggung jawab keamanan informasi. Penerapan SMKI dalam lingkup Provinsi Papua Barat dikoordinasikan oleh Dinas Komunikasi Informatika, Persandian dan Statistik.

1.2 Maksud dan Tujuan

Dokumen SMKI dimaksudkan sebagai dukungan manajemen terkait penerapan kebijakan keamanan informasi guna memandu proses pengamanan informasi dalam lingkup pemerintah Provinsi Papua Barat agar prinsip-prinsip keamanan informasi meliputi aspek kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi dapat dipertahankan. Kebijakan dan standar ini disusun dengan tujuan agar manajemen dapat:

a. Memastikan terpeliharanya kerahasiaan, integritas dan ketersediaan informasi beserta seluruh sistem dan sumber daya informasi;
b. Membangun pengamanan untuk melindungi aset informasi dari ancaman pencurian, penyalahgunaan, dan kerusakan;
c. Memastikan terlaksananya prinsip (istilah indonesia) atau *non-repudiation* atas pihak-pihak yang terlibat dalam proses bisnis organisasi;
d. Menetapkan tanggung jawab dan akuntabilitas pengguna dalam mengakses informasi milik organisasi;
e. Memastikan terpenuhinya kepatuhan terhadap hukum, undang-undang, dan peraturan eksternal yang berlaku;
f. Memastikan kemampuan pemulihan (*recovery*) ketika terjadi insiden keamanan informasi atau ancaman terhadap sistem informasi organisasi yang signifikan;

g. Mendorong manajemen dan seluruh pegawai, serta pihak terkait untuk memiliki kesadaran (*awareness*), pengetahuan dan keterampilan yang memadai agar dapat memenuhi kewajiban masing-masing dalam menjaga keamanan aset informasi organisasi;
h. Memiliki sumber daya yang memadai untuk melaksanakan program keamanan informasi yang efektif;
i. Memastikan konsistensi dan ketangguhan dalam menerapkan keamanan informasi.

1.3 Acuan Penyusunan

Dokumen SMKI ini disusun dengan mengacu pada beberapa peraturan dan dokumen sebagai berikut:

a. Peraturan Presiden Nomor 82 Nomor 2023 tentang Percepatan Transformasi Digital dan Sistem Pemerintahan Berbasis Elektronik (SPBE).
b. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.
c. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional.
d. Peraturan Menteri PAN-RB RI Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE Nasional.
e. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016, tentang Sistem Manajemen Pengamanan Informasi.
f. 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.
g. Peraturan Gubernur Provinsi Papua Barat Nomor 33 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah.
h. Peraturan Gubernur Provinsi Papua Barat Nomor 18 Tahun 2018 tentang uraian tugas dan fungsi Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat.

1.4 Ruang Lingkup

Dokumen ini menyediakan satu set referensi kontrol termasuk panduan implementasi kebijakan keamanan informasi dalam lingkup Pemerintah Provinsi Papua Barat di bawah koordinasi Dinas Komunikasi Informatika, Persandian dan Statistik berdasarkan kerangka ISO/IEC 27001:2013, sebuah dokumen standar terkait kontrol keamanan informasi yang diakui secara internasional. Garis besar elemen kontrol SMKI sebagaimana terangkum pada Tabel 1.1.

Tabel 1.1. Domain & Elemen Kendali SMKI

No	Domain	Elemen Kontrol	Aspek Pengendalian Keamanan SPBE (Pergub 33 Tahun 2023)
1	**Kebijakan Keamanan Informasi**. Menyediakan kebijakan keamanan informasi yang sesuai dengan konteks organisasi dan relevan dengan aturan/ regulasi yang berlaku.	Pedoman organisasi terkait keamanan informasi	Audit Internal Keamanan SPBE (r)
2	**Organisasi Keamanan Informasi.** Menetapkan kerangka kerja untuk menginisiasi dan mengontrol proses penerapan/pelaksanaan keamanan informasi dalam organisasi (internal), serta pihak luar (eksternal) yang terkait.	a. Internal organisasi. b. External organisasi: *Mobile Device & networking.*	Penanganan Insiden Keamaman Informasi (m)
3	**Keamanan Sumber Daya Manusia.** Menetapkan pedoman bagi para pegawai dan kontraktor/pihak ketiga terkait tanggung jawab keamanan informasi.	a. Sebelum penempatan, b. Selama masa penugasan, c. Setelah berhenti/pindah tugas.	Keamanan Sumber Daya Manusia (f)
4	**Pengelolaan Aset.** Memberikan panduan dalam melindungi dan menjamin keamanan aset informasi.	a. Tanggung jawab terhadap aset informasi, b. Klasifikasi aset, c. Penanganan aset informasi.	Pengelolaan Aset (g)
5	**Pengendalian Akses.** Memastikan perangkat pengolah informasi baik akses fisik maupun logik dalam hal ini perangkat pengolah informasi melalui kontrol otoritas akses pengguna.	a. Persyaratan dalam pengendalian akses, b. Pengelolaan hak akses pengguna, c. Tanggung jawab pengguna, d. Pengendalian akses informasi, e. Pengendalian akses jaringan,	Keamanan Jaringan (b); Keamanan Pusat Data (c); Keamanan Surat Elektronik (d); Keamanan data pribadi (h);

No	Domain	Elemen Kontrol	Aspek Pengendalian Keamanan SPBE (Pergub 33 Tahun 2023)
		f. Pengendalian akses perangkat *mobile* dan *telecommuting*.	
6	**Kriptografi.** Mengelola *key management* untuk memastikan kerahasiaan dan keaslian informasi dalam saluran komunikasi.	Pengaturan *key management*, terkait dengan pembuatan, pertukaran, penyimpanan, pengamanan, penggunaan, dan penggantian *key*.	Kriptografi (i)
7	**Keamanan Fisik dan Lingkungan**. Memberikan perlindungan terhadap fasilitas fisik yang berisi aset informasi.	a. Pengamanan area, b. Pengamanan peralatan.	Keamanan Fisik & Lingkungan (j)
8	**Keamanan Operasi**. Memastikan keamanan dalam pengoperasian fasilitas pemrosesan aset informasi.	a. Prosedur dan tanggung jawab operasional, b. Perencanaan dan penerimaan sistem, c. Perlindungan dari *malware,* d. Cadangan, e. *Logging* dan pemantauan, f. Kontrol perangkat lunak operasional, g. Manajemen kerentanan teknis, h. Pertimbangan audit sistem informasi.	Keamanan Operasional (k)
9	**Keamanan Komunikasi**. Mengendalikan informasi aset yang ditransmisikan melalui jaringan komunikasi beserta perangkat pendukungnya.	a. Pengelolaan keamanan jaringan, b. Keamanan dalam transfer informasi.	Keamanan Komunikasi (l)
10	**Akuisisi Sistem, Pengembangan dan Pemeliharaan**. Memastikan bahwa keamanan aset informasi merupakan bagian terintegrasi dengan sistem informasi, mencegah	a. Persyaratan keamanan sistem informasi, b. Keamanan dalam proses pengembangan dan dukungan, c. Data uji.	Keamanan dalam proses akuisisi, pengembangan, dan Pemeliharaan sistem informasi (m); Keamanan pembangunan dan

No	Domain	Elemen Kontrol	Aspek Pengendalian Keamanan SPBE (Pergub 33 Tahun 2023)
	kesalahan, kehilangan serta modifikasi oleh pihak yang tidak berwenang.		pengembangan aplikasi SPBE (e)
11	**Hubungan dengan Pihak Ketiga/Pemasok.** Memastikan perlindungan aset organisasi (informasi) yang dapat diakses oleh pihak ketiga/pemasok.	a. Keamanan informasi dalam hubungan pemasok, b. Manajemen pemberian layanan oleh pemasok.	Kebijakan terhadap pihak ketiga (n)
12	**Manajemen Insiden Keamanan Informasi**. Memastikan kejadian dan kelemahan keamanan informasi yang terkait dengan sistem informasi dikomunikasikan dengan baik sehingga tindakan perbaikan dapat dilakukan tepat waktu.	Manajemen dan penang anan insiden keamanan informasi	Penanganan Insiden Keamaman Informasi (m); (q)
13	**Keamanan Informasi dari Aspek Manajemen Kelangsungan Organisasi**. Memastikan ketersediaan fasilitas sistem informasi pada situasi darurat.	a. Kesinambungan keamanan informasi, b. Ketersediaan cadangan.	Kelangsungan bisnis atau layanan TIK atau *bussiness continuity* (p)
14	**Kepatuhan.** Menghindari pelanggaran terhadap hukum, undang-undang, peraturan, atau kontrak yang terkait dengan keamanan informasi.	a. Kepatuhan terhadap persyaratan hukum dan kontrak, b. Ulasan keamanan informasi.	Kepatuhan keamanan SPBE (s)

BAB II
RUANG LINGKUP SISTEM MANAJEMEN KEAMANAN INFORMASI

2.1 Pengendalian Kebijakan Keamanan Informasi

Pengendalian kebijakan keamanan informasi memberikan pedoman umum bagi unit terkait dalam mengelola dan menerapkan Sistem Manajemen Keamanan Informasi (SMKI), sehingga aset informasi dapat terlindungi. Pengamanan aset informasi dilaksanakan oleh seluruh unit kerja, pegawai (baik sebagai pengguna maupun pengelola TIK), serta pihak ketiga yang ikut terlibat dalam proses bisnis organisasi.

A. Kebijakan

1. Dokumen SMKI mengatur tanggung jawab keamanan informasi, meliputi:
   a. Kebutuhan dan Persyaratan keamanan informasi pihak-pihak yang berkepentingan terhadap keamanan informasi.
   b. Pelaksanaan pengamanan dan perlindungan aset informasi.
   c. Peningkatan pengetahuan, keterampilan dan kepedulian terhadap keamanan informasi pada seluruh unit perangkat daerah, pegawai, serta pihak ketiga.
   d. Penerapan manajemen risiko keamanan informasi yang mencakup kajian terhadap pemenuhan persyaratan dan kebutuhan keamanan informasi oleh pihak-pihak yang berkepentingan terhadap keamanan informasi.
   e. Pelaksanaan audit internal SMKI untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif sesuai dengan kebijakan dan standar yang telah ditetapkan.
   f. Evaluasi terhadap kepatuhan dan efektifitas penerapan SMKI serta melakukan tindak lanjut yang diperlukan
2. Dokumen SMKI wajib dijaga kemutakhiran dan efektifitas pelaksanaannya, serta terhindar dari segala jenis kerusakan dan akses oleh pihak yang tidak berwenang.
3. Dokumen SMKI disahkan sebagai dokumen resmi organisasi, dan dikomunikasikan serta disosialisasikan kepada seluruh pegawai maupun pihak ketiga.

B. Standar

1. Penyusunan dokumen pendukung kebijakan keamanan informasi wajib memuat:
   a) Tujuan dan ruang lingkup dokumen pendukung kebijakan dan keamanan informasi.
   b) Kerangka kerja pengendalian keamanan informasi.

c) Metodologi penilaian risiko.
d) Penjelasan mengenai standar, prosedur, dan kepatuhan termasuk persyaratan peraturan yang wajib dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran.

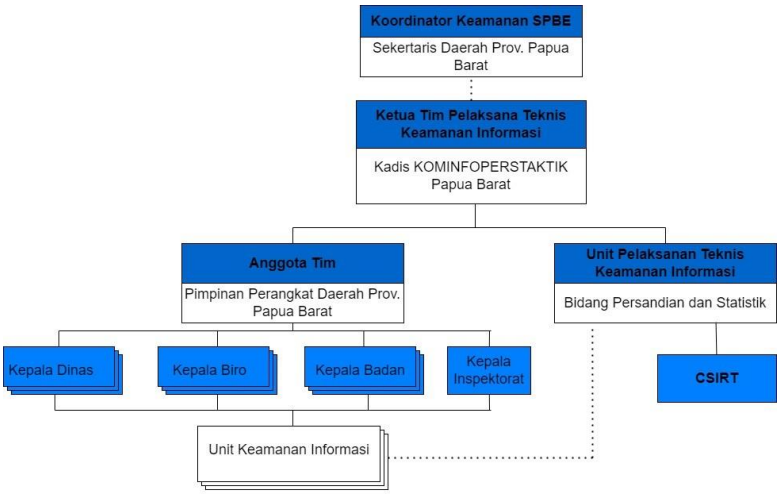
2. Standar catatan penerapan kebijakan dan standar SMKI mencakup:
   a. Memastikan terdokumentasinya catatan penerapan kebijakan dan standar SMKI sehingga kepatuhan dan efektivitas penerapan SMKI dapat diukur.
   b. Catatan penerapan Kebijakan dan Standar SMKI meliputi:
      1) Formulir-formulir sesuai prosedur operasional yang dijalankan;
      2) Catatan gangguan atau insiden keamanan informasi;
      3) Catatan dari sistem (*logs*);
      4) Catatan pengunjung di *secure areas;*
      5) Kontrak dan perjanjian layanan;
      6) Perjanjian kerahasiaan;
      7) Laporan audit.
3. Dokumen SMKI perlu dilakukan peninjauan dan disesuaikan dengan perkembangan organisasi minimal setahun sekali. Hasil peninjauan dokumen serta dokumen penunjang lainnya hendaknya didokumentasikan pada formulir kontrol revisi dokumen (*Formulir 01*).
4. Sosialisasi kebijakan dan standar SMKI, khususnya yang berkaitan langsung dengan pegawai serta pihak ketiga dilaksanakan sekurang-kurangnya sekali dalam setahun (*Formulir 02*).
5. Audit internal SMKI dilaksanakan minimal sekali dalam setahun
6. Persiapan, pelaksanaan, dan tindak lanjut audit internal SMKI harus terencana dan terdokumentasi (*Formulir 03*, 04, dan 05).
7. Rapat tinjauan manajemen berkenaan dengan evaluasi kepatuhan dan implementasi SMKI setidaknya mencakup evaluasi terhadap:
   a. Hasil audit internal SMKI.
   b. Pencapaian sasaran keamanan informasi, termasuk kinerja penanganan insiden keamanan informasi.
   c. Pencapaian persyaratan dan kebutuhan keamanan informasi baik dalam lingkup internal maupun pihak eksternal.
   d. Umpan balik dari pihak eksternal.
   e. Penerapan manajemen risiko SMKI.
   f. Kemungkinan untuk meningkatkan kinerja SMKI.

2.2 Pengendalian Organisasi Keamanan Informasi

Pengendalian organisasi keamanan informasi memberikan pedoman bagi organisasi terkait unit fungsional keamanan informasi yang akan bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkup Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat.

A. Kebijakan

1. Wewenang dan tanggung jawab keamanan informasi dipetakan dalam jabatan struktural dalam hal ini oleh Kepala Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat yang berperan sebagai Ketua Tim Pelaksana Teknis Keamanan Informasi (*Chief Information Security Officer "CISO"*) dibawah koordinasi Sekretaris Daerah Provinsi Papua Barat selaku koordinator keamanan SPBE (Pergub Provinsi Papua Barat nomor 33 Tahun 2023).
2. Pimpinan organisasi perangkat daerah dalam lingkup pemerintah Provinsi Papua Barat, meliputi para kepala dinas, kepala biro, kepala badan, serta kepala inspektorat perangkat daerah, bertindak sebagai anggota tim pelaksana teknis keamanan informasi dan bertanggang jawab terhadap pengelolaan aset informasi dalam lingkup kerja masing-masing dengan dengan membentuk unit keamanan informasi yang senantiasa berkoordinasi aktif dengan unit struktural maupun fungsional Dinas Komunikasi Informatika, Persandian dan Statistik Provinsi Papua Barat. Organisasi keamanan informasi Provinsi Papua Barat Sebagaimana ditampilkan pada Gambar 2.1.



Gambar 2.1 Organisasi Keamanan Informasi Provinsi Papua Barat

3. Tanggung jawab dan wewenang CISO dan unit keamanan informasi diuraikan dalam standar organisasi keamanan informasi.
4. Kesigapan penanganan insiden keamanan informasi perlu ditunjang dengan membentuk tim penanganan insiden keamanan siber (*Cyber Security Independent Resilient Team "CSIRT"*).
5. Pengangkatan CISO, anggota unit pelaksana teknis keamanan informasi dan CSIRT hendaknya sesuai dengan syarat standar kompetensi yang diperlukan.
6. Pengendalian terhadap keamanan informasi harus diaplikasikan pada seluruh fase pengelolaan proyek/pekerjaan.
7. Pengendalian terhadap komunikasi eksternal (*Mobile Device dan Teleworking*) dengan:
   a. Membangun kepedulian pengguna *mobile device dan teleworking* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan.
   b. Memastikan pengguna *mobile device* dan *teleworking* mengikuti prosedur penggunaan secara disiplin.
8. Seluruh insiden pelanggaran keamanan informasi harus dilaporkan, diinvestigasi dan didokumentasikan.

B. Standar

1. Kepala Dinas Komunikasi Informatika, Persandian dan Statistik selaku CISO yang dalam tugas teknisnya terkait manajemen keamanan informasi dilaksanakan oleh Bidang Persandian, bertanggung jawab untuk:
   a. Mengkoordinasikan perumusan dan penyempurnaan SMKI.
   b. Memelihara dan mengendalikan penerapan SMKI di seluruh area yang menjadi tujuan sasaran pengendalian.
   c. Menyusun target keamanan informasi serta rencana kerja tahunan.
   d. Memastikan efektivitas dan konsistensi penerapan SMKI serta mengukur kinerja keseluruhan dengan melakukan audit internal mengacu pada standar audit Keamanan Informasi (KAMI) yang diterbitkan oleh BSSN.
2. Unit keamanan informasi pada setiap satuan kerja, bertanggung jawab untuk:
   a. Mengendalikan penerapan SMKI dalam lingkup satuan kerja masing-masing.
   b. Mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan.
   c. Melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi kerahasiaan untuk

menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
   d. Mengidentifikasi dan menjalin kerjasama dengan pihak-pihak eksternal yang terkait dengan keamanan informasi.
   e. Menjalin kerjasama dengan komunitas keamanan informasi melalui pelatihan, seminar, atau forum lain yang relevan.
   f. Unit keamanan informasi tidak bertanggung jawab atas kerugian atau kerusakan data maupun perangkat lunak milik pihak ketiga yang diakibatkan dari upaya untuk melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi.
3. Syarat anggota unit pelaksana teknis keamanan informasi dan CSIRT minimal memiliki sertifikasi kompetensi keamanan infrastuktur TIK.
4. Pelaporan dan investigasi insiden pelanggaran keamanan informasi didokumentasikan menggunakan formulir kontrol insiden keamanan informasi (Formulir 06 dan Formulir 07).
5. Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:
   a. Definisi dari informasi yang akan dilindungi.
   b. Durasi yang diharapkan dari sebuah perjanjian kerahasiaan.
   c. Tanggung jawab dan tindakan penanda tangan untuk menghindari pengungkapan informasi secara tidak sah.
   d. Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual.
   e. Izin dan hak-hak menggunakan informasi rahasia.
   f. Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia.
   g. Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi.
   h. Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri.
   i. Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian.
   j. Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian kerahasiaan.

2.3 Pengendalian Sumber Daya Manusia

Pengendalian sumber daya manusia bertujuan untuk memastikan bahwa pengguna aset informasi baik itu pegawai dan pihak ketiga dalam lingkup Pemerintah Provinsi Papua Barat memahami tugas dan tanggung jawab masing-masing terkait keamanan informasi, sadar akan potensi ancaman

keamanan informasi, serta mengetahui proses terkait keamanan informasi sebelum, selama, dan setelah bertugas.

A. Kebijakan

1. Pegawai bertanggung jawab untuk menjaga keamanan informasi pada satuan kerja masing-masing.
2. Pihak ketiga wajib menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi.
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi harus didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan.
4. Satuan kerja melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan ketentuan yang berlaku.
5. Seluruh pegawai wajib mendapatkan pendidikan, pelatihan dan atau sosialisasi keamanan sistem informasi secara berkala sesuai tingkat tanggung jawabnya.
6. Pihak ketiga diberikan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi jika diperlukan.
7. Seluruh pegawai dan pihak ketiga yang yang melanggar SMKI di lingkungan pemerintah Provinsi Papua Barat akan diberikan sanksi atau tindakan disiplin sesuai dengan ketentuan yang berlaku.
8. Kepatuhan pegawai terhadap SMKI di lingkungan pemerintah Provinsi Papua Barat wajib diawasi oleh atasan atau unit terkait pada satuan kerja masing-masing.
9. Pegawai yang berhenti bekerja atau mutasi wajib mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.
10. Pihak ketiga yang habis masa kontrak kerjanya wajib mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di lingkungan pemerintah Provinsi Papua Barat.
11. Satuan kerja wajib menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan dan/atau menjalani proses hukum terkait dengan dugaan pelanggaran SMKI di lingkungan pemerintah Provinsi Papua Barat.
12. Unit terkait wajib mencabut hak akses terhadap akses informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja.

B. Standar

1. Peran dan tanggung jawab pegawai terhadap keamanan informasi menjadi bagian dari penjabaran tugas dan fungsinya, terkhusus bagi yang memiliki akses terhadap aset informasi.

2. Pimpinan dari pegawai berkeahlian khusus atau yang berada pada posisi kunci, harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara jika pegawai yang bersangkutan dimutasi/berhenti.
3. Pemeriksaan latar belakang calon pegawai dan pihak ketiga wajib memperhitungkan privasi, perlindungan data pribadi dan pekerjaan, meliputi: (Formulir 08)
    a. Ketersediaan referensi, baik referensi hubungan kerja maupun pribadi.
    b. Pemeriksaan kelengkapan dan ketepatan riwayat hidup pemohon.
    c. Konfirmasi kualifikasi akademik dan profesional yang diklaim.
    d. Pemeriksaan identitas (kartu penduduk/paspor serta dokumen identitas lainnya).
    e. Pemeriksaan lebih rinci, seperti pemeriksaan kredit atau pemeriksaan catatan kriminal.
4. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:
    a. Bertindak sesuai dengan kebijakan dan standar organisasi keamanan informasi.
    b. Melindungi aset informasi dari akses yang tidak sah, penyingkapan, modifikasi, dan kerusakan atau gangguan.
    c. Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya.
    d. Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan kebijakan dan standar SMKI.

2.4 Pengelolaan Aset

Tata kelola pengelolaan aset informasi bertujuan untuk melindungi dan menjamin seluruh aset informasi organisasi, termasuk data, perangkat lunak, perangkat keras, infrastruktur serta informasi lain dari akses, penggunaan, pengungkapan, perubahan, dan penyalahgunaan yang tidak sah. Tujuan klasifikasi aset informasi untuk melindungi informasi dari akses yang tidak sah serta memastikan bahwa informasi hanya diakses oleh pihak yang berwenang.

A. Kebijakan

Pemilik aset informasi menetapkan kebijakan pengelolaan aset informasi yang terdiri atas:

1. Aturan penggunaan aset informasi.
2. Prosedur Tanggung Jawab terhadap terhadap pengelolaan aset informasi
    a. Mengidentifikasi dan mendokumentasikan semua aset informasi dalam daftar inventaris aset.

b. Mengklasifikasikan dan melindungi aset informasi dengan tepat sesuai dengan tingkat kerahasiaannya.
c. Memonitoring serta mengecek aktivitas aset secara berkala untuk memastikan penggunaan yang sah, mencegah penyalahgunaan, dan mendeteksi potensi pelanggaran keamanan.
d. Pihak-pihak (pegawai dan pihak ketiga) yang telah menyelesaikan masa kerja, mutasi, atau pemutusan hubungan kerja dan lainnya diwajibkan untuk mengembalikan semua aset informasi yang digunakan.

3. Pemilik aset informasi menetapkan prosedur mengklasifikasikan aset Informasi (mungkin yang dimaksud pengklasifikasian aset informasi):
   a. Pemilik Aset mengklasifikasi informasi ke dalam tiga tingkat kerahasiaan yaitu sangat rahasia, rahasia dan terbatas.
   b. Dalam mengklasifikasikan aset informasi berdasarkan kerahasiaan harus sesuai dengan ketentuan yang diatur dalam peraturan mengenai tata kelola TIK di lingkup Pemerintah Provinsi Papua Barat.
   c. Pemberian label klasifikasi aset informasi dilakukan secara konsisten terhadap seluruh aset informasi.
   d. Pemilik aset informasi menetapkan dan menerapkan prosedur penanganan yang sesuai dengan klasifikasi aset informasi. Prosedur ini harus mencakup mekanisme pengaksesan, penyimpanan, penggunaan, dan pemusnahan.
4. Pemilik aset informasi menyediakan prosedur media Penyimpanan Informasi
   a. Pemilik aset informasi bertanggung jawab untuk mengelola media penyimpanan informasi untuk mencegah pengungkapan, modifikasi, pemindahan, dan penghapusan informasi secara tidak sah. Hal ini termasuk:
      1) Mengklasifikasikan media penyimpanan informasi berdasarkan tingkat kerahasiaannya;
      2) Menerapkan kontrol akses fisik dan logis untuk media penyimpanan informasi;
      3) Menyimpan media penyimpanan informasi di tempat yang aman;
      4) Melakukan *backup* media penyimpanan informasi secara teratur;
      5) Memusnahkan media penyimpanan informasi yang tidak lagi digunakan dengan aman. Pemilik aset informasi mengelola media penyimpanan informasi untuk mencegah pengungkapan, modifikasi, pemindahan, dan penghapusan informasi secara tidak sah.

b. Media yang memuat informasi harus dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah pada saat dipindahkan. Hal ini termasuk:
   1) Menggunakan media penyimpanan informasi yang aman dan terenkripsi;
   2) Membatasi akses ke media penyimpanan informasi hanya kepada personel yang berwenang;
   3) Membuat catatan tentang pemindahan media penyimpanan informasi.
c. Media yang tidak lagi dibutuhkan harus dihancurkan dengan aman menggunakan prosedur yang berlaku serta didokumentasikan. Hal ini termasuk:
   1) Memusnahkan media penyimpanan informasi secara fisik;
   2) Menghapus data dari media penyimpanan informasi secara elektronik;
   3) Mendokumentasikan proses pemusnahan media penyimpanan informasi.

B. Standar

1. Aturan penggunaan aset informasi terdiri dari.
   a. Mengakses aset informasi.
      1) Pihak-pihak yang memerlukan akses ke informasi harus mengajukan permohonan tertulis kepada pemilik informasi; (Formulir 09)
      2) Pemilik informasi wajib memastikan bahwa pihak-pihak yang memerlukan akses telah menandatangani perjanjian kerahasiaan sesuai ketentuan yang berlaku; (Formulir 09)
      3) Persetujuan diberikan oleh pemilik informasi dan disampaikan kepada pengguna sebagai pemberitahuan, serta diikuti dengan pemberian hak akses kepada pengguna terhadap informasi yang diminta.
   b. Cara menyimpan aset informasi. (Formulir 10)
      1) Aset informasi disimpan ditempat yang aman dan terlindungi untuk mencegah akses yang tidak sah, pencurian, dan kerusakan;
      2) Informasi dalam bentuk fisik disimpan dalam penyimpanan yang aman, terjaga, dan terlindungi;
      3) Informasi dalam bentuk digital harus dilindungi dengan enkripsi, kata sandi yang kuat, dan disimpan di server yang aman atau layanan penyimpanan awan (*cloud*) yang terpercaya;
      4) Untuk informasi dalam bentuk digital, prosedur pencadangan data harus diterapkan secara berkala untuk memastikan

bahwa aset informasi dapat dipulihkan jika terjadi kehilangan atau kerusakan.

c. Cara menggunakan dan membagikan aset informasi. (Formulir 11)
    1) Memberikan akses informasi hanya jika semua persyaratan telah dipenuhi;
    2) Pengguna aset informasi hanya menggunakan akses sesuai kebutuhan dan izin yang diberikan;
    3) Melakukan peninjauan berkala terhadap hak akses informasi, termasuk memeriksa tingkatan akses yang diberikan;
    4) Setiap pengembalian aset informasi harus dicatat dan didokumentasikan untuk tujuan audit dan verifikasi. (formulir 12)

d. Pemusnahan aset informasi. (*Formulir 13)*
    1) Mencakup dokumen fisik, dokumen digital, serta perangkat keras;
    2) Pemusnahan aset informasi harus mendapatkan persetujuan dari pihak yang berwenang dan diawasi oleh individu atau tim yang ditunjuk untuk memastikan bahwa proses dilakukan sesuai dengan kebijakan yang berlaku;
    3) Aset informasi harus dimusnahkan menggunakan metode yang memastikan bahwa data tidak dapat dipulihkan kembali;
    4) Setiap proses pemusnahan aset informasi harus dibuatkan laporan pemusnahan dan didokumentasikan dengan baik. Dokumentasi ini mencakup jenis aset yang dimusnahkan, metode pemusnahan, tanggal dan waktu pemusnahan, serta pihak yang bertanggung jawab atas pemusnahan tersebut.

2. Untuk menjaga kerahasiaan (*confidential)*, integritas (*integrity)* dan ketersediaan (*availability)* informasi, pemilik aset informasi menetapkan pihak-pihak yang berhak mengaksesnya. Hal ini termasuk:
    a. Mengidentifikasi dan mengelompokkan pengguna berdasarkan kebutuhan akses mereka. Pihak-pihak yang mendapatkan akses informasi adalah yang memiliki peran dan tanggung jawab yang relevan dengan informasi tersebut.
    b. Mengimplementasikan kontrol akses yang sesuai, seperti sistem otentikasi dan otorisasi yang kuat.
    c. Melakukan audit secara berkala untuk memastikan bahwa akses yang diberikan tetap relevan dan sesuai dengan kebutuhan tugas. (Formulir 14)
3. Klasifikasi aset informasi yang terdiri atas Sangat Rahasia, Rahasia, dan Terbatas memiliki defenisi sebagai berkut: **Sangat Rahasia** yaitu

Informasi yang hanya boleh diakses oleh personel yang memiliki kewenangan khusus. Akses terhadap informasi ini sangat terbatas dan hanya diberikan kepada individu yang benar-benar memiliki otorisasi untuk mengaksesnya. **Rahasia** yaitu Informasi yang hanya dapat diakses dan diberikan oleh personel, individu, ataupun organisasi yang membutuhkan dalam menjalankan tugasnya. Informasi ini tersedia bagi mereka yang peran dan tanggung jawabnya memerlukan akses tersebut. **Terbatas** yaitu Informasi yang dapat diakses oleh personel yang bekerja di unit terkait.

2.5 Pengendalian Akses

Pengendalian akses bertujuan untuk memastikan aset informasi, baik akses fisik maupun non-fisik, terlindungi melalui kontrol otorisasi akses pengguna. Hal ini untuk mencegah akses yang dimiliki Pemerintah Provinsi Papua Barat diakses oleh pihak-pihak yang tidak berkepentingan. Akses kontrol meliputi: persyaratan bisnis dalam pengendalian akses, pengelolaan hak akses pengguna, tanggung jawab pengguna, pengendalian akses jaringan, pemisahan dalam jaringan dan perangkat bergerak (*mobile*) dan *telecommuting.*

A. Kebijakan

Pemilik aset informasi menetapkan kebijakan pengendalian terhadap akses aset informasi yang terdiri atas:

1. Prosedur penyusunan dan perlindungan terhadap insiden yang mengganggu atau mengancam berjalannya sistem.
2. Prosedur perjanjian kerahasiaan dan pematuhan kebijakan serta prosedur yang untuk (yang atau untuk) menjaga keamanan dan integritas informasi.
3. Prosedur Pengelolaan Hak Akses Pengguna.
4. Prosedur Pengguna bertanggung jawab terhadap penggunaan akses infomasi.
5. Prosedur pengendalian akses informasi aplikasi.
6. Prosedur pengendalian akses jaringan.

B. Standar

1. Pengendalian akses meliputi penyusunan prosedur perlindungan terhadap aset informasi berdasarkan persyaratan keamanan.
2. Pengelolaan hak akses terdiri dari:
    a. Pemilik aset bertanggung jawab:
        1) Menyediakan prosedur pendaftaran pengguna, serta mekanisma pemberian hak akses terhadap aset informasi; (Formulir 09)
        2) Memastikan penggunaan izin akses diperoleh dari pemilik aset informasi;

3) Memastikan bahwa hak akses yang diberikan telah sesuai dengan prosedur;
4) Akses terhadap suatu informasi diberikan setelah pemohon mengajukan permohonan kepada pemilik aset informasi secara tertulis; (*Formulir 14 dan Fomulir 15)*
5) Memastikan pengguna menandatangani pernyataan bahwa merekamemahami aturan mengenai hak akses;
6) Memastikan pemberian aset informasi dilakukan hanya setelah proses otorisasi telah dilakukan dengan mempertimbangkan nilai, sensitivitas informasi, dan tingkat risiko terhadap organisasi;
7) Memastikan akses informasi hanya diberikan berdasarkan kebutuhan.

b. Prosedur otentikasi kata sandi (*password*):
1) Tampilan karakter kata sandi diganti dengan simbol tertentu pada saat masuk (*login)*;
2) Kata sandi sementara harus diganti pada saat penggunaan pertama kali;
3) Panjang minimal karakter kata sandi adalah 8 (delapan) karakter;
4) Jumlah percobaan ulang untuk *login* maksimal 3(tiga) kali;
5) Kriteria kata sandi yaitu mudah diingat, tidak mudah ditebak, menggunakan kombinasi angka, huruf besar, huruf kecil, dan tanda baca;
6) Sistem tidak boleh memberikan detail otentikasi sukses dilakukan;
7) Validasi dilakukan hanya setelah semua informasi *login* (identitas pengguna dan kata sandi) telah dimasukkan.

3. Peninjauan hak akses pengguna perlu memperhatikan:
a. Dilakukan secara berkala setiap 3 (tiga) bulan sekali dan atau setiap ada perubahan terhadap pengguna seperti promosi, demosi, dan mutasi.
b. Otorisasi untuk hak akses khusus harus ditinjau sekali setiap 2 (dua) bulan.
c. Pemilik aset informasi memantau penggunaan hak akses khusus untuk memastikan tidak adanya akses tanpa izin.
d. Perubahan pada hak akses khusus perlu didokumentasikan dalam riwayat akses (*log*) untuk kemudian dilakukan peninjauan.

4. Pengendalian akses informasi aplikasi meliputi:
a. Akses ke informasi dan sistem aplikasi dibatasi sesuai dengan kebijakan pengendalian hak akses yang telah ditentukan.
b. Pembatasan akses informasi perlu dilakukan berdasarkan kebutuhan bisnis.

c. Pembatasan akses perlu dilakukan untuk seluruh aplikasi dan sistem informasi, mencakup hak membaca (*read*), menulis (*write*), menghapus (*delete*) dan menjalankan (*execute*).
d. Menjaga keamanan aset informasi dengan menggunakan perangkat lunak pengaman (*anti malware*).
e. Menggunakan perangkat lunak berlisensi.
f. Akses aset informasi untuk pengguna yang melaksanakan pekerjaan secara *telecommuting* atau aktivitas pekerjaan diluar kantor menggunakan VPN layanan yang telah disediakan.
g. Memastikan bahwa lalu lintas data dalam jaringan yang digunakan aman (*secure*) sesuai dengan standar keamanan.

5. Pengendalian akses jaringan
   a. Menerapkan prosedur otorisasi pemberian akses ke layanan jaringan meliputi prosedur pengajuan, verifikasi, dan pengecekan kelayakan.
   b. Menerapkan teknik autentikasi akses dari koneksi eksternal, seperti teknik kriptografi, *token hardware*, dan *dial-back*.
   c. Melakukan penghentian atau isolasi layanan jaringan pada area yang mengalami gangguan keamanan informasi.
6. Identifikasi, Otentikasi, dan Otorisasi:
   a. Identifikasi
      1) Setiap pengguna harus memiliki identitas unik seperti *username* atau ID pengguna untuk membedakan satu pengguna dari yang lain;
      2) Proses pendaftaran yang mengharuskan pengguna memberikan informasi yang diperlukan untuk membuat identitas unik;
      3) Memelihara dan memperbarui informasi identitas pengguna sesuai dengan perubahan status atau peran pengguna dalam organisasi.
   b. Otentikasi
      1) Kata sandi harus kompleks, dengan kombinasi huruf besar dan kecil, angka, dan simbol. Kata sandi juga harus diubah secara berkala;
      2) Selain kata sandi, pengguna harus melaksanakan *Multi Factor Autentikasi* (*MFA*) seperti kode yang dikirimkan ke ponsel atau perangkat autentikasi lainnya;
      3) Menggunakan sidik jari, pengenalan wajah, atau iris mata sebagai metode tambahan untuk memastikan identitas pengguna.
   c. Otorisasi
      1) Menentukan hak akses berdasarkan peran pengguna dalam organisasi. Setiap peran memiliki akses yang sesuai dengan tanggung jawabnya;

2) Menentukan hak akses berdasarkan atribut pengguna seperti departemen, lokasi, atau proyek yang sedang dikerjakan;
3) Memberikan akses minimal yang diperlukan pengguna untuk melakukan tugasnya;
4) Secara rutin memantau dan mengaudit akses pengguna untuk memastikan kepatuhan terhadap kebijakan keamanan;
5) Melakukan peninjauan berkala terhadap hak akses dan mencabut akses yang tidak lagi diperlukan atau tidak relevan.

7. Prosedur sistem penanganan aset pada saat terjadi situasi darurat. Prosedur tersebut meliputi:
   a. Menentukan aset informasi yang paling kritis untuk operasional organisasi.
   b. Melakukan penilaian risiko untuk mengidentifikasi potensi ancaman dan dampak dari situasi darurat.
   c. Mendokumentasikan rencana pemulihan yang komprehensif.
   d. Membentuk tim tanggap darurat yang terdiri dari anggota dari berbagai departemen, termasuk TI, keamanan dan manajemen.
   e. Melakukan simulasi darurat secara berkala untuk menguji dan memastikan kesiapan organisasi dalam menghadapi situasi darurat.
   f. Membuat rencana evakuasi untuk memastikan keselamatan aset informasi.
   g. Memastikan bahwa semua data penting di *backup* secara berkala dan disimpan di lokasi yang aman.
   h. Membuat prosedur pemulihan data yang cepat dan efektif untuk mengembalikan data yang hilang atau rusak selama situasi darurat.
   i. Menyiapkan daftar kontak darurat yang mencakup informasi kontak semua tim tanggap darurat (IT), karyawan dan pihak eksternal yang relevan.
   j. Memastikan adanya sistem komunikasi alternatif seperti telepon satelit atau radio dua arah jika sistem komunikasi utama terganggu.
   k. Membuat rencana pemulihan infrastruktur TI yang mencakup langkah-langkah perbaikan.
   l. Memastikan semua prosedur, kontak dan rencana terdokumentasi dengan baik dan mudah diakses.
8. Menyediakan perangkat lunak terintegrasi yang dapat memonitoring dan mengontrol aktivitas pengendalian aset informasi, meliputi:
   a. Menyediakan *dashboard* yang memberikan gambaran umum tentang aktivitas pengelolaan aset. Misalnya mencatat secara

rinci setiap aktivitas yang terjadi terkait dengan aset informasi, termasuk siapa yang mengakses, kapan dan apa yang dilakukan.
   b. Memungkinkan administrator untuk mengatur dan mengelola hak akses pengguna dengan cara yang fleksibel, seperti menentukan peran dan level akses.
   c. Memberikan notifikasi secara *real-time* atau peringatan ketika terdeteksi aktivitas mencurigakan atau pelanggaran kebijakan keamanan.
   d. Memungkinkan untuk mengelola kejadian keamanan dengan cepat dan efisien, termasuk respon dan mitigasi terhadap insiden yang terjadi.
   e. Memantau kinerja sistem dan jaringan terkait dengan pengelolaan aset, termasuk penggunaan sumber daya dan kinerja aplikasi. Hal ini untuk memastikan semua sistem benar-benar sesuai dengan kebijakan kontrol akses dan dilindungi dengan prosedur yang aman, yaitu melakukan audit berkala, simulasi keamanan, memantau aktivitas sistem secara *real-time*, dan monitoring log-aktivitas untuk mengidentifikasi anomali .
9. Prosedur pengelolaan hak akses pengguna yang mencakup proses:
   a. Menentukan individu yang berhak mendapatkan izin akses terhadap aset informasi.
   b. Memberikan izin akses berdasarkan level dan peran masing-masing .
   c. Mengklasifikasikan pengguna yang dapat mengakses sumber daya.
   d. Memeriksa dan memvalidasi atribut terkait seperti identitas, peran, dan hal-hal lain yang relevan.
   e. Memberikan perlindungan terhadap aset informasi agar tidak diakses oleh pihak yang tidak berkepentingan.
   f. Memastikan bahwa pengguna yang mengakses aset informasi adalah orang yang tepat, pada waktu yang tepat, dan untuk tujuan yang tepat.
   g. Menghapus atau memperbarui hak akses terhadap aset informasi saat terjadi pemberhentian pegawai, pergantian, atau perubahan posisi dalam departemen.
   h. Memastikan pengendalian kewenangan pengguna dalam hak akses seperti membaca, menulis, memperbarui, dan menghapus.
10. Tanggung jawab pengguna terhadap penggunaan akses infomasi
   a. Menjaga kerahasiaan dalam menggunakan akun dan kata sandi yang menyangkut akun surat elektronik maupun akun lain melalui akses intranet dan internet di lingkup Pemerintah Provinsi Papua Barat.

b. Memastikan perangkat pengelola informasi mendapat perlindungan pada saat digunakan.
c. Menjaga akun beserta informasinya agar tidak disalahgunakan.
d. Saat menggunakan komputer publik, hindari mengakses akun pribadi yang melalui akses publik.
e. Melaporkan kepada administrator IT jika mencurigai bahwa akun yang digunakan telah diretas atau disalahgunakan.

11. Informasi terkait prosedur pengendalian layanan akses jaringan meliputi:
    a. Pengguna hanya diperbolehkan untuk mengakses layanan yang diizinkan sesuai area kerjanya. Kebijakan dan prosedur penggunaan jaringan dan layanan jaringan mencakup hal berikut:
        1) Jaringan dan layanan jaringan yang dapat diakses;
        2) Otorisasi untuk memastikan jaringan; dan layanan jaringan yang tersedia hanya dapat diakses oleh pengguna yang berwenang;
        3) Mengendalikan akses ke jaringan dan layanan jaringan;
        4) Metode yang disetujui untuk mengakses jaringan dan layanan jaringan;
        5) Selaras dengan kebijakan dan prosedur pengendalian bisnis organisasi.
    b. Pengelolaan aset informasi dalam jaringan diklasifikasi berdasarkan kelompok layanan aplikasi, informasi dan pengguna.

2.6 Kriptografi

Penerapan kriptografi berkaitan dengan proses pengamanan aset informasi untuk melindungi keaslian informasi dalam saluran komunikasi.

A. Kebijakan

Pemilik aset informasi menetapkan kebijakan penerapan kirptografi pengendalian terhadap akses aset informasi yang terdiri atas:

1. Penggunaan teknologi kriptografi dalam melindungi aset informasi organisasi.
2. Sistem kriptografi melindungi aset informasi yang bersifat rahasia.
3. Kebijakan penerapan kriptografi menggunakan prinsip enkripsi dan deskripsi.

B. Standar

1. Penerapan Kriptografi.
    a. Data dan informasi yang menerapkan kriptografi terdiri atas:
        1) Klasifikasi aset informasi yang bersifat rahasia;

2) Perlindungan aset informasi berupa *password*, kartu akses *login*, atau biometrik seperti sidik jari, retina, telapak tangan dan tanda tangan digital.

b. Pengendalian akses dengan membatasi penggunaan sistem informasi hanya kepada pengguna yang berwenang.
c. Menjamin koneksi internet atau jaringan *ad-hoc* yang aman antara sistem dan perangkat TIK.
d. Mengaktifkan fitur verifikasi, otentikasi, identifikasi dan validasi untuk menjamin hanya pengguna yang memiliki hak akses yang bisa masuk ke sistem.
e. Menjamin konsistensi, akurasi, serta kepercayaan terhadap data setiap waktu.
f. Membentuk mekanisme pengelolaan kunci kriptografi yang mengatur penerbitan, penyebaran, pembatalan keabsahan, penghapusan, dan penerbitan kembali.
g. Meninjau secara berkala kontrol kriptografi untuk memastikan aset informasi benar-benar aman.

2. Penerapan *key management* meliputi:
   a. Pembuatan, pertukaran, penyimpanan, pengamanan, penggunaan, dan penggantian *key*.
   b. Penerapan *key management* meliputi desain protokol kriptografi, *key server*, prosedur pengguna, dan protokol lainnya yang relevan.
   c. Penggunaan *public key* perlu mempertimbangkan proses otentikasi yang dapat dilakukan dengan menggunakan *public key certificates* yang dikeluarkan otoritas khusus yang telah dipercaya.
   d. Pemilik aset informasi perlu membuatkan pedoman khusus dalam enkripsi dan *key management.*

2.7 Keamanan Fisik dan Lingkungan

Tujuan dari pelaksanaan aspek ini adalah untuk:
1. Mencegah terjadinya akses fisik secara ilegal terhadap aset informasi pada organisasi.
2. Mencegah terjadinya kehilangan, kerusakan, pencurian, serta gangguan terhadap aset informasi pada organisasi.

A. Kebijakan

Pemilik aset informasi menetapkan kebijakan keamanan fisik dan lingkungan terdiri atas:
1. Pengamanan Area
   a. Penyimpanan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai.

b. Akses ke pusat aset informasi yang memiliki klasifikasi rahasia harus dibatasi dan hanya diberikan kepada pegawai yang diberi akses.
c. Pihak lain yang memasuki pusat aset informasi, harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan.
d. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi rahasia wajib dilindungi secara memadai.
e. Menyusun SOP pengamanan area.

2. Pengamanan Peralatan
a. Perangkat pengolah informasi dan perangkat pendukung wajib ditempatkan di lokasi yang terlindung dan diletakkan pada area aman dari akses oleh pihak yang tidak berwenang.
b. Penggunaan perangkat yang dibawa ke luar dari lingkungan organisasi wajib disetujui oleh Pejabat yang berwenang dengan pengawasan khusus.
c. Melakukan pengawasan untuk mendeteksi kondisi lingkungan, seperti suhu dan kelembaban, yang bisa mempengaruhi berfungsinya fasilitas pengolah informasi.
d. Menyediakan perangkat penangkal petir pada bangunan yang dilewati jalur komunikasi dan tenaga listrik.
e. Kabel sumber daya listrik dan kabel telekomunikasi yang mengalirkan informasi wajib dilindungi dari kerusakan dan penyadapan.
f. Perangkat pengolah informasi wajib dipelihara secara berkala untuk menjamin ketersediaan, keutuhan dan fungsinya.
g. Perangkat pengolah informasi yang sudah tidak digunakan lagi, wajib disanitasi sebelum digunakan kembali.
h. Perangkat pengolah informasi yang sensitif, yang tidak digunakan kembali dapat dimusnahkan melalui prosedur pemusnahan.

B. Standar

1. Pengamanan Area
a. Pengamanan area terhadap aset informasi dilengkapi dengan pintu elektronik, sistem pemadam kebakaran, alarm bahaya, kamera pengawas, perangkat pemutus aliran listrik serta perangkat lain yang mendukung;
b. Akses ke dalam area harus dibatasi, hanya untuk personil yang berkepentingan;
c. Pintu darurat perlu dilengkapi dengan sistem peringatan(*alarm*), selalu dimonitor dengan baik, dan diuji untuk memastikan berfungsi sebagaimana mestinya;

d. Sistem untuk mendeteksi adanya usaha akses tanpa izin perlu dipasang pada area keamanan khusus apabila diperlukan;
e. Fasilitas pemrosesan informasi organisasi harus terpisah secara fisik dari area kerja pihak ketiga.

2. Pengamanan Peralatan
   a. Pengunjung yang datang ke area kerja organisasi harus dicatat tanggal danwaktu masuk maupun keluarnya. (*Formulir 16)*
   b. Pengunjung harus didampingi kecuali telah mendapatkan izin akses.
   c. Pengunjung perlu diberi informasi mengenai syarat keamanan area, beserta prosedur dalam keadaan darurat.
   d. Akses masuk ke dalam area tempat pemrosesan atau penyimpanan informasi sensitif harus dikendalikan melalui proses otorisasi.
   e. Semua pengguna baik internal maupun eksternal wajib mengenakan *ID Card* ketika masuk ke dalam area peralatan.
   f. Pihak ketiga yang masuk ke area khusus dipastikan terpantau dengan baik.
   g. Hak akses ke area tertutup harus selalu ditinjau secara rutin.
3. Pengamanan Kantor, Ruang Kerja, dan Fasilitas Organisasi:
   a. Menerapkan standar kesehatan dan keamanan berdasarkan regulasi yang berlaku.
   b. Penempatan fasilitas penting organisasi yang digunakan untuk aktivitas pemrosesan dan penyimpanan informasi sensitif, sebaiknya tidak diberikan tanda khusus agar tidak mudah teridentifikasi oleh masyarakat umum.
4. Perlindungan terhadap ancaman eksternal dan ancaman lingkungan:
   a. Material yang berpotensi menimbulkan bahaya dan mudah terbakar harus di simpan di tempat yang aman dan terpisah dari ruang aktivitas kerja.
   b. Media cadangan *(backup)* harus disimpan di tempat aman dan terpisah untuk menghindari kerusakan apabila terjadi bencana di *main site*.
   c. Peralatan pemadam kebakaran harus selalu tersedia dan ditempatkan dengan baik.
   d. Memastikan area khusus memiliki detektor api dan asap serta pipa pembuangan air.
   e. *Data Center* dan area sensitif yang berisi peralatan komputer penting harus dilengkapi dengan perangkat deteksi api dan sistem alarm otomatis serta berada pada lokasi yang lebih tinggi.
   f. Perangkat deteksi api dan sistem pemadaman harus diperiksa secara berkala paling sedikit satu kali setiap tahun.
   g. Menerapkan larangan merokok serta membawa makanan dan minuman dalam area khusus.

5. Bekerja di area keamanan khusus:
   a. Segala aktivitas pekerjaan yang dilakukan di area tertutup dipastikan diawasi dengan baik dan seksama.
   b. Pintu masuk dan lokasi kunci pada area yang rawan dilengkapi dengan kamera pengawas.
   c. Area keamanan khusus harus selalu terkunci dan secara rutin dilakukan pengecekan.
   d. Segala peralatan perekam (*audio, video*, foto) tidak boleh dibawa masuk ke dalam area keamanan khusus.
   e. Dilarang merokok serta membawa makanan dan minuman di dalam area khusus.
6. Sarana Pendukung
   a. Generator harus terpasang untuk mendukung penyediaan listrik *Data Center*.
   b. Sumber Daya Listrik harus didukung oleh baterai cadangan atau *UPS* (*Uninterrupted Power Supply*), dan harus mampu untuk mendukung kapasitas untuk periode sekurang-kurangnya 30 (tiga puluh) menit pada saat terjadi pemadaman Listrik.
   c. Ruang generator dan *UPS* harus aman dan terkunci. Kunci harus disimpan dan hanya dapat diberikan kepada petugas yang ditunjuk.
   d. Ruang generator dan *UPS* harus mempunyai ventilasi yang memadai dan dilengkapi dengan sistem deteksi dan perlindungan api.
7. Pengamanan Pengkabelan
   a. Kabel listrik dan telekomunikasi yang digunakan untuk fasilitas pemrosesan informasi harus dipasang secara aman sedemikian(mungkin sebaiknya dihapus saja) sehingga dapat terlindungi dengan baik.
   b. Pelabelan kabel listrik dan telekomunikasi untuk mempermudah penanganan apabila terjadi masalah dan menghindari kesalahan.
   c. Instalasi kabel dan jalurnya harus didokumentasikan dengan baik.
   d. Sistem kritikal perlu perlindungan tambahan sebagai berikut:
      1) Penggunaan pelindung kabel dan kotak atau ruangan terkunci untuk melindungi kabel, terutama pada titik terminasi atau pemeriksaan;
      2) Penggunaan *routing* maupun media transmisi alternatif;
      3) Penggunaan pelindung elektromagnetik;
      4) Pemeriksaan teknis secara fisik untuk memastikan tidak ada peralatan yang tidak terhubung ke sistem komunikasi.
8. Pemeliharaan peralatan
   a. Melakukan pemeliharaan peralatan secara rutin sesuai

spesifikasi dan rekomendasi vendor.
b. Aktivitas pemeliharaan hanya boleh dilakukan oleh personil yang memiliki izin.
c. Setiap dugaan dan kerusakan yang benar-benar terjadi serta perbaikan yang bersifat korektif dan preventif harus didokumentasikan dengan baik.
d. Setiap pemeliharaan perlu mempertimbangkan informasi yang terkandung dalam peralatan tersebut.
e. Seluruh persyaratan yang diminta oleh pihak asuransi harus dipatuhi.

9. Pemindahan peralatan:
   a. Semua personel baik internal maupun eksternal yang diizinkan membawa keluar aset milik organisasi harus teridentifikasi.
   b. Aset yang dibawa keluar harus dibatasi dengan jelas waktu pengembaliannya serta didokumentasikan dengan baik. (*Formulir* 17)
   c. Bila memungkinkan dan dibutuhkan aset yang dibawa keluar area organisasi harus terdokumentasikan.
   d. Apabila diperlukan pemeriksaan dapat dilakukan terhadap personel yang keluar dari area organisasi.

2.8 Komunikasi dan Manajemen Operasi

Keamanan operasi bertujuan untuk memastikan keamanan dalam pengoperasian fasilitas pemrosesan informasi yang berada dalam lingkup Pemerintah Provinsi Papua Barat

A. Kebijakan

1. Prosedur Operasional dan Tanggung Jawab
   a. Dokumentasi Prosedur Operasional
      1) Prosedur operasional harus didokumentasikan, dipelihara dan tersedia untuk seluruh pengguna sistem informasi organisasi yang membutuhkannya;
      2) Prosedur yang terdokumentasi harus disiapkan untuk aktivitas sistem yang terkait dengan fasilitas pemrosesan informasi dan komunikasi, seperti prosedur *startup* dan *shutdown* server, *backup*, pemeliharaan perangkat, penanganan media, dan pengelolaan email;
      3) Prosedur operasional harus secara spesifik memberikan rincian mengenai pelaksanaan kegiatan yang mencakup:
         a) Pengelolaan dan pengolahan informasi;
         b) Cadangan (*backup*);
         c) Penjadwalan aktivitas kerja yang perlu mempertimbangkan ketergantungan antar sistem;

d) Prosedur penanganan kesalahan (*error*) selama aktivitas pekerjaan berlangsung;
e) Pihak yang harus dihubungi untuk mendapatkan dukungan (*support*) apabila terjadi masalah atau kesulitan;
f) Prosedur *restart* dan *recovery* sistem;
g) Pengelolaan *audit trail* dan *log* sistem.

4) Dokumentasi prosedur operasional harus diperlakukan sebagai dokumen formal, dan setiap perubahan pada dokumen tersebut harus disetujui oleh manajemen.

b. Manajemen Perubahan
1) Perubahan sistem informasi dan fasilitas pengolahan informasi harus dikelola dan dikendalikan;
2) Sistem operasi dan aplikasi perangkat lunak harus dikelola dan dikendalikan melalui manajemen perubahan yang formal. Berdasarkan tingkat kepentingannya, perubahan digolongkan sebagai berikut:
a) Perubahan terencana adalah perubahan yang telah direncanakan sebelumnya;
b) Perubahan darurat adalah perubahan yang diperlukan untuk memperbaiki permasalahan pada sistem TI agar proses operasional dapat segera pulih, dan harus mendapatkan persetujuan dari pejabat yang berwenang.
3) Manajemen perubahan perlu mencakup, namun tidak terbatas pada:
a) Perencanaan dan pengujian setiap perubahan;
b) Penilaian potensi dampak, termasuk dampak dari sisi keamanan yang mungkin timbul akibat perubahan;
c) Prosedur persetujuan secara formal untuk setiap perubahan;
d) Komunikasi seluruh detail perubahan kepada personel yang relevan;
e) Prosedur *fallback* yang mencakup tanggung jawab untuk membatalkan dan memulihkan perubahan yang gagal atau menghadapi kejadian yang tidak terduga.

c. Pemisahan Tugas dan Tanggung Jawab bertujuan untuk:
1) Mengurangi risiko perubahan tanpa izin atau yang tidak disengaja serta penyalahgunaan aset organisasi;
2) Memastikan bahwa tidak ada seorang pun yang memiliki hak akses untuk memodifikasi atau menggunakan aset tanpa otorisasi atau deteksi.

d. Pemisahan Tanggung Jawab dalam Aktivitas Pengembangan, Pengujian, dan Operasional

1) Fasilitas sistem pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi risiko akses atau perubahan tanpa izin serta yang tidak disengaja pada sistem operasional;
2) Pemisahan antara lingkungan pengembangan, pengujian, dan operasional harus diidentifikasi dan dikendalikan. Hal-hal berikut perlu dipertimbangkan dalam proses pemisahan:
   a) Prosedur transfer perangkat lunak dari lingkungan pengembangan (*development*) ke lingkungan operasional (*production*) harus ditetapkan dan didokumentasikan dengan jelas;
   b) Perangkat lunak atau aplikasi yang digunakan di lingkungan pengembangan dan operasional harus dijalankan pada sistem atau perangkat keras yang terpisah serta pada domain atau direktori yang berbeda;
   c) *Compiler, editor,* dan *tools* pengembangan lainnya tidak diperbolehkan diakses dari sistem operasional kecuali sangat dibutuhkan;
   d) Apabila memungkinkan, lingkungan pengujian harus memiliki kesamaan baik konfigurasi maupun spesifikasi dengan lingkungan operasional;
   e) Pengguna harus menggunakan profil yang berbeda ketika menjalankan sistem di lingkungan operasional dan pengujian;
   f) Menu dalam aplikasi harus menampilkan keterangan yang jelas untuk meminimalkan kesalahan;
   g) Data yang bersifat sensitif tidak diperbolehkan disalin (*copy*) ke lingkungan pengujian.

2. Perencanaan dan Penerimaan Sistem
   a. Manajemen Kapasitas
      1) Penggunaan sumber daya pengolahan dalam sistem informasi organisasi harus dipantau, dilakukan proses *tuning*, dan dibuat proyeksi untuk menjamin kinerja sistem yang diharapkan tetap tersedia dan menghindari kegagalan sistem;
      2) Proyeksi penggunaan sistem di masa depan perlu mempertimbangkan kebutuhan bisnis, kondisi sistem informasi organisasi saat ini, serta tren perkembangan sistem;
      3) Aktivitas dalam sistem informasi, baik yang sedang berjalan maupun yang akan dijalankan, harus memuat item kebutuhan kapasitas sistem, seperti kapasitas memori atau

penyimpanan pada server, utilisasi *CPU* server atau utilisasi *backbone* jaringan *WAN*;

4) Proses *tuning* dan pemantauan penggunaan sistem harus dilakukan untuk meningkatkan ketersediaan dan efisiensi sistem;
5) Proses manajemen kapasitas perlu memperhatikan efisiensi biaya, waktu, dan sumber daya manusia;
6) Proyeksi kebutuhan masa depan harus diperhitungkan dengan memperhatikan kebutuhan bisnis dan sistem sesuai dengan tren saat ini;
7) Proses manajemen kapasitas perlu mempertimbangkan ketergantungan sumber daya manusia yang dapat menimbulkan ancaman terhadap kerahasiaan, integritas, serta ketersediaan informasi dan sistem informasi.

b. Penerimaan Sistem
   1) Kriteria penerimaan sistem informasi baru atau penggunaan versi baru harus ditetapkan dan disertai dengan pengujian sistem sebelum sistem tersebut secara formal diterima dan digunakan oleh organisasi;
   2) Manajemen terkait harus memastikan bahwa seluruh persyaratan dan kriteria penerimaan sistem baru telah didefinisikan dengan jelas, disetujui, didokumentasikan, dan diuji;
   3) Migrasi sistem baru atau penggunaan versi baru ke lingkungan produksi hanya dapat dilakukan setelah melalui proses penerimaan formal, dengan memperhatikan hal-hal berikut:
      a) Spesifikasi kebutuhan dan kinerja fasilitas pengolahan informasi;
      b) Pemulihan dari kegagalan (*error recovery*), prosedur *restart*, serta rencana dalam kondisi darurat (*contingency plan*);
      c) Persiapan dan pengujian prosedur operasional yang rutin dijalankan untuk dijadikan prosedur operasional standar;
      d) Kontrol keamanan yang telah disetujui;
      e) Prosedur manual yang efektif;
      f) Penyusunan rencana kelangsungan bisnis;
      g) Bukti bahwa instalasi sistem baru tidak menimbulkan gangguan pada sistem yang telah beroperasi;
      h) Pelatihan untuk penggunaan sistem baru;
      i) Kemudahan penggunaan sistem.

3. Perlindungan terhadap program yang membahayakan (*Malware*)

a. Unit terkait harus menerapkan sistem yang mampu melakukan pendeteksian, pemulihan, dan pencegahan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan.
b. Perlindungan terhadap ancaman program yang membahayakan akan ditetapkan dalam ketentuan khusus.

4. Cadangan (*Backup*)
   Beberapa hal berikut perlu dipertimbangkan dalam proses *backup* informasi:
   a. Organisasi harus menentukan informasi yang perlu dicadangkan (*backup*).
   b. Daftar informasi yang telah dicadangkan harus didokumentasikan dalam sebuah catatan yang harus selalu dipelihara.
   c. Prosedur pengembalian (*restore*) data harus didokumentasikan secara resmi.
   d. Hasil *backup* informasi harus mendapatkan perlindungan secara fisik.
   e. Media *backup* harus diuji secara berkala untuk memastikan bahwa media tersebut dapat berfungsi dengan baik saat dibutuhkan.
   f. Informasi yang bersifat sensitif perlu dilindungi dengan enkripsi pada data yang telah dicadangkan.
5. Pencatatan riwayat dan pemantauan mencakup:
   a. Kegagalan akses (*access failures*).
   b. Pola *logon* yang mengindikasikan penggunaan yang tidak wajar.
   c. Alokasi dan Penggunaan Hak Akses Khusus (*Privileged Access Capability*).
   d. Penelusuran transaksi dan pengiriman *file* tertentu yang mencurigakan.
   e. Penggunaan sumber daya sensitif.
6. Pengendalian operasional perangkat lunak mencakup:
   a. Pengendalian akses terhadap perangkat lunak sebelum dilakukan pengembangan.
   b. Petunjuk mengenai pengembangan, penggunaan lisensi, pengoperasian, dan pemeliharaan perangkat lunak.
7. Pengelolaan kerentanan teknis meliputi:
   a. Mengidentifikasi sumber informasi yang dapat digunakan untuk meningkatkan kewaspadaan terhadap kerentanan teknis.
   b. Apabila terjadi kerentanan teknis yang memerlukan penanganan, harus diambil tindakan sesuai dengan kontrol yang telah ditetapkan.
   c. Menguji dan mengevaluasi penggunaan *patch* sebelum proses instalasi untuk memastikan *patch* bekerja secara efektif dan tidak menimbulkan risiko lain.

d. Jika *patch* tidak tersedia, harus melakukan hal-hal berikut:
   1) Mematikan komponen yang terhubung dengan kerentanan;
   2) Menambahkan pengendalian akses seperti *firewall*;
   3) Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian;
   4) Meningkatkan kewaspadaan terhadap kerentanan teknis.
e. Menyimpan audit log yang memuat prosedur dan langkah-langkah yang telah diambil.
f. Melakukan pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis secara berkala.
g. Mengutamakan pengelolaan kerentanan teknis terhadap sistem informasi yang memiliki tingkat risiko tinggi.

8. Audit operasional mencakup:
   a. Prosedur perencanaan audit.
   b. Proses untuk melakukan audit.
   c. Proses pelaporan dan pemantauan tindak lanjut audit.
   d. Persyaratan auditor.

A. Standar

1. Dokumentasi prosedur operasional mencakup:
   a. Tata cara pengelolaan dan penanganan informasi;
   b. Tata cara menangani kesalahan-kesalahan yang terjadi; (Formulir 18).
   c. Cara memfungsikan dan mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
   d. Tata cara backup dan restore; (Formulir 19).
   e. Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian.
2. Pemisahan perangkat pengembangan, pengujian, dan operasional harus mempertimbangkan hal-hal berikut:
   a. Pengembangan dan operasional perangkat lunak harus dilakukan pada sistem serta domain atau direktori yang berbeda;
   b. Instruksi kerja (*working instruction*) mengenai pengembangan perangkat lunak hingga operasional harus ditetapkan dan didokumentasikan;
   c. *Compiler*, *editor*, dan *tools* pengembangan lainnya tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
   d. Lingkungan pengujian sistem sebaiknya disamakan dengan lingkungan sistem operasional;
   e. Pengguna harus menggunakan profil yang berbeda untuk sistem operasional guna mengurangi risiko kesalahan;
   f. Data yang memiliki klasifikasi sangat rahasia, rahasia, dan terbatas tidak boleh disalin ke dalam lingkungan pengujian sistem.
3. Pencatatan riwayat dan pemantauan mencakup:

a. Kegagalan akses (*access failures*);
b. Pola *logon* yang mengindikasikan penggunaan yang tidak wajar;
c. Alokasi dan penggunaan hak akses khusus (*privileged access capability*);
d. Penelusuran transaksi dan pengiriman *file* tertentu yang mencurigakan;
e. Penggunaan sumber daya sensitif.

4. Pengendalian operasional perangkat lunak mencakup:
   a. Pengendalian akses terhadap perangkat lunak sebelum dilakukan pengembangan;
   b. Petunjuk penerapan (*deployment*), penggunaan lisensi, pengoperasian dan pemeliharaan perangkat lunak
5. Pengelolaan kerentanan teknis mencakup:
   a. Penunjukan fungsi dan tanggung jawab terkait dengan pengelolaan kerentanan teknis, termasuk penilaian risiko kerentanan, *patching*, registrasi aset, dan koordinasi dengan pihak terkait, harus dilakukan dengan jelas.
   b. Pengidentifikasian sumber informasi yang dapat digunakan untuk meningkatkan kesadaran terhadap kerentanan teknis harus dilakukan secara efektif.
   c. Rentang waktu untuk mengambil tindakan terhadap potensi kerentanan teknis harus ditentukan dengan tepat.
   d. Jika terjadi kerentanan teknis yang membutuhkan penanganan, maka tindakan harus diambil sesuai dengan kontrol yang telah ditetapkan.
   e. Pengujian dan evaluasi penggunaan *patch* harus dilakukan sebelum proses instalasi untuk memastikan *patch* bekerja secara efektif dan tidak menimbulkan risiko lain.
   f. Penyimpanan audit log harus mencakup prosedur dan langkah-langkah yang telah diambil.
   g. Pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala.
   h. Pengelolaan kerentanan teknis harus diprioritaskan pada sistem informasi yang memiliki tingkat risiko tinggi.

2.9 Keamanan Komunikasi

Tujuannya untuk mengendalikan informasi yang ditransmisikan melalui jaringan komunikasi beserta perangkat pendukungnya yang ada di lingkup Diskominfo Provinsi Papua Barat.

A. Kebijakan

1. Manajemen Keamanan Jaringan meliputi:
   a. Pengendalian Jaringan

1) Unit terkait harus mengelola dan melindungi jaringan dari berbagai bentuk ancaman;
2) Ketentuan pengendalian jaringan pada unit terkait diuraikan dalam standar pengelolaan layanan jaringan.

b. Keamanan layanan jaringan
Unit terkait harus mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan, serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan, termasuk penyediaan layanan jaringan oleh pihak ketiga.

2. Keamanan dalam transfer informasi meliputi:
   a. Pertukaran informasi dan perangkat lunak dengan pihak ketiga hanya bisa dilakukan atas kesepakatan tertulis kedua belah pihak.
   b. Unit terkait harus melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi.
   c. Unit terkait menerapkan pengendalian keamanan untuk mengirim informasi melalui surat elektronik, atau melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang.
   d. Ketentuan pertukaran informasi pada unit terkait diuraikan dalam standar pengelolaan komunikasi dan operasional.

B. Standar

1. Pengelolaan keamanan jaringan mencakup: (*Formulir 20)*
   a. Pemantauan kegiatan pengelolaan jaringan harus dilakukan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien.
   b. Pengendalian dan pengaturan mengenai penyambungan atau perluasan jaringan, baik internal maupun eksternal, harus diterapkan.
   c. Pengendalian dan pengaturan akses ke sistem jaringan, baik internal maupun eksternal, harus dilakukan dengan ketat.
   d. Pencatatan kegiatan pihak ketiga yang diizinkan mengakses jaringan sistem informasi harus dilakukan dengan cermat.
   e. Pemutusan layanan tanpa pemberitahuan sebelumnya harus dilakukan jika terjadi gangguan keamanan informasi.
   f. Perlindungan jaringan dari akses yang tidak berwenang mencakup:
      1) Penetapan penanggung jawab pengelolaan jaringan yang dipisahkan dari pengelolaan perangkat pengelola informasi;
      2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum, antara lain dengan penggunaan enkripsi dan tanda tangan digital;

3) Pendokumentasian arsitektur jaringan yang mencakup seluruh komponen perangkat keras dan perangkat lunak jaringan.

g. Penerapan fitur keamanan layanan jaringan mencakup:
   1) Teknologi keamanan jaringan, seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;
   2) Parameter yang diperlukan untuk keamanan koneksi pada layanan jaringan harus disesuaikan dengan aturan koneksi jaringan.

2. Keamanan dalam transfer informasi
   a. Prosedur pertukaran informasi ketika menggunakan perangkat komunikasi elektronik, mencakup:
      1) Perlindungan, pencegatan, penyalinan, modifikasi, *miss-routing* dan perusakan;
      2) Pendeteksian dan perlindungan terhadap kode bahaya (*malicious code*) yang dikirim melalui perangkat komunikasi elektronik;
      3) Perlindungan informasi elektronik dalam bentuk *attachment* yang memiliki klasifikasi sangat rahasia, rahasia dan terbatas;
      4) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel harus dilakukan secara cermat;
      5) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel.
   b. Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik mengacu pada ketentuan yang berlaku. (Formulir 21 dan Formulir 22)
   c. Pengendalian pertukaran informasi yang menggunakan perangkat komunikasi elektronik, mencakup:
      1) Pencegahan terhadap penyalahgunaan wewenang oleh pegawai dan pihak ketiga yang dapat membahayakan organisasi harus dilakukan dengan serius;
      2) Penggunaan teknik kriptografi harus diterapkan untuk melindungi informasi;
      3) Larangan meninggalkan informasi sensitif pada perangkat pengelola informasi harus ditegakkan dengan ketat;
      4) Pembatasan penerusan informasi secara otomatis harus diterapkan untuk menghindari penyebaran yang tidak diinginkan;
      5) Membangun kepedulian terhadap ancaman pencurian informasi harus dilakukan, misalnya terhadap:
         a) Pengungkapan informasi sensitif harus dilakukan dengan hati-hati untuk menghindari penyadapan saat melakukan panggilan telepon;

b) Akses terhadap pesan harus dibatasi sesuai dengan kewenangannya;
c) Pemrograman mesin faks, baik yang dilakukan secara sengaja maupun tidak sengaja, untuk mengirim pesan ke nomor tertentu harus dihindari;
d) Pengiriman dokumen dan pesan harus dilakukan dengan hati-hati agar tidak sampai ke tujuan yang salah;
e) Pendaftaran data demografis, seperti alamat surel atau informasi pribadi lainnya, harus dilakukan untuk menghindari pengumpulan informasi yang tidak sah;
f) Penyediaan informasi internal kepada masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

2.10 Akuisisi Sistem, Pengembangan dan Pemeliharaan

Akuisisi sistem, pengembangan dan pemeliharaan bertujuan untuk memastikan bahwa keamanan informasi terintegrasi dengan sistem informasi serta mencegah kesalahan, kehilangan, dan modifikasi oleh pihak yang tidak berwenang.

A. Kebijakan

1. Persyaratan keamanan sistem informasi setidaknya mencakup:
   a. Unit terkait menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi sebelum pengadaan, pengembangan atau pemeliharaan sistem informasi baru.
   b. Pengolahan informasi pada aplikasi, mencakup:
      1) Validasi data yang masuk;
      2) Data yang akan dimasukkan ke aplikasi harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya;
      3) Pengendalian proses internal;
      4) Setiap aplikasi harus disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan;
      5) Validasi data keluaran.
   c. Data keluaran aplikasi harus divalidasi untuk memastikan bahwa data yang dihasilkan benar.
2. Keamanan dan proses pengembangan data pendukung
   a. Pengolahan data elektronik harus mengendalikan perubahan pada sistem operasi sesuai dengan prosedur yang berlaku.
   b. Pengolahan data elektronik harus mengendalikan perubahan terhadap perangkat lunak, baik yang dikembangkan sendiri maupun yang berasal dari pihak ketiga.
   c. Kajian teknis aplikasi setelah perubahan sistem operasi atau perangkat lunak harus memastikan bahwa tidak ada dampak

merugikan pada operasional atau keamanan informasi unit terkait.

d. Unit terkait harus mencegah terjadinya kebocoran informasi.
e. Unit terkait harus melakukan supervisi dan pemantauan terhadap perubahan perangkat lunak yang berasal dari pihak ketiga.

3. Keamanan Sistem File
   a. Unit terkait harus memiliki prosedur untuk pengendalian perangkat lunak pada sistem operasinya.
   b. Unit terkait harus menentukan sistem pengujian data untuk melindungi dari kemungkinan kerusakan, kehilangan, atau perubahan data oleh pihak yang tidak berwenang.
   c. Unit terkait harus mengendalikan akses ke kode program secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.

B. Standar

1. Spesifikasi kebutuhan perangkat pengolahan informasi yang dikembangkan, baik oleh internal maupun pihak ketiga harus didokumentasikan secara formal.
2. Standar Pengolahan Data dan Informasi adalah sebagai berikut:
   a. Pemeriksaan data masukan harus mencakup:
      1) Penerapan laporan rangkap atau mekanisme pengecekan masukan lainnya untuk mendeteksi kesalahan berikut:
         a) Nilai diluar rentang atau batas yang diperlukan;
         b) Karakter tidak valid dalam *field* data;
         c) Data yang hilang atau tidak lengkap;
         d) Melebihi batas atas dan bawah volume data;
         e) Data yang tidak diotorisasi dan tidak konsisten.
      2) Pengkajian secara berkala terhadap isi *field* kunci atau data untuk mengonfirmasi keabsahan dan integrasi data;
      3) Memeriksa dokumen *hard copy* untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otoritas;
      4) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;
      5) Prosedur untuk menguji kewajaran data masukan;
      6) Menguraikan tanggung jawab seluruh pegawai yang terkait dengan perekaman data;
      7) Sistem harus mampu membuat dan mengeluarkan catatan aktivitas terkait proses perekaman data.
   b. Menyusun daftar yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasil secara aman. Proses pemeriksaan mencakup:
      1) Pengendalian sesi atau batch untuk mencocokkan data setelah perubahan transaksi;

2) Pengendalian *balancing* untuk memeriksa data sebelum dan setelah transaksi;
3) Validasi data masukan yang dihasilkan sistem;
4) Memastikan keutuhan dan keaslian data yang diunduh (*download*) atau diunggah (*upload*);
5) Total *hash* dari *record* dan file;
6) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
7) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi;
8) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c. Pemeriksaan data keluaran harus mempertimbangkan:
1) Pelajaran dari data keluaran yang dihasilkan;
2) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;
3) Menyediakan informasi yang cukup pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;
4) Prosedur untuk menindak lanjuti validasi data keluaran;
5) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran dan;
6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

3. Keamanan *File* Sistem
a. Pengembangan prosedur pengendalian perangkat lunak pada sistem operasional harus mempertimbangkan:
1) Proses pemutakhiran perangkat lunak operasional, aplikasi, dan *library* hanya boleh dilakukan oleh administrator terlatih setelah melalui proses otorisasi;
2) Sistem operasional hanya berisi program aplikasi yang telah diotorisasi, tidak boleh berisi kode program;
3) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian;
4) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem;
5) Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan;
6) Catatan audit harus dipelihara untuk menjaga pemutakhiran *library*;
7) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontingensi;

8) Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi prosedur, parameter, konfigurasi, dan perangkat lunak pendukung.

b. Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
   1) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
   2) Pengelolaan kode program (*source code*) dan *library* harus mengikuti prosedur yang telah ditetapkan;
   3) Pengelola TI tidak boleh memiliki akses yang tidak terbatas ke kode program (*source code*) dan *library*;
   4) Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program kepada *programmer* hanya dapat dilakukan setelah melalui proses otorisasi;
   5) *Listing* program harus disimpan dalam *secure areas*;
   6) Catatan audit dari seluruh akses ke kode program *library* harus dipelihara;
   7) Pemeliharaan dan penyalinan kode program dan *library* harus mengikuti prosedur pengendalian perubahan.

4. Keamanan dalam proses pengembangan dan pendukung
   a. Prosedur pengendalian perubahan sistem operasi dan perangkat lunak, mencakup:
      1) Memelihara catatan persetujuan sesuai dengan kewenangannya;
      2) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;
      3) Melakukan *review* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
      4) Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diubah;
      5) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan (Formulir 24);
      6) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;
      7) Memastikan bahwa dokumentasi pemutakhiran sistem dan dokumen versi sebelumnya diarsip;
      8) Memelihara versi perubahan aplikasi;
      9) Memelihara jejak audit perubahan aplikasi;
      10) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan;
      11) Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak mengganggu kegiatan.

b. Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan perangkat lunak, mencakup:
   1) Melakukan *review* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
   2) Memastikan rencana dan anggaran tahunan yang mencakup peninjauan dan pengujian sistem terhadap perubahan sistem operasi;
   3) Memastikan pemberitahuan perubahan sistem informasi dalam jangka waktu yang tepat dan telah dilaksanakan sebelum implementasi;
   4) Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan.
c. Pengendalian dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:
   1) Melakukan pemantauan terhadap aktivitas pegawai dan pihak ketiga, sesuai ketentuan yang berlaku;
   2) Melakukan pemantauan terhadap aktivitas penggunaan *desktop* dan perangkat *mobile*.
d. Pengembangan perangkat lunak oleh pihak ketiga harus mempertimbangkan:
   1) Ada persetujuan dari yang berwenang dalam hal ini bidang infrastruktur teknologi informasi dan komunikasi;
   2) Perjanjian lisensi, kepemilikan *source code*, dan hak atas kekayaan intelektual (HAKI);
   3) Perjanjian jaminan pelaksanaan (*escrow*);
   4) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
   5) Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;
   6) Uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi.

2.11 Hubungan dengan Pihak Ketiga atau Pemasok

Hubungan dengan pihak ketiga atau pemasok bertujuan untuk memastikan perlindungan aset organisasi dari akses pihak ketiga atau pemasok. Oleh karena itu, organisasi diharuskan melakukan penilaian risiko keamanan informasi secara menyeluruh ketika memberikan akses kepada pihak ketiga atau pemasok terhadap sistem informasi dan aset organisasi. Penilaian ini bertujuan untuk mengidentifikasi dan meminimalkan potensi kerentanan yang dapat dieksploitasi oleh pihak ketiga atau pemasok untuk melakukan akses tidak sah terhadap informasi dan aset organisasi. Selain itu, organisasi juga perlu

menerapkan ketentuan yang jelas dan tegas untuk melindungi informasi dan aset dari akses tidak sah.

A. Kebijakan

1. Keamanan Informasi dalam Hubungan Pihak Ketiga atau Pemasok
    a. Unit terkait diharuskan untuk secara proaktif mengidentifikasi dan menerapkan prosedur guna memitigasi risiko keamanan yang timbul dari penggunaan produk dan layanan oleh pihak ketiga atau pemasok.
    b. Unit terkait harus secara tegas mewajibkan pihak ketiga atau pemasok untuk mematuhi kebijakan organisasi dan memastikan tidak ada upaya ilegal yang dilakukan untuk mengakses informasi dan aset.
    c. Unit terkait diharuskan untuk membuat perjanjian dengan pihak ketiga atau pemasok yang didasarkan pada kontrol keamanan informasi dan kebutuhan bisnis yang memuat klausul mewajibkan mereka untuk mematuhi standar keamanan informasi yang ditetapkan dan memenuhi kebutuhan bisnis yang telah disepakati.
    d. Unit terkait diharuskan untuk secara jelas mendefinisikan keamanan informasi, serta menetapkan persyaratan yang jelas dalam mengakses produk atau layanan informasi dan teknologi komunikasi.
    e. Unit terkait diharuskan untuk menyusun dan menerapkan prosedur yang efektif dalam memantau dan memvalidasi produk dan layanan, dengan tujuan memastikan kepatuhan pihak ketiga atau pemasok terhadap persyaratan keamanan yang telah disepakati.
    f. Unit terkait diharuskan untuk merencanakan dan menyelenggarakan sesi penyadaran bagi anggota organisasi pihak ketiga atau pemasok yang akan diberikan akses terhadap informasi dan aset organisasi.
2. Manajemen Pemberian Layanan oleh Pihak Ketiga atau Pemasok
    a. Unit terkait diharuskan untuk menerapkan langkah-langkah pencegahan yang efektif dalam memantau dan meninjau layanan pihak ketiga atau pemasok, dengan mempertimbangkan tingkat keamanan dan layanan yang telah disepakati.
    b. Unit terkait diharuskan untuk secara konsisten melakukan pemantauan, peninjauan, dan audit terhadap kinerja pihak ketiga atau pemasok.
    c. Pihak ketiga atau pemasok diharuskan untuk mempertimbangkan kekritisan informasi bisnis, sistem dan proses yang berjalan, serta penilaian risiko dalam melakukan perubahan pada penyediaan layanan, termasuk pemeliharaan

dan peningkatan kebijakan, prosedur, dan kontrol keamanan informasi yang ada.

B. Standar

1. Keamanan informasi dalam hubungan pihak ketiga atau pemasok
   a. Keamanan informasi untuk hubungan pihak ketiga atau pemasok
      1) Mengidentifikasi dan mendokumentasikan jenis-jenis pihak ketiga atau pemasok yang memiliki akses ke informasi organisasi dan dapat memengaruhi kerahasiaan, integritas, dan ketersediaan informasi organisasi;
      2) Merumuskan dan menerapkan mekanisme evaluasi dan pemilihan pihak ketiga atau pemasok yang komprehensif dan terukur, dengan mempertimbangkan tingkat sensitivitas informasi, produk, dan layanan yang akan diakses atau disediakan;
      3) Mendefinisikan secara jelas dan terukur informasi organisasi, layanan TIK, dan infrastruktur fisik yang dapat diakses, dipantau, dikontrol, atau digunakan oleh pihak ketiga atau pemasok;
      4) Menilai dan mengelola risiko keamanan informasi yang terkait dengan: (Formulir 08)
         a) Penggunaan informasi organisasi dan aset terkait lainnya oleh pihak ketiga atau pemasok, termasuk risiko yang berasal dari personel pemasok yang berpotensi jahat;
         b) Malfungsi atau kerentanan produk (termasuk komponen perangkat lunak dan subkomponen yang digunakan dalam produk ini) atau layanan yang disediakan oleh pihak ketiga atau pemasok.
      5) Memantau kepatuhan pihak ketiga atau pemasok terhadap persyaratan keamanan informasi yang telah ditetapkan;
      6) Menangani insiden dan kontinjensi yang terkait dengan produk dan layanan pihak ketiga atau pemasok dengan menetapkan tanggung jawab yang jelas dan terukur bagi organisasi dan pihak ketiga atau pemasok;
      7) Mendefinisikan dan mendokumentasikan langkah-langkah pemulihan dan kontinjensi yang jelas dan terukur untuk memastikan ketersediaan informasi organisasi;
      8) Menyelenggarakan pelatihan bagi personel organisasi yang berinteraksi dengan personel pihak ketiga atau pemasok. Pelatihan ini harus mencakup pemahaman tentang aturan, kebijakan, proses dan prosedur, serta perilaku yang diharapkan berdasarkan jenis dan tingkat akses pihak ketiga atau pemasok ke sistem dan informasi organisasi;

9) Memastikan persyaratan pemutusan hubungan pihak ketiga atau pemasok yang aman, diantaranya:
   a) Pencabutan hak akses; (Formulir 09)
   b) Penanganan informasi;
   c) Menentukan kepemilikan kekayaan intelektual yang dikembangkan selama keterikatan;
   d) Portabilitas informasi jika terjadi perubahan pihak ketiga atau pemasok atau *insourcing*;
   e) Pengelolaan arsip;
   f) Pengembalian aset; (Formulir 12)
   g) Pembuangan informasi dan aset terkait lainnya secara aman; (Formulir 25 dan Formulir 13)
   h) Persyaratan kerahasiaan yang berlangsung.

b. Mengatasi keamanan dalam perjanjian pemasok
   1) Uraikan dengan jelas informasi yang akan diakses dan metode pengaksesan informasi tersebut;
   2) Klasifikasi informasi menurut skema klasifikasi organisasi;
   3) Pemetaan antara skema klasifikasi organisasi dan skema klasifikasi pihak ketiga atau pemasok;
   4) Memastikan adanya persyaratan hukum, undang-undang, peraturan dan kontrak yang berlaku, termasuk persyaratan terkait perlindungan data, penanganan informasi pengenal pribadi, hak kekayaan intelektual dan hak cipta;
   5) Memastikan kewajiban masing-masing pihak terdapat dalam kontrak sebagai perangkat kontrol yang disepakati, termasuk kontrol akses, tinjauan kinerja, pemantauan, pelaporan dan audit, dan kewajiban untuk mematuhi persyaratan keamanan informasi organisasi;
   6) Menentukan prosedur untuk otorisasi dan penghapusan otorisasi dalam penggunaan informasi organisasi dan aset terkait lainnya oleh personel pihak ketiga atau pemasok;
   7) Terdapat persyaratan ganti rugi dan remediasi atas kegagalan pihak ketiga atau pemasok;
   8) Terdapat persyaratan dan prosedur manajemen insiden;
   9) Menentukan aturan yang relevan untuk sub-kontrak, termasuk kontrol yang perlu diterapkan, seperti perjanjian penggunaan sub-pemasok;
   10) Terdapat kontak person untuk masalah keamanan informasi;
   11) Melakukan audit terhadap proses dan kontrol pihak ketiga atau pemasok sesuai dengan perjanjian;
   12) Kewajiban pihak ketiga atau pemasok untuk secara berkala menyampaikan laporan sebagai efektivitas kontrol yang di disepakati;

13) Terdapat proses resolusi cacat dan resolusi konflik;
14) Penyediaan metode untuk memusnahkan secara aman informasi organisasi yang disimpan oleh pihak ketiga atau pemasok segera setelah tidak lagi diperlukan; (Formulir 25 dan Formulir 13)
15) Memastikan pada akhir kontrak, pihak ketiga atau pemasok menyerahkan seluruh data/aset pendukung kepada pemilik aset informasi. (Formulir 12)

c. Rantai Pasok Teknologi Informasi dan Komunikasi
1) Mendefinisikan persyaratan keamanan informasi untuk diterapkan pada akuisisi produk atau layanan TI;
2) Mengharuskan pihak ketiga atau pemasok layanan TI menyebarkan persyaratan keamanan organisasi diseluruh rantai pasokan jika mereka mensubkontrakkan bagian dari layanan TI yang disediakan untuk organisasi;
3) Mengharuskan pihak ketiga atau pemasok produk TI menyebarkan praktik keamanan yang sesuai diseluruh rantai pasokan jika produk ini mencakup komponen yang dibeli atau diperoleh dari pemasok lain atau entitas lain;
4) Mengharuskan pihak ketiga atau pemasok produk TI untuk memberikan informasi yang menjelaskan komponen perangkat lunak yang digunakan dalam produk;
5) Mengharuskan pihak ketiga atau pemasok produk TI untuk memberikan informasi yang menjelaskan fungsi keamanan yang diterapkan dari produknya beserta konfigurasinya;
6) Menerapkan proses pemantauan dengan metode yang dapat diterima untuk memvalidasi bahwa produk dan layanan TI yang dikirimkan memenuhi persyaratan keamanan informasi; (Formulir 26)
7) Menerapkan proses untuk mengidentifikasi dan mendokumentasikan komponen produk atau layanan penting untuk mempertahankan fungsionalitas;
8) Memerlukan perhatian khusus, pengawasan, dan tindak lanjut terhadap komponen produk yang dibangun di luar organisasi terutama jika pihak ketiga atau pemasok mengalihdayakan aspek komponen produk atau layanan ke pihak lain; (Formulir 26)
9) Menjamin bahwa komponen penting dan asalnya dapat dilacak di seluruh rantai pasokan;
10) Menjaminan bahwa produk TI yang dikirimkan berfungsi seperti yang diharapkan dan tidak terdapat fitur yang tidak diharapkan; (Formulir 26)

11) Menerapkan proses untuk memastikan bahwa komponen dari pihak ketiga atau pemasok adalah asli dan tidak berubah dari spesifikasinya; (Formulir 26)
12) Menjamin bahwa produk TI mencapai tingkat keamanan yang dipersyaratkan, misalnya, melalui sertifikasi formal atau skema evaluasi seperti *Common Criteria Recognition Arrangement*; (Formulir 26)
13) Menetapkan aturan yang jelas dan terukur mengenai berbagi informasi terkait rantai pasok dan setiap potensi masalah dan kompromi yang dapat terjadi antara organisasi dan pihak ketiga atau pemasok;
14) Menerapkan proses khusus untuk mengelola siklus hidup komponen TI dan ketersediaan serta risiko keamanan terkait. Ini termasuk mengelola risiko komponen yang tidak lagi tersedia karena pihak ketiga atau pemasok tidak lagi berbisnis atau pihak ketiga atau pemasok tidak lagi menyediakan komponen ini karena kemajuan teknologi.

2. Manajemen Pengiriman Layanan Pemasok
   a. Pemantauan, peninjauan dan perubahan layanan pemasok
      1) Memantau tingkat kinerja layanan untuk memverifikasi kepatuhan terhadap perjanjian;
      2) Memantau perubahan yang dilakukan oleh pihak ketiga atau pemasok, termasuk:
         a) peningkatan pada layanan yang ditawarkan saat ini;
         b) pengembangan aplikasi dan sistem baru;
         c) modifikasi atau pembaruan kebijakan dan prosedur pihak ketiga atau pemasok;
         d) kontrol baru atau yang diubah untuk menyelesaikan insiden keamanan informasi dan untuk meningkatkan keamanan informasi.
      3) Memantau perubahan dalam layanan pihak ketiga atau pemasok termasuk:
         a) perubahan dan peningkatan jaringan;
         b) penggunaan teknologi baru;
         c) adopsi produk baru atau versi atau rilis yang lebih baru;
         d) alat dan lingkungan pengembangan baru;
         e) perubahan lokasi fisik fasilitas pelayanan;
         f) perubahan sub-pemasok;
         g) sub-kontrak ke pemasok lain.
      4) Meninjau laporan layanan yang dihasilkan oleh pihak ketiga atau pemasok dan mengatur pertemuan kemajuan rutin seperti yang dipersyaratkan oleh perjanjian;
      5) Melakukan audit terhadap pihak ketiga atau pemasok dan sub-pemasok, bersamaan dengan penelaahan atas laporan

auditor independen jika tersedia dan tindak lanjut atas masalah yang teridentifikasi;

6) Memberikan informasi tentang insiden keamanan informasi dan meninjau informasi ini sebagaimana disyaratkan oleh perjanjian;
7) Meninjau jejak audit pihak ketiga atau pemasok dan catatan peristiwa keamanan informasi, masalah operasional, kegagalan, penelusuran kesalahan dan gangguan terkait dengan layanan yang diberikan;
8) Menanggapi dan mengelola setiap peristiwa atau insiden keamanan informasi yang teridentifikasi;
9) Mengidentifikasi kerentanan keamanan informasi dan mengelolanya;
10) Memastikan bahwa pihak ketiga atau pemasok mempertahankan kemampuan layanan dan keamanan yang memadai bersama dengan rencana yang dapat diterapkan yang dirancang untuk memastikan bahwa tingkat kesinambungan layanan yang disepakati dipertahankan setelah kegagalan atau bencana layanan besar;
11) Memastikan bahwa pihak ketiga atau pemasok menetapkan tanggung jawab untuk meninjau kepatuhan dan menegakkan persyaratan perjanjian.

2.12 Manajemen Insiden Keamanan Informasi

Manajemen insiden keamanan informasi bertujuan untuk menyusun dan menerapkan mekanisme komunikasi yang efektif dan efisien terkait kejadian dan kelemahan keamanan sistem informasi. Mekanisme ini harus memastikan bahwa informasi tersebut dikomunikasikan dengan jelas, akurat dan tepat waktu kepada pihak-pihak yang berkepentingan, sehingga tindakan perbaikan dapat berjalan secara efektif dan tepat waktu, serta untuk mencegah terulangnya kejadian serupa.

A. Kebijakan

1. Unit terkait diwajibkan untuk menetapkan tanggung jawab dan prosedur yang jelas dan terukur untuk memastikan tanggapan yang cepat, efektif, dan teratur terhadap insiden keamanan informasi.
2. Unit terkait diwajibkan untuk mencatat dan melaporkan semua peristiwa keamanan informasi melalui prosedur manajemen yang tersedia secepat mungkin.
3. Unit terkait diharuskan untuk meminta dan mewajibkan pegawai dan pihak ketiga yang menggunakan sistem dan layanan informasi organisasi untuk mencatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai dalam sistem atau layanan.

4. Unit terkait diwajibkan untuk menilai dan memutuskan setiap peristiwa keamanan informasi untuk menentukan apakah peristiwa tersebut diklasifikasikan sebagai insiden keamanan informasi.
5. Unit terkait diwajibkan untuk merespons setiap peristiwa keamanan informasi dengan mengikuti prosedur yang telah ditetapkan dan didokumentasikan dengan baik.
6. Unit terkait diwajibkan untuk memanfaatkan pengetahuan yang diperoleh dari analisis dan penyelesaian insiden keamanan informasi untuk mengurangi kemungkinan dampak insiden di masa depan.
7. Unit terkait diwajibkan untuk menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, perolehan, dan pelestarian informasi yang dapat difungsikan sebagai bukti.

B. Standar

1. Jenis Insiden Keamanan Informasi
   Beberapa skenario yang dapat dianggap sebagai insiden keamanan informasi diantaranya namun tidak terbatas pada:
   a. Insiden atas hilangnya layanan, perangkat atau fasilitas.
   b. Insiden atas kerusakan fungsi sistem.
   c. Insiden atas kelebihan beban sistem.
   d. Insiden atas perubahan sistem tidak sah atau diluar kendali.
   e. Insiden atas kesalahan atau kelalaian manusia.
   f. Insiden atas pelanggaran keamanan informasi.
   g. Insiden atas praktik yang tidak diikuti sesuai kebijakan dan prosedur.
   h. Insiden atas kesalahan dalam sistem perangkat lunak atau perangkat keras.
2. Pelaporan insiden keamanan informasi mencakup :
   a. Pelaporan dapat dilakukan secara langsung dan atau tidak *langsung*.
   b. Pelaporan secara langsung disampaikan secara tatap muka kepada petugas pelayanan pengaduan melalui ruang layanan pengaduan.
   c. Pengaduan secara tidak langsung disampaikan melalui media resmi pengaduan kementerian dan atau pemerintah daerah yaitu:
      1) SP4N-LAPOR!;
      2) Surat;
      3) *Website*;
      4) Surat Elektronik;
      5) *Faksimile*;
      6) *Call Centre*;
      7) *Short Message Service*;
      8) Media Sosial;

9) *Whistle Blowing System*;
10) Aplikasi pengaduan lainnya yang terintegrasi dengan SP4N-LAPOR!.

d. Pelaporan paling sedikit memuat informasi identitas pelapor, subtansi pengaduan, pihak terlibat, waktu, tempat, kronologi kejadian dan bukti pendukung apabila tersedia.
e. Mekanisme pelaporan insiden dan tindakan tanggapan terhadap insiden.
f. Ketersediaan formulir pelaporan insiden keamanan informasi. (*Formulir 07*)
g. Pelaporan tindakan penanganan terhadap peningkatan insiden serta tindakan pemulihan dari insiden.
h. Detail insiden harus direkam yaitu jenis masalah, pesan yang muncul di layar dan lain lain, yang dapat dibagikan dengan petugas insiden untuk penyelesaian yang lebih cepat.
i. Pelaporan status insiden kepada pelapor insiden dan mengumpulkan umpan balik dari insiden untuk memastikan bahwa dampak insiden telah teratasi dan status insiden dapat ditutup.

3. Penilaian dan Keputusan tentang kejadian keamanan informasi, menilai peristiwa keamanan informasi untuk memutuskan apakah peristiwa keamanan benar-benar merupakan insiden keamanan informasi, penilaian dilakukan oleh petugas insiden dengan mengacu pada skala klasifikasi insiden dan terdokumentasi. (Formulir 27)
4. Prosedur penanganan perlu dibuat untuk menangani berbagai tipe insiden keamanan informasi, yang meliputi namun tidak terbatas pada:
   a. Hilangnya layanan, peralatan atau fasilitas sistem informasi.
   b. *Malicious code virus, worm*, *trojan horse*, atau jenis program jahat lainnya yang berhasil menginfeksi suatu *host.*
   c. *Denial of service* suatu serangan yang mengakibatkan penolakan atau gangguan atas penggunaan sistem, jaringan, atau aplikasi.
   d. *Multiple Component* suatu insiden yang merupakan gabungan dari beberapa jenis insiden.
   e. Kesalahan yang diakibatkan oleh data yang tidak lengkap atau tidak akurat.
   f. Kebocoran informasi yang menyebabkan hilangnya aspek kerahasiaan dan integritas informasi.
   g. Penyalahgunaan sistem informasi.
   h. Ketidakpatuhan terhadap kebijakan dan prosedur yang berlaku.
   i. Kerusakan pada perangkat lunak maupun perangkat keras.
5. Selain dari rencana penanggulangan, prosedur juga perlu mencakup:
   a. Analisa dan identifikasi penyebab dari insiden.

b. Karantina atau pembatasan gangguan.
c. Perencanaan dan implementasi tindakan korektif, bila diperlukan, untuk mencegah terulangnya insiden.
d. Komunikasi dengan pihak-pihak yang terpengaruh atau terlibat dalam pemulihan dari insiden.
e. Pelaporan tindakan yang dilakukan kepada pihak yang berwenang.
f. Analisa bukti permasalahan secara internal.
g. Bukti audit dapat digunakan sebagai bukti forensik untuk mencari potensi pelanggaran kontrak, regulasi atau digunakan sebagai bukti dalam proses hukum.
h. Tuntutan ganti rugi kepada pihak terkait.

6. Respons terhadap insiden keamanan informasi, meliputi:
   a. Setelah insiden terjadi, semua bukti harus dicatat.
   b. Semua tanggapan atas insiden keamanan harus dicatat, karena mungkin diperlukan dimasa mendatang untuk tujuan analisis.
   c. Menentukan akar penyebab insiden keamanan informasi.
   d. Setelah semua tindakan yang diperlukan diambil pada insiden tersebut, statusnya harus berubah menjadi ditutup dan semua detail harus dicatat.
7. Tindakan pemulihan dari pelanggaran keamanan serta mengoreksi kegagalan sistem harus dikendalikan secara formal dan secara hati-hati untuk menjamin:
   a. Hanya orang yang berwenang yang mengakses data dan sistem yang berjalan.
   b. Seluruh tindakan darurat terdokumentasi dengan baik dan detail;
   c. Tindakan darurat dilaporkan kepada manajemen dan ditinjau dengan semestinya.
   d. Konfirmasi mengenai integritas sistem bisnis dan proses pengendaliannya dengan cepat.
8. Unit terkait diwajibkan untuk menganalisis seluruh data yang dikumpulkan selama evaluasi insiden keamanan informasi untuk mengidentifikasi kontrol keamanan yang tepat untuk diimplementasikan dalam rangka meminimalkan kemungkinan terjadinya kejadian serupa dan dampak insiden keamanan informasi.
9. Unit terkait diwajibkan untuk membuat ketentuan guna melindungi dan menyimpan informasi secara aman, dengan tujuan agar informasi tersebut dapat difungsikan sebagai bukti potensial. Unit terkait juga diwajibkan untuk melakukan pemantauan terhadap akses terhadap bukti, guna mencegah perubahan atau penghapusan bukti oleh pihak yang tidak berwenang.

2.13 Keamanan Informasi dari Aspek Manajemen Kelangsungan Organisasi

Keamanan informasi dari aspek manajemen kelangsungan organisasi bertujuan untuk memastikan ketersediaan fasilitas pemrosesan informasi. Hal ini dapat dilakukan dengan membangun sistem manajemen kelangsungan organisasi yang kuat. Sistem ini harus memastikan bahwa sistem dan alat tersedia dan berfungsi selama situasi darurat. Situasi darurat dapat mencakup namun tidak terbatas pada kebakaran, pemadaman listrik, banjir, serangan peretas, gempa bumi, huru-hara, dan situasi darurat negara.

A. Kebijakan

1. Kesinambungan Keamanan Informasi
   a. Unit terkait diwajibkan untuk dapat mengelola keberlangsungan kegiatan pada saat keadaan darurat.
   b. Unit terkait diwajibkan untuk menentukan persyaratan keamanan informasi dan kesinambungan manajemen keamanan informasi dalam situasi darurat.
   c. Unit terkait diwajibkan untuk melakukan penilaian risiko dan analisis dampak terhadap organisasi dari situasi darurat.
   d. Unit terkait diwajibkan untuk menetapkan, mendokumentasikan, menerapkan, dan memelihara proses, prosedur, dan kontrol guna memastikan tingkat kontinuitas yang diperlukan untuk keamanan informasi selama situasi darurat.
   e. Unit terkait diwajibkan untuk memverifikasi kontrol kesinambungan keamanan informasi yang telah ditetapkan dan diterapkan secara berkala, guna memastikan bahwa kontrol tersebut masih sesuai dan efektif digunakan selama situasi darurat.
2. Ketersediaan cadangan
   a. Unit terkait diwajibkan untuk mengimplementasikan fasilitas pemrosesan informasi dengan cadangan yang cukup, guna memenuhi persyaratan ketersediaan.
   b. Unit terkait diwajibkan untuk memastikan bahwa sistem dan alat penting organisasi tetap aktif dan beroperasi selama situasi darurat untuk mendukung kelancaran operasi organisasi.

B. Standar

1. Kesinambungan Keamanan Informasi
   a. Perencanaan Kesinambungan Keamanan Informasi mencakup :
      1) Prosedur saat situasi darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak-pihak berwenang;

2) Prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang berlaku;
3) Prosedur saat kondisi telah normal, adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
4) Prosedur uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya;
5) Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
6) Tanggungjawab dan peran serta setiap petugas pelaksanaan pengelolaan proses kelangsungan;
7) Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat situasi darurat, *fallback* dan saat telah normal kembali.

b. Menerapkan kesinambungan keamanan informasi mencakup:
1) Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
2) Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;
3) Identifikasi sumber daya mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;
4) Memastikan keselamatan pegawai dan perlindungan terhadap perangkat pengolah informasi dan aset;
5) Penyusunan dan pendokumentasian rencana kelangsungan kegiatan harus disesuaikan dengan Rencana Strategis;
6) Pelaksanaan uji coba dan pemeliharaan rencana kelangsungan kegiatan secara berkala;
7) Bila memungkinkan menggunakan jasa asuransi sebagai bagian dari proses kelangsungan bisnis dan manajemen risiko operasional secara keseluruhan;
8) Mengintegrasikan pengelolaan kelangsungan bisnis dengan proses dan struktur organisasi.

c. Kesinambungan keamanan informasi dilaksanakan dengan:
1) Meninjau dan memeriksa apakah ada perubahan operasional dalam organisasi yang memerlukan perencanaan dan prosedur kelangsungan organisasi untuk diubah;
2) Ujicoba pemulihan (*recovery)* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;

3) Ujicoba *recovery* sistem informasi menggunakan fasilitas pada lokasi alternatif. Dilakukan dengan menjalankan proses organisasi pada lokasi utama secara paralel dengan proses organisasi pada fasilitas *recovery* pada lokasi alternatif;
4) Ujicoba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga;
5) Uji coba prosedur, alat, teknologi, infrastruktur, dan lain-lain secara keseluruhan untuk memastikan semuanya mutakhir, relevan, dan cukup untuk membantu organisasi.

2. Ketersediaan Cadangan
   a. Server cadangan kedua harus direncanakan yang berfungsi jika terjadi kegagalan pada server utama atau pada saat server kritis;
   b. Memastikan bahwa tidak terdapat kehilangan data informasi selama beberapa detik perpindahan server ke server cadangan; (Formulir 19)
   c. Penting untuk melakukan ujicoba *server* cadangan secara terencana untuk memastikan sistem bekerja seperti yang diharapkan.

2.14 Kepatuhan

Bertujuan untuk menghindari pelanggaran terhadap hukum, undang-undang, peraturan, atau kontrak yang terkait dengan keamanan informasi. Organisasi diwajibkan untuk melindungi diri dengan mematuhi hukum dan/atau kewajiban yang disebutkan sebagai bagian dari kontrak dan perjanjian yang berkaitan dengan persyaratan keamanan informasi.

A. Kebijakan

1. Kepatuhan terhadap Peraturan Perundangan dan Kontrak yang terkait keamanan informasi.
   a. Diwajibkan bagi semua unsur pegawai dan pihak ketiga untuk mentaati peraturan perundangan yang berlaku terkait keamanan informasi.
   b. Unit terkait diwajibkan untuk mengidentifikasi, mendokumentasikan dan memperbarui secara eksplisit semua persyaratan perundang-undangan, peraturan, kontrak, dan ketentuan organisasi yang terkait dengan sistem informasi.
   c. Unit terkait diwajibkan untuk melindungi informasi, perangkat lunak, alat, kode sumber, atau materi lain yang dapat dianggap sebagai kekayaan intelektualnya. Dilarang melakukan penggandaan terhadap informasi, perangkat lunak, alat, kode sumber, atau materi lain yang dapat dianggap sebagai kekayaan intelektual organisasi secara tidak sah dan merupakan bentuk pelanggaran.

d. Unit terkait diwajibkan untuk mematuhi ketentuan penggunaan lisensi terhadap perangkat lunak yang dikelolanya. Dilarang melakukan pengadaan perangkat lunak secara tidak sah dan merupakan bentuk pelanggaran.
e. Unit terkait diwajibkan untuk melindungi catatan atau rekaman dari kehilangan, kehancuran, pemalsuan, akses tidak sah, dan pelepasan tidak sah, sesuai dengan persyaratan perundangan, peraturan dan kontrak.
f. Unit terkait diwajibkan untuk memastikan privasi dan perlindungan informasi pribadi sesuai dengan persyaratan undang-undang dan peraturan yang berlaku.
g. Unit terkait diwajibkan untuk menggunakan kontrol kriptografi sesuai dengan semua perjanjian, undang-undang, dan peraturan yang relevan.

2. Ulasan Keamanan Informasi
   a. Unit terkait diwajibkan untuk meninjau secara independen pengelolaan dan penerapan keamanan informasi pada interval yang direncanakan atau ketika terjadi perubahan signifikan.
   b. Unit terkait diwajibkan untuk membuat perencanaan, persyaratan dan ruang lingkup dalam proses audit sistem operasional, guna mengurangi kemungkinan risiko gangguan yang dapat terjadi selama proses audit.
   c. Unit terkait melarang penggunaan alat bantu (*tools*), baik perangkat lunak maupun perangkat keras, untuk mengetahui kelemahan keamanan, memindai kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi.
   d. Unit terkait diwajibkan untuk melakukan tinjauan kepatuhan teknis terhadap standar dan prosedur keamanan informasi di area operasional secara berkala guna memastikan efektivitasnya.

B. Standar

1. Kepatuhan terhadap Peraturan Perundangan dan Kontrak yang Terkait Keamanan Informasi
   a. Identifikasi Perundang-undangan yang berlaku dan Persyaratan Kontrak
      1) Mengidentifikasi dan mendokumentasikan semua undang-undang yang berlaku dan persyaratan kontrak yang harus dipatuhi; (Formulir 28)
      2) Mengidentifikasi dan revisi dokumen terhadap perubahan undang-undang dan atau kewajiban kontrak. (Fomulir 01)
   b. Hak Kekayaan Intelektual
      1) Menyebutkan dalam kontrak atau surat kerja bahwa setiap pegawai harus melindungi hak kekayaan intelektual

organisasi dalam semua perjanjian bisnis atau perjanjian kerja yang dibuat dengan pihak ketiga atau pemasok;

2) Semua perangkat lunak atau perangkat keras yang dibeli yang dipasang dan digunakan di organisasi harus berlisensi dan sah untuk digunakan. Pemeriksaan terhadap kedaluwarsa lisensi dan kebutuhan pembaharuan dilakukan secara berkala; (Formulir 26)
3) Pembuatan kebijakan yang mengatur perlindungan terhadap hak atas kekayaan intelektual yang mencakup penggunaan perangkat lunak maupun informasi lainnya;
4) Memberikan pemberitahuan secara reguler terhadap seluruh pegawai terhadap kebijakan perlindungan hak atas kekayaan intelektual termasuk pemberitahuan mengenai sanksi yang akan diberikan bagi pegawai yang melanggar kebijakan tersebut;
5) Identifikasi aset yang memiliki kaitan dengan kebijakan perlindungan hak atas kekayaan intelektual;
6) Menyimpan bukti kepemilikan terhadap lisensi, *master disk*, serta manual perangkat lunak maupun informasi yang terkait dengan hak atas kekayaan intelektual;
7) Mengimplementasikan pengendalian untuk menjamin jumlah lisensi yang terpasang tidak melebihi jumlah lisensi yang dimiliki;
8) Melakukan pemeriksaan secara berkala dengan perangkat audit yang sesuai untuk menjamin hanya perangkat lunak yang diizinkan dan berlisensi saja yang terpasang;
9) Mematuhi seluruh syarat dan prasyarat dari lisensi perangkat lunak atau informasi yang dimiliki;
10) Tidak melakukan proses duplikasi atau perubahan format dari perangkat lunak atau informasi dan data lainnya sesuai dengan hukum hak atas kekayaan intelektual.

c. Perlindungan Catatan
   1) Membuat kebijakan dan prosedur penyimpanan data;
   2) Mententukan periode penyimpanan data untuk setiap jenis informasi, data dan rekaman;
   3) Mententukan aturan penyimpanan data yaitu kertas, *file* dan media elektronik;
   4) Menentukan aturan pengelolaan akses ke informasi yang disimpan;
   5) Menentukan aturan pemusnahan dokumen/data setelah periode penyimpanan data berakhir.
d. Privasi dan Perlindungan Informasi Identitas Pribadi
   1) Membuat kebijakan dan prosedur untuk diikuti oleh pemangku kepentingan;

2) Setiap pegawai atau pihak ketiga dapat memperoleh persetujuan tertulis untuk menyimpan informasi, dengan mengisi formulir yang berisi rincian informasi yang akan disimpan, jangka waktu, dan tujuan penyimpanan; (*Formulir 29*)
3) Menempatkan pesan permintaan di situs web agar setiap pengunjung diberitahukan informasi *cookie,* serta diberi opsi untuk menerima atau menolak permintaan ini;
4) Formulir apa pun yang diisi secara *online* di situs web dan menyimpan informasi pribadi harus mendapatkan persetujuan;
5) Persetujuan dari pihak ketiga dan pemasok dapat melalui kontrak atau perjanjian;
6) Memasang kontrol untuk melindungi informasi yang disimpan;
7) Membuat aturan tatacara permintaan penghapusan data pribadi mereka.

e. Regulasi Kontrol Kriptografi
1) Larangan untuk mengimpor dan atau mengekspor perangkat keras dan lunak yang memiliki fungsi pemrosesan kriptografi;
2) Larangan untuk mengimpor dan atau mengekspor perangkat keras dan lunak yang memiliki fungsi tambahan kriptografi;
3) Memberikan akses kepada pihak berwenang negara terhadap informasi yang dienkripsi.

2. Ulasan Keamanan Informasi
a. Tinjauan independen keamanan informasi
1) Merencanakan audit independen secara berkala untuk memastikan bahwa sistem manajemen keamanan informasi sudah sesuai dengan yang direncanakan;
2) Audit dapat dilakukan oleh lembaga eksternal yang terampil dan berpengalaman;
3) Audit juga dapat dilakukan oleh tim internal, namun auditor harus berasal dari area atau departemen yang berbeda sehingga tidak ada bias saat melakukan audit;
4) Hasil audit harus dipresentasikan kepada manajemen untuk penyadaran dan perbaikan.

b. Pengendalian terhadap Audit Sistem Informasi
1) Persyaratan audit perlu disetujui dengan pihak manajemen yang terkait;
2) Ruang lingkup audit harus disepakati dan dikontrol;
3) Hak akses untuk pemeriksaan audit terhadap data dan aplikasi perlu dibatasi dengan akses *read only;*

4) Hak akses selain *read only* hanya dibolehkan untuk salinan dari *file* yang terbatas dan terisolasi. Salinan tersebut perlu segera dihapus setelah proses audit selesai atau diberikan perlindungan yang memadai apabila ada kebutuhan untuk mendokumentasikan salinan dari *file* tersebut;
5) Sumber daya yang dibutuhkan untuk melakukan audit harus diidentifikasi dan kemudian disediakan;
6) Kebutuhan untuk melakukan pemrosesan khusus maupun tambahan perlu diidentifikasi dan disepakati;
7) Seluruh akses ke sistem informasi harus dimonitor dan dicatat (*log*) untuk menghasilkan jejak referensi (*reference trail*). Penggunaan penanda waktu (*timestamp*) perlu dipertimbangkan untuk *reference trail* dari data atau sistem yang kritikal;
8) Seluruh prosedur, persyaratan dan tanggung jawab proses audit sistem informasi harus didokumentasi;
9) Pelaksana audit harus memiliki independensi dari aktivitas yang diaudit.

c. Kepatuhan terhadap kebijakan dan standar keamanan
1) Menentukan dan mengevaluasi penyebab ketidakpatuhan;
2) Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang lagi;
3) Mengkaji tindakan perbaikan yang dilakukan.

d. Tinjauan Kepatuhan Teknis
Sistem informasi diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan. (Formulir 30)

BAB III
PENUTUP

Dokumen Sistem Manajemen Keamanan Informasi (SMKI) ini ditetapkan sebagai pedoman dalam melindungi aset informasi pada lingkup pemerintahan dari berbagai bentuk ancaman, baik yang bersumber dari dalam maupun dari luar, dengan tujuan menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi. Dokumen SMKI ini dilengkapi pula dengan formulir kontrol sebagai panduan pendokumentasian kegiatan pengendalian keamanan informasi pada aspek terkait.

Hal-hal bersifat teknis dan spesifik yang belum diatur dalam dokumen SMKI ini, secara khusus akan diatur dalam dokumen atau standar operasional prosedur terpisah. Selain itu untuk menjaga kemutakhirannya, dokumen SMKI ini akan ditinjau sekurang-kurangnya sekali dalam setahun.

LAMPIRAN

Formulir 01 Revisi Dokumen

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	RIWAYAT PERUBAHAN DOKUMEN	No. Rev	00
		Tgl	
		Hal	

No. Rev	Tanggal Revisi	Nama Dokumen	Nomor Dokumen	Uraian Perubahan
00				
01				
02				
03				

Formulir 02 Daftar Distribusi Dokumen

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	DAFTAR DISTRIBUSI DOKUMEN	No. Rev	00
		Tgl	
		Hal	

NO	Nama Dokumen	Penanggung Jawab - Departemen	TTD

Formulir 03 Rangkuman, Rencana & Verifikasi Perbaikan Hasil Audit Internal

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	FORM RANGKUMAN, RENCANA, & VERIFIKASI PERBAIKAN HASIL AUDIT INTERNAL	No. Rev	00
		Tgl	
		Hal	

Auditee		Ketidaksesuaian			Rencana Tindakan Perbaikan	
No	Departemen	Deskripsi	Klausal	Kategori	Akar Masalah	Rencana Tindakan Perbaikan

Formulir 04 Rencana Audit Internal

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	FORM RENCANA AUDIT INTERNAL	No. Rev	00
		Tgl	
		Hal	

Auditor		Auditee		Detil Audit		
Nama	Departemen	Nama	Departemen	Tanggal	Jam	Lokasi

Formulir 05 Rekapitulasi Temuan Audit Internal

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	REKAPITULASI TEMUAN AUDIT INTERNAL	No. Rev	00
		Tgl	
		Hal	

Bidang (yang diaudit)	Ketidaksesuaian	Kategori			Status		Proses
		Major	Minor	Obs	Open	Closed	

Formulir 06 Logbook Insiden Keamanan Informasi

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	LOGBOOK INSIDEN KEAMANAN INFORMASI	No. Rev	00
		Tgl	
		Hal	

Nomor Keamanan Insiden	Tanggal Laporan	Penanggung jawab	Pemasalahan

Formulir 07 Laporan Insiden Keamanan Informasi

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	LAPORAN INSIDEN KEAMANAN INFORMASI	No. Rev	00
		Tgl	
		Hal	

No. Laporan Insiden Keamanan Informasi: .....

Tujuan Pelaporan :

☐ Kelemahan (Vulnerability) ☐ Insiden

☐ Simulasi Kelemahan ☐ Simulasi Insiden

Petunjuk :

1. *Isilah semua data secara lengkap*
2. *Pelapor mengisi A dan B secara jelas*
3. *Kirim formulir ke Departemen TI untuk di proses*
4. *MR dan TIM mengisi kolom C dan D sebagai tindak lanjut hasil pelaporan*

A. DATA PEMOHON	
Nama Lengkap	:
NIK	:
Departemen/Bagian	:

B. URAIAN INSIDEN / KELEMAHAN SISTEM TI	
Waktu dan Tanggal Insiden :	
Lokasi Indisen	:
Jenis insiden / Kelemahan	:

Formulir 08 Penilaian/Evaluasi Pihak Ketiga atau Pemasok

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	EVALUASI PEMASOK	No. Rev	00
		Tgl	
		Hal	

Dikeluarkan Oleh	Penanggung Jawab	Tanggal	Halaman

PEMASOK : PERIODE :

PRODUK :

NO	FAKTOR KEAMANAN INFORMASI YANG DINILAI	NILAI 4	3	2	1	HASIL PENILAIAN
A	_____					
B	_____					
C	_____					
D	_____					
E	_____					
	TOAL NILAI					

Catatan:	NILAI	Manokwari ,……..
Pemasok masuk kategori OK/Bagus ……. Jumlah nilai minimal 12 dan ……	1 : KURANG BAIK 2 : CUKUP BAIK 3 : BAIK 4 : SANGAT BAIK	Mengetahui ( )

Formulir 09 Permohonan User/Hak Akses Sistem/Aplikasi

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PERMOHONAN USER/ HAK AKSES SISTEM/APLIKASI	No. Rev	00
		Tgl	
		Hal	

Pemohon :	Tanggal :
Unit Kerja :	Email :
Telpon :	

Permintaan : ☐ Pendaftaran ☐ Penghapusan ☐ Perubahan

Jenis Akses : ☐ E-mail ☐Internet ☐ Aplikasi ☐ Sistem/OS ☐ Sharing ☐ Lainnya

Dengan memenuhi ketentuan dan syarat berikut :

- Keperluan dan Alasan Akses:

  _____

- Kolom dibawah ini diisi hanya untuk pengajuan Aplikasi System.

NO	LAYANAN	JENIS	LEVEL HAK AKSES
			1/2/3

*note : 1 - admin, 2 - manager, 3 - user (Disesuaikan konteks organisasi)

- Sifat Akses : ☐ Rutin ☐ Sementara ☐ Permanen
- Waktu Akses : ☐ 7 x 24 Jam ☐ 08.00 – 16 (Hari Kerja) ☐ Lainnya
- Masa Berlaku Akses sampai dengan : _____
- Ketentuan Akses :
  1. User menyetujui dan mematuhi kebijakan keamanan informasi, kebijakan pengamanan sistem/aplikasi prosedur terkait;
  2. User dilarang mengalihkan dan/atau meminjamkan hak akses kepada pihak lain;
  3. User dilarang menyalahgunakan akses untuk kepentingan selain penugasan yang telah di tetapkan;
  4. User harus memberitahukan dan mengembalikan hak akses kepada atasannya/penganggung jawab hak akses, apabila sudah tidak lagi berkerja dibidang yang menjadi dasar pemberian hak akses;
  5. Pelanggaran terhadap pengamanan sistem/aplikasi dan prosedur terkait akan menyebabkan pecabutan hak akses, tidak disiplin, atau sanki sesuai peraturan yang berlaku.

"Saya meneyetujui dan bersedia mematuhi ketentuan ini. Saya akan menggunakan hak akses ke sistem/aplikasi sesuai tugas dan pekerjaan saya dan akan melaporkan setiap masalah atau insiden keamanan informasi yang saya ketahui"

Atasan Pemohon, ( )	Pemohon, ( )
Mengetahui, ( )	Pelaksana Teknis ( )

Alasan Penolakan:_____

Formulir 10 Penyimpanan Aset Informasi

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PENYIMPANAN ASET INFORMASI	No. Rev	00
		Tgl	
		Hal	

a. Umum

Penanggung Jawab : _____

Jabatan : _____

Tanggal : _____

b. Detail Aset Informasi

Isilah tabel berikut membantu unutk memastikan bahwa aset informasi Anda disimpan dengan aman dan terlindungi dari akses yang tidak sah, pencurian, dan kerusakan.

Jenis Aset Informasi	Lokasi Penyimpanan	Pengendalian Akses	Prosedur Pencadangan	Komentar
Dokumen	Kabinet terkunci di departemen keuangan	Kunci fisik, kata sandi	Dicadangkan setiap hari ke server internal	
Perangkat Lunak	Server internal	Enkripsi, kata sandi yang kuat	Dicadangkan setiap minggu ke server eksternal	
Perangkat Keras	Gudang yang aman	Kunci fisik, kamera keamanan	Dicadangkan setiap bulan ke layanan penyimpanan awan (cloud)	

c. Tanda Tangan

( )

Formulir 11 Penggunaan dan Pembagian Aset Informasi

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PENGGUNAAN DAN PEMBAGIAN ASET INFORMASI	No. Rev	00
		Tgl	
		Hal	

Jenis Aset Informasi	Nama Aset Informasi	Pengguna Aset Informasi	Tujuan Penggunaan	Izin Akses	Tanggal Penggunaan	Komentar
Dokumen	Kebijakan Keamanan Informasi	Semua karyawan	Membaca dan memahami	Baca	2024-07-16	
Perangkat Lunak	Antivirus	Tim TI	Memasang dan memperbarui	Ubah	2024-07-16	
Perangkat Keras	Laptop	Departemen Penjualan	Digunakan untuk presentasi dan pelacakan klien	Baca, tulis	2024-07-16	

Formulir 12 Pengembalian Aset

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	FORM PENGEMBALIAN ASET	No. Rev	00
		Tgl	
		Hal	

A. Informasi Umum

1. Nama Karyawan : _____
2. Jabatan : _____
3. Departemen : _____
4. Tanggal Pengembalian : _____

B. Detail Aset

No	Nama Aset	Nomor Seri	Kondisi	Ket
1				
2				
3				

Mengembalikan Penerima

( ) ( )

Formulir 13 Berita Acara Pemusnahan Dokumen dan Perangkat

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	FORM BERITA ACARA PEMUSNAHAN DOKUMEN/PERANGKAT	No. Rev	00
		Tgl	
		Hal	

No	Nama Dokumen/ Perangkat	No. Dokumen /Perangkat	Masa Simpan	Tanggal Pemusnahan	Dept. / PIC	Ket

Formulir 14 Hak Akses Pengguna

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	HAK AKSES PENGGUNA	No. Rev	00
		Tgl	
		Hal	

NO	STRUKTUR FOLDER	NO	NAMA FOLDER	NAMA USER	HAK AKSES			
					R	W	D	E

Formulir 15 Struktur Folder Untuk Akses Pengguna

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	STRUKTUR FOLDER UNTUK AKSES PENGGUNA	No. Rev	00
		Tgl	
		Hal	

Formulir 16 Visitor Log Book Secure Area

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	VISITOR LOG BOOK SECURE AREA	No. Rev	00
		Tgl	
		Hal	

NUMBER (NOMOR ID)	COMPANY NAME (if any) (NAMA PERUSAHAAN)	*NAME OF PERSON BEING VISITED* (NAMA PEJABAT YANG DIKUNJUNGI)	*AREA* (AREA)	*PURPOSE VISIT* (MAKSUD KEDATANGAN)	*VISITOR BADGE NUMBER* (NOMOR ID PENGUNJUNG)	*ARRIVAL TIME* (JAM DATANG)	*DEPAR. TIME* (JAM KELUAR)	VISITOR (TAMU)

Formulir 17 Permohonan Peminjaman Fasilitas TI

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PERMOHONAN PEMINJAMAN FASILITAS TI	No. Rev	00
		Tgl	
		Hal	

Instruksi:
1. Isilah semua data secara lengkap
2. Mintalah persetujuan Atasan di kolom C
3. Kirim Formulir ke Departemen TI untuk diproses

A. DATA PEMOHON	
Nama Lengkap	:
NIK	:
Departemen	:
Bagian	:
Alasan Peminjaman	:
Rencana Peminjaman	: … s.d …

B. FASILITAS

☐Flashdisk : _____
☐PC/Laptop : _____
☐Printer : _____
☐Modem : _____
☐Other : _____

Tolong tulis spesifikasi seperti : Brand / Type / Serial No. / ID (jika ada) disamping jenis fasilitas.

C. PERMINTAAN DAN PERSETUJUAN ATASAN LANGSUNG

_____
PIMPINAN

Formulir 18 Laporan Kerusakan Dan Perbaikan Perangkat Teknologi Informasi

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	LAPORAN KERUSAKAN DAN PERBAIKAN PERANGKAT TEKNOLOGI INFORMASI	No. Rev	00
		Tgl	
		Hal	

No. Laporan : ……

Auditee : …… Auditor : …… **Deskripsi Permasalahan (***oleh Pelapor***)** …… …… …… ……	☐Hasil Audit ☐Tinjauan Manager
Analisis (*oleh Pelaksana Perbaikan***)** …… …… …… ……	

Tindakan Perbaikan	**Tindakan Pencegahan**
…… …… …… …… …… …… …… …… …… ……	…… …… …… …… …… …… …… …… …… ……

Formulir 19 Backup Checklist

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	BACKUP CHECKLIST	No. Rev	00
		Tgl	
		Hal	

Type of Backup : ☐daily ☐weekly ☐monthly
Media of Bakcup : ☐hard driver ☐CD ☐……..

NO	DATABASE BAKCUP	CHECK	STATUS (OK/NOT OK)	REMARKS

Formulir 20 Prosedur Pengelolaan Keamanan Jaringan

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PROSEDUR PENGELOLAAN KEAMANAN JARINGAN	No. Rev	00
		Tgl	
		Hal	

Catatan Revisi

REV	DESKRIPSI REVISI	PEMBUAT	TANGGAL

Catatan Pengesahan Dokumen

REV	TAHAP	NAMA & JABATAN	TANDA TANGAN	TANGGAL
	Dibuat oleh:			
	Diperiksa oleh:			
	Disahkan oleh:			

Formulir 21 Komunikasi Eksternal

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	KOMUNIKASI EKSTERNAL	No. Rev	00
		Tgl	
		Hal	

Nama Pelanggan		
Media Komunikasi	☐Telp ☐Fax ☐E-Mail ☐Surat lain-lain, TV, Web dll _____ ☐Kunjungan Langsung * Lampiran Surat, Faks, E-mail dari pelanggan bila ada	
URAIAN PERMASALAHAN		
Sumber Informasi *Tulis sumber media pada nama	Nama : _____ No KTP : _____ TGL/Jam : _____	Tanda Tangan
	Manokwari, ……..	
Dibuat Oleh _____	Diketahui Oleh _____	

Formulir 22 Komunikasi Internal

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	KOMUNIKASI INTERNAL	No. Rev	00
		Tgl	
		Hal	

☐Pelatihan	☐Rapat	☐Pertemuan	☐……
Tanggal : Tempat : Waktu :			
Materi :			
Hasil/Saran/Kesimpulan :			

Mengetahui,

_____

Formulir 23 Log Book Kerusakan Dan Perbaikan Perangkat Teknologi Informasi

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	LOG BOOK KERUSAKAN DAN PERBAIKAN PERANGKAT TEKNOLOGI INFORMASI	No. Rev	00
		Tgl	
		Hal	

No	Nomor Laporan	Tanggal terbit	Penanggung jawab	Permasalahan
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
Note:				

Formulir 24 Permintaan Perubahan

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PERMINTAAN PERUBAHAN	No. Rev	00
		Tgl	
		Hal	

INSTRUKSI :

1. Isilah semua data secara lengkap
2. Pelapor mengisi kolom A, B dan C secara jelas
3. Kirim Formulir ke Departemen TI untuk di proses
4. Pengajuan dan Pengesahan harus ditandatangani secara jelas pada kolom D.

A. DATA PEMOHON			
Nama Lengkap : _____ NIK : _____ Departemen/Bagian : _____			
B. INFORMASI PERMINTAAN PERUBAHAN			
Sistem : _____ Alasan : _____ _____			
Jenis Perubahan	☐Pengembangan	☐Rencana Manajemen	☐Insiden
Tanggal Permintaan :			
Uraian Perubahan : _____ _____			
Manokwari, …….. Pemohon ( )	Penerima Permintaan ( )	Mengetahui ( ) Pimpinan	

Formulir 25 Permohonan Pembuangan/Pemusnahan Aset

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PERMOHONAN PEMBUANGAN/PEMUSNAHAN ASET	No. Rev	00
		Tgl	
		Hal	

d. **Informasi Umum**

1. Nama Pemohon : _____
2. Jabatan : _____
3. Departemen : _____
4. Tanggal Permohonan : _____

e. **Detail Aset**

No	Nama Aset	Nomor Seri	Kondisi	Alasan Pembuangan/Pemusnahan
1				
2				
3				

f. **Alasan Pembuangan/Pemusnahan**

1. Apakah aset sudah tidak dapat digunakan lagi?
   - [ ] Ya
   - [ ] Tidak, jelaskan: _____
2. Apakah aset mengalami kerusakan yang tidak dapat diperbaiki?
   - [ ] Ya
   - [ ] Tidak, jelaskan: _____
3. Apakah aset sudah usang atau tidak sesuai dengan kebutuhan saat ini?
   - [ ] Ya
   - [ ] Tidak, jelaskan: _____

g. **Persetujuan**

1. Kepala Departemen: Nama: _____ Tanda Tangan: _____
2. Manajer IT: Nama: _____Tanda Tangan: _____
3. Kepala Bagian Aset: Nama: _____ Tanda Tangan: _____

h. **Tanda Tangan Pemohon**

Nama: _____ Tanda Tangan: _____

Formulir 26 Validasi/Evaluasi Kelayakan Produk IT

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	FORM VALIDASI/EVALUASI KELAYAKAN PRODUK IT	No. Rev	00
		Tgl	
		Hal	

A. Informasi Umum
   1. Nama Produk : _____
   2. Versi Produk : _____
   3. Tanggal Evaluasi : _____

B. Tujuan Evaluasi Instrumen ini digunakan untuk mengukur validitas dan kelayakan produk IT yang dikembangkan. Pendapat, kritik, saran, dan penilaian dari evaluator akan sangat bermanfaat untuk memperbaiki dan meningkatkan kualitas produk.

C. Petunjuk Pengisian
   1. Berikan penilaian dengan memberi tanda silang (X) pada skor yang sesuai.
   2. Berikan saran atau komentar pada kolom yang disediakan.

D. Kriteria Penilaian

No	*Kriteria*	*Skor*	*Saran/Komentar*
1	Kesesuaian dengan kebutuhan pengguna	1 2 3 4 5	
2	Kemudahan penggunaan (usability)	1 2 3 4 5	
3	Kinerja dan kecepatan	1 2 3 4 5	
4	Keamanan data	1 2 3 4 5	
5	Kompatibilitas dengan sistem lain	1 2 3 4 5	
6	Dokumentasi dan bantuan pengguna	1 2 3 4 5	
7	Desain antarmuka	1 2 3 4 5	
8	Fitur dan fungsionalitas	1 2 3 4 5	
9	Stabilitas dan reliabilitas	1 2 3 4 5	
10	Dukungan teknis	1 2 3 4 5	

E. Kesimpulan Berdasarkan penilaian di atas, produk IT ini dinyatakan:
   - [ ] Layak digunakan
   - [ ] Perlu perbaikan
   - [ ] Tidak layak digunakan

F. Tanda Tangan Evaluator

(<NAMA>)

Formulir 27 Post Incident review

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	POST INCIDENT REVIEW	No. Rev	00
		Tgl	
		Hal	

No	Review Items
1	Ringkasan Insiden
2	Akar Masalah Insiden
3	Apakah Business Continuity Plan berjalan dengan baik dan efektif?
4	Apakah Tim telah disiapkan dengan baik untuk menghadapi insiden?
5	Apakah sumber daya, equipment, dan sdm yang dibutuhkan tersedia?
6	Apakah komunikasi berjalan efektif? (komunikasi diantara individual departements, dengan management, crisis team, employees, suppliers, customers, pemerintahan, dan fungsi lain yang terkait)
7	Item apa yg berjalan dengan baik sesuai dengan rencana?

Formulir 28 Evaluasi Kesesuaian Persyaratan Dan Peraturan Perundungan

	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	EVALUASI KESESUAIAN PERSYARATAN DAN PERATURAN PERUNDANGAN	No. Rev	00
		Tgl	
		Hal	

NO	NAMA & PERATURAN	ISI PERATURAN (PASAL-PASAL TERKAIT)		KRITIKAL POINT	PATUH		KET	RENCANA
		PASAL	RINGKASAN		Y	N		
UNDANG-UNDANG								
KEPUTUSAN PRESIDEN								
KEPUTUSAN MENTERI								
PERSYARATAN LAIN								

Formulir 29 Permohonan Penyimpanan Informasi/Data

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	FORMULIR PERMOHONAN PENYIMPANAN INFORMASI/DATA	No. Rev	00
		Tgl	
		Hal	

No. Pendaftaran……(diisi petugas)

Nama :
Alamat :

No. Tlp :
Rincian Informasi yang disimpan :

Tujuan Penyimpanan Informasi:

Lama Penyimpanan (Tahun) :

Format Informasi : ☐ Tercetak
☐ File

Manokwari, ……..

Petugas Pelayanan Informasi
(Penerima Permohonan)

( )
Nama dan Tanda Tangan

Pemohon Informasi

( )
Nama dan Tanda Tangan

Mengetahui

( )
Pimpinan

Formulir 30 Prosedur Kesesuaian Terhadap Persyaratan

PAPUA BARAT	NAMA OPD/SATKER PEMERINTAH PROVINSI PAPUA BARAT	No. Dok	
	PROSEDUR KESESUAIAN TERHADAP PERSYARATAN	No. Rev	00
		Tgl	
		Hal	

Catatan Revisi

REV	DESKRIPSI REVISI	PEMBUAT	TANGGAL

Catatan Pengesahan Dokumen

REV	TAHAP	NAMA & JABATAN	TANDA TANGAN	TANGGAL
	Dibuat oleh:			
	Diperiksa oleh:			
	Disahkan oleh:			