PEMERINTAH KABUPATEN KENDAL
SEKRETARIAT DAERAH
Jl. Soekarno – Hatta No. 193 Kendal Telp. Fax. (0294) 381232 Kode Pos 51311
e-mail : setda@kendalkab.go.id website : setda.kendalkab.go.id

SEKRETARIS DAERAH KABUPATEN KENDAL

KEPUTUSAN SEKRETARIS DAERAH KABUPATEN KENDAL

NOMOR : 100.3.3.5/ 24 /2026

TENTANG

PENETAPAN PROSEDUR PENGENDALIAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL

SEKRETARIS DAERAH KABUPATEN KENDAL,

Menimbang :

a. bahwa dalam rangka mewujudkan jaminan keamanan informasi dalam Sistem Pemerintahan Berbasis Elektronik pada Pemerintah Kabupaten Kendal dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Pemerintah Kabupaten kendal, diperlukan prosedur pengendalian keamanan informasi sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Kendal sebagai panduan dalam pelaksanaannya;
b. bahwa dalam rangka meningkatkan efektifitas jaminan keamanan informasi prosedur pengendalian keamanan informasi sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Kendal yang telah ditetapkan dengan Keputusan Sekretaris Daerah Kabupaten Kendal Nomor : 360.2/128/2023 tanggal 9 Januari 2023 tentang Penetapan Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal dipandang sudah tidak sesuai dengan kondisi sekarang sehingga perlu dicabut dan diganti;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, maka perlu menetapkan Keputusan Sekretaris Daerah tentang Penetapan Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal;

Mengingat :

1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan Mengubah Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 52, Tambahan Lembaran Negara Republik Indonesia Nomor 2757);

2. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana (Lembaran Negara Republik Indonesia Tahun 2026 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 7153);
4. Peraturan Pemerintah Nomor 32 Tahun 1950 tentang Penetapan mulai Berlakunya Undang-Undang 1950 Nomor 12, 13, 14 dan 15 dari Hal Pembentukan Daerah-daerah Kabupaten di Jawa Timur/Tengah/Barat dan Daerah Istimewa Yogyakarta;
5. Peraturan Pemerintah Nomor 16 Tahun 1976 tentang Perluasan Kotamadya Daerah Tingkat II Semarang (Lembaran Negara Republik Indonesia Tahun 1976 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 3079);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 182, Tambahan Berita Negara Republik Indonesia Nomor 4843);
7. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Berita Negara Republik Indonesia Tahun 2022 Nomor 129);
8. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Berita Negara Republik Indonesia Tahun 2023 Nomor 99);
9. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);
10. Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2021 Nomor 35) sebagaimana telah diubah dengan Peraturan Bupati Kendal Nomor 33 Tahun 2024 tentang Perubahan Atas Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal Berita Daerah Kabupaten Kendal Tahun 2024 Nomor 34);
11. Peraturan Bupati Kendal Nomor 57 Tahun 2023 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2023 Nomor 57);

MEMUTUSKAN:

Menetapkan :

KESATU : Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan ini.

KEDUA : Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal sebagaimana dimaksud diktum KESATU digunakan sebagai pedoman atau standar dalam rangka melindungi aset informasi dan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Kendal dari berbagai bentuk ancaman baik dari dalam maupun dari luar lingkungan Pemerintah Kabupaten Kendal dengan tujuan untuk menjamin kerahasiaan, keutuhan, ketersediaan, autentifikasi dan kenirsangkalan aset informasi.

KETIGA : Pada saat Keputusan ini mulai berlaku, maka Keputusan Sekretaris Daerah Kabupaten Kendal Nomor : 360.2/128/2023 tanggal 9 Januari 2023 tentang Penetapan Prosedur Pengendalian Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kendal dicabut dan dinyatakan tidak berlaku.

KEEMPAT : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Kendal
pada tanggal 3 Juni 2026

SEKRETARIS DAERAH
KABUPATEN KENDAL,

AGUS DWI LESTARI

SALINAN : Keputusan ini disampaikan kepada Yth :
1. Segenap Agen Siber yang bersangkutan; dan
2. Arsip.

LAMPIRAN
KEPUTUSAN SEKRETARIS DAERAH
KABUPATEN KENDAL
NOMOR : 100.3.3.5 / 24 / 2026
TANGGAL : 3 JUNI 2026

PROSEDUR PENGENDALIAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL

DAFTAR ISI

DAFTAR ISTILAH

Istilah/Singkatan	Definisi
ACL	*Access Control List* — daftar aturan yang mengendalikan lalu lintas jaringan pada perangkat *router*/*switch*.
Anonimisasi	Proses menghilangkan identitas dari data sehingga tidak dapat dikaitkan kembali dengan individu.
ATS	*Automatic Transfer Switch* — perangkat peralihan otomatis suplai daya dari sumber utama ke cadangan.
Baseline	Konfigurasi standar minimum yang ditetapkan sebagai acuan.
BCP	*Business Continuity Plan* — rencana kelangsungan bisnis.
BIA	*Business Impact Analysis* — analisis dampak bisnis.
BSSN	Badan Siber dan Sandi Negara.
BSrE	Balai Sertifikasi Elektronik — penyelenggara sertifikat elektronik untuk TTE pemerintah.
BYOD	*Bring Your Own Device* — penggunaan perangkat pribadi untuk keperluan dinas.
CAB	*Change Advisory Board* — dewan penasihat perubahan.
CIS	*Center for Internet Security* — organisasi penyedia benchmark konfigurasi keamanan.
CMDB	*Configuration Management Database* — basis data manajemen konfigurasi.
CSIRT	*Computer Security Incident Response Team*.
CVSS	*Common Vulnerability Scoring System* — sistem penilaian tingkat keparahan kerentanan.
DDoS	*Distributed Denial of Service* — serangan penolakan layanan terdistribusi.
Degaussing	Proses penghapusan data dengan menghilangkan medan magnet pada media penyimpanan.
DRP	*Disaster Recovery Plan* — rencana pemulihan bencana.
E2E	*End-to-End* — enkripsi dari pengirim hingga penerima.
Failover	Peralihan otomatis ke sistem cadangan saat terjadi kegagalan.
Hashing	Proses konversi data menjadi nilai *hash* tetap yang tidak dapat dikembalikan ke bentuk asli.
IDS/IPS	*Intrusion Detection*/*Prevention System* — sistem deteksi dan pencegahan intrusi.
ISP	*Internet Service Provider* — penyedia layanan internet.
KAK	Kerangka Acuan Kerja.
LAN	*Local Area Network* – Jaringan Lokal
MFA	*Multi-Factor Authentication* — autentikasi multi-faktor.
NAC	*Network Access Control* — pengendalian akses jaringan.
NDA	*Non-Disclosure Agreement* — perjanjian kerahasiaan.
NIST	*National Institute of Standards and Technology*.
NTP	Network Time Protocol — protokol sinkronisasi waktu.
OPD	Organisasi Perangkat Daerah.
OWASP	*Open Worldwide Application Security Project*.
PDP	Pelindungan Data Pribadi (UU No. 27 Tahun 2022).
Pentest	*Penetration Testing* — pengujian penetrasi/simulasi serangan.
Pseudonimisasi	Penggantian identitas dengan identitas semu, dengan kunci konversi yang disimpan terpisah.

RBAC	*Role-Based Access Control* — pengendalian akses berbasis peran.
RFC	*Request for Change* — permintaan perubahan.
RPO	*Recovery Point Objective* — titik waktu terakhir data yang dapat diterima hilang.
RTO	*Recovery Time Objective* — waktu maksimum pemulihan.
Sanitasi	Proses penghapusan data secara permanen dan tidak dapat dipulihkan.
SAST	*Static Application Security Testing* — pengujian keamanan kode secara statis.
SBOM	*Software Bill of Materials* — daftar komponen perangkat lunak pihak ketiga.
SDLC	*Software Development Life Cycle* — siklus hidup pengembangan perangkat lunak.
SLA	*Service Level Agreement* — perjanjian tingkat layanan.
SMKI	Sistem Manajemen Keamanan Informasi.
SPBE	Sistem Pemerintahan Berbasis Elektronik.
TIK	Teknologi Informasi dan Komunikasi.
TLS	*Transport Layer Security* — protokol enkripsi transmisi.
TTE	Tanda Tangan Elektronik.
UPS	*Uninterruptible Power Supply* — catu daya tak terputus.
VA	*Vulnerability Assessment* — penilaian kerentanan.
VLAN	*Virtual Local Area Network* — jaringan lokal virtual.
VPN	*Virtual Private Network* — jaringan privat virtual.
XSS	*Cross-Site Scripting* — serangan injeksi skrip.

BAB I
PENDAHULUAN

A. Maksud dan Tujuan

Dokumen ini dimaksudkan untuk memberikan panduan teknis operasional yang terstruktur, terukur, dan dapat diaudit bagi seluruh OPD di lingkungan Pemerintah Kabupaten Kendal dalam mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan persyaratan ISO/IEC 27001:2022 dan ketentuan Peraturan Bupati Kendal Nomor 57 Tahun 2023.

Prosedur Pengendalian Keamanan Informasi bertujuan untuk:

1. Menetapkan kerangka manajemen risiko keamanan informasi yang sistematis sebagai landasan pengambilan keputusan pengendalian di seluruh OPD Pemerintah Kabupaten Kendal;
2. Menetapkan prosedur teknis operasional untuk setiap kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022 Annex A yang relevan dengan konteks, aset, dan regulasi Pemerintah Kabupaten Kendal;
3. Memberikan panduan ketentuan yang jelas, terstruktur, dan dapat diimplementasikan oleh seluruh OPD sebagai bukti pelaksanaan kontrol keamanan informasi yang dapat diverifikasi pada saat audit;
4. Mendukung kepatuhan Pemerintah Kabupaten Kendal terhadap kewajiban perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi;
5. Memperkuat ketahanan siber infrastruktur TIK dan layanan elektronik Pemerintah Kabupaten Kendal guna menjamin keberlangsungan layanan publik yang andal dan terpercaya;
6. Menyediakan pedoman yang berlaku seragam bagi seluruh OPD agar implementasi keamanan informasi dapat dilaksanakan secara mandiri, konsisten, dan sesuai dengan standar ISO/IEC 27001:2022.

B. Ruang Lingkup

Dokumen ini berlaku untuk:

1. Organisasi: Seluruh 57 (lima puluh tujuh) Organisasi Perangkat Daerah (OPD) di lingkungan Pemerintah Kabupaten Kendal, termasuk Sekretariat Daerah, Sekretariat DPRD, Dinas, Badan, Inspektorat, Kecamatan, dan unit kerja lain yang berada di bawah Pemerintah Kabupaten Kendal.
2. Sumber Daya Manusia:
   a. Seluruh Aparatur Sipil Negara (ASN) yang bertugas di lingkungan Pemerintah Kabupaten Kendal;
   b. Pejabat fungsional dan struktural yang memiliki akses terhadap sistem informasi dan/atau aset informasi Pemerintah Kabupaten Kendal;
   c. Tenaga kontrak, mitra kerja, konsultan, dan pihak ketiga lainnya yang diberikan hak akses terhadap sistem informasi atau infrastruktur TIK Pemerintah Kabupaten Kendal, sepanjang hal tersebut diatur dalam perjanjian kerja sama atau kontrak yang berlaku.
3. Sistem Informasi dan Aplikasi: Seluruh sistem informasi, aplikasi SPBE, dan layanan publik elektronik yang dikelola, dioperasikan, atau digunakan oleh Pemerintah Kabupaten Kendal, baik yang dikembangkan secara mandiri, diperoleh dari pihak ketiga, maupun yang merupakan aplikasi umum pemerintahan, termasuk namun tidak terbatas pada:

a. Aplikasi pengelolaan data kependudukan dan data pribadi masyarakat;
b. Sistem layanan tanda tangan elektronik (TTE) pejabat struktural;
c. Sistem pengelolaan keuangan dan anggaran daerah;
d. Portal dan aplikasi layanan publik elektronik lainnya.

4. Infrastruktur TIK: Seluruh infrastruktur teknologi informasi dan komunikasi milik Pemerintah Kabupaten Kendal, meliputi:
   a. Jaringan fiber optic yang menghubungkan antar-OPD;
   b. Server, data center, dan fasilitas pendukungnya;
   c. Perangkat keras, perangkat lunak, dan media penyimpanan data;
   d. Infrastruktur keamanan jaringan (firewall, IDS/IPS, dan sejenisnya).

5. Informasi dan Data: Seluruh informasi dan data yang dikelola oleh Pemerintah Kabupaten Kendal dalam berbagai bentuk dan media, baik dalam format digital maupun fisik, yang berkaitan dengan penyelenggaraan pemerintahan dan pelayanan publik.

Koordinasi dan pengawasan implementasi dokumen ini dilaksanakan oleh unit kerja yang membidangi teknologi informasi dan komunikasi, di bawah arahan pejabat yang bertanggung jawab atas kebijakan dan strategi pengelolaan teknologi informasi dan komunikasi di lingkungan Pemerintah Kabupaten Kendal dan Tim Teknis SMKI yang ditetapkan berdasarkan ketentuan yang berlaku.

C. Definisi dan Istilah

Dalam dokumen ini, yang dimaksud dengan:

1. Keamanan Informasi — Upaya terpadu untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi, termasuk sifat-sifat lain yang relevan seperti keaslian (*authenticity*), akuntabilitas (*accountability*), nirsangkal (*non-repudiation*), dan keandalan (*reliability*).
2. Sistem Manajemen Keamanan Informasi (SMKI) — Kerangka kebijakan, prosedur, proses, dan pengendalian terstruktur yang dikelola secara sistematis untuk melindungi aset informasi organisasi berdasarkan pendekatan risiko, mengacu pada ISO/IEC 27001:2022.
3. Aset Informasi — Segala sesuatu yang memiliki nilai bagi organisasi dan perlu dilindungi, mencakup data dan informasi (dalam format apapun), perangkat keras, perangkat lunak, layanan, sumber daya manusia, dan infrastruktur yang mendukung proses bisnis organisasi.
4. Risiko Keamanan Informasi — Potensi terjadinya peristiwa yang dapat menyebabkan dampak negatif terhadap kerahasiaan, integritas, atau ketersediaan aset informasi, diukur berdasarkan kemungkinan terjadinya ancaman dan besaran dampak yang ditimbulkan.
5. Ancaman (*Threat*) — Penyebab potensial dari suatu insiden yang tidak diinginkan, yang dapat mengakibatkan kerugian terhadap sistem atau organisasi, baik berasal dari faktor alam, kesalahan manusia, maupun tindakan yang disengaja.
6. Kerentanan (*Vulnerability*) — Kelemahan pada suatu aset informasi atau pengendalian yang dapat dieksploitasi oleh satu atau lebih ancaman, sehingga meningkatkan kemungkinan terjadinya insiden keamanan informasi.
7. Insiden Keamanan Informasi — Satu atau serangkaian peristiwa keamanan informasi yang tidak diinginkan atau tidak diharapkan, yang memiliki kemungkinan signifikan untuk mengganggu operasi bisnis dan mengancam keamanan informasi organisasi.

8. Organisasi Perangkat Daerah (OPD) — Perangkat daerah pada Pemerintah Kabupaten Kendal yang dibentuk berdasarkan peraturan perundang-undangan, meliputi Sekretariat Daerah, Sekretariat DPRD, Dinas, Badan, Inspektorat, Kecamatan, dan unit kerja lain di lingkungan Pemerintah Kabupaten Kendal.
9. Aparatur Sipil Negara (ASN) — Profesi bagi Pegawai Negeri Sipil (PNS) dan Pegawai Pemerintah dengan Perjanjian Kerja (PPPK) yang bekerja pada instansi pemerintah, sebagaimana dimaksud dalam Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara.
10. Sistem Pemerintahan Berbasis Elektronik (SPBE) — Penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE, sebagaimana dimaksud dalam Peraturan Presiden Nomor 95 Tahun 2018.
11. Teknologi Informasi dan Komunikasi (TIK) — Seluruh perangkat keras, perangkat lunak, jaringan, infrastruktur, dan layanan yang digunakan untuk memperoleh, menyimpan, memproses, mengolah, dan mendistribusikan informasi dalam rangka penyelenggaraan pemerintahan dan pelayanan publik di lingkungan Pemerintah Kabupaten Kendal.
12. Tanda Tangan Elektronik (TTE) — Tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi identitas penandatangan, sebagaimana dimaksud dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
13. Data Pribadi — Setiap data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung, melalui sistem elektronik atau nonelektronik, sebagaimana dimaksud dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
14. Pengguna (*User*) — Setiap individu yang diberikan hak akses untuk menggunakan sistem informasi atau layanan TIK milik Pemerintah Kabupaten Kendal dalam rangka pelaksanaan tugas dan fungsinya, termasuk ASN, pejabat, tenaga kontrak, dan mitra kerja yang sah.
15. Pengelola Sistem OPD — ASN atau personel yang ditunjuk secara resmi oleh Pimpinan OPD untuk mengelola, mengoperasikan, dan memelihara sistem informasi atau infrastruktur TIK di tingkat OPD, serta memiliki tanggung jawab atas keamanan informasi pada sistem yang dikelolanya. Pengelola Sistem OPD berfungsi sebagai Administrator Sistem pada tingkat OPD.
16. Pimpinan OPD — Kepala Dinas, Kepala Badan, Inspektur, Camat, atau pejabat setingkat yang memimpin suatu OPD di lingkungan Pemerintah Kabupaten Kendal.
17. Pihak Ketiga — Individu, organisasi, atau badan hukum di luar Pemerintah Kabupaten Kendal yang memiliki hubungan kontraktual atau perjanjian dan diberikan akses terhadap sistem informasi, infrastruktur TIK, atau aset informasi Pemerintah Kabupaten Kendal, meliputi vendor pengembang aplikasi, penyedia layanan cloud, kontraktor pemeliharaan, mitra integrasi data, konsultan, dan auditor eksternal.
18. Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*/CSIRT) — Tim yang dibentuk oleh unit kerja yang membidangi TIK untuk mengoordinasikan respons terhadap insiden keamanan informasi lintas OPD di lingkungan Pemerintah Kabupaten Kendal.

19. Agen Siber — Personel yang ditunjuk pada setiap OPD untuk menerima dan meneruskan laporan insiden atau dugaan insiden keamanan informasi kepada CSIRT Pemerintah Kabupaten Kendal melalui kanal pelaporan resmi yang ditetapkan.
20. Pejabat Pelindungan Data Pribadi (*Data Protection Officer*/DPO) — Pejabat yang ditunjuk oleh pimpinan daerah atau pejabat yang diberi wewenang untuk memberikan saran mengenai kewajiban pelindungan data pribadi, memantau kepatuhan, dan menjadi kontak utama bagi subjek data dan otoritas pengawas, sebagaimana dipersyaratkan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
21. Badan Siber dan Sandi Negara (BSSN) — Lembaga pemerintah yang bertanggung jawab atas keamanan siber nasional, termasuk pemberian pedoman teknis, standar keamanan informasi, dan koordinasi penanganan insiden siber di lingkungan instansi pemerintah, sebagaimana ditetapkan berdasarkan peraturan perundang-undangan yang berlaku.
22. Enkripsi — Proses pengubahan data atau informasi ke dalam bentuk yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai, dengan tujuan menjaga kerahasiaan dan integritas informasi selama penyimpanan maupun transmisi.
23. Perangkat Pribadi (*Bring Your Own Device*/BYOD) — Perangkat milik pribadi ASN atau personel yang digunakan untuk mengakses sistem informasi atau data dinas Pemerintah Kabupaten Kendal, yang penggunaannya tunduk pada persyaratan dan ketentuan keamanan yang ditetapkan.
24. Perjanjian Tingkat Layanan (*Service Level Agreement*/SLA) — Perjanjian tertulis antara Pemerintah Kabupaten Kendal dengan pihak ketiga penyedia layanan yang menetapkan target kinerja layanan, ketersediaan, waktu respons, dan parameter keamanan informasi yang wajib dipenuhi selama masa kontrak.
25. Perjanjian Kerahasiaan (*Non-Disclosure Agreement*/NDA) — Perjanjian tertulis yang mengikat pihak yang menandatanganinya untuk menjaga kerahasiaan informasi yang diperoleh selama masa kerja atau hubungan kontraktual, dan tidak mengungkapkannya kepada pihak yang tidak berwenang.

BAB II
MANAJEMEN RISIKO

A. Ketentuan Umum

Manajemen risiko keamanan informasi merupakan proses sistematis dan berkelanjutan untuk mengidentifikasi, menganalisis, mengevaluasi, dan menangani risiko yang dapat mengancam kerahasiaan, integritas, dan ketersediaan aset informasi di lingkungan Pemerintah Kabupaten Kendal. Ketentuan dalam BAB II ini merupakan aturan pertama yang mengatur manajemen risiko keamanan informasi secara operasional di lingkungan Pemerintah Kabupaten Kendal, sebagai penjabaran teknis dari Peraturan Bupati Kendal Nomor 57 Tahun 2023.

Prinsip dasar yang wajib dipedomani dalam pelaksanaan manajemen risiko keamanan informasi:

1. Berbasis Bukti — Setiap penilaian risiko harus didukung oleh data, informasi faktual, dan dokumentasi yang dapat diverifikasi;
2. Proporsional — Upaya penanganan risiko harus sebanding dengan tingkat risiko yang teridentifikasi dan sumber daya yang tersedia;
3. Terintegrasi — Manajemen risiko keamanan informasi merupakan bagian tidak terpisahkan dari tata kelola SPBE Pemerintah Kabupaten Kendal;
4. Dinamis — Penilaian risiko harus diperbarui secara berkala dan setiap kali terjadi perubahan signifikan pada lingkungan TIK atau setelah terjadinya insiden keamanan informasi;
5. Menyeluruh — Seluruh OPD wajib melaksanakan manajemen risiko keamanan informasi terhadap aset informasi yang berada dalam tanggung jawabnya.

Ruang lingkup manajemen risiko mencakup seluruh aset informasi sebagaimana didefinisikan dalam BAB I Pasal B dokumen ini, yang dikelola oleh seluruh OPD di lingkungan Pemerintah Kabupaten Kendal.

B. Metodologi Penilaian Risiko

Penilaian risiko keamanan informasi di lingkungan Pemerintah Kabupaten Kendal menggunakan metode kuantitatif sederhana berbasis **Matriks Risiko 5×5** dengan pendekatan distribusi natural.

Penilaian dilakukan dengan menetapkan nilai **Kemungkinan** dan nilai **Dampak** terlebih dahulu. Selanjutnya, nilai risiko ditentukan berdasarkan perpotongan antara nilai Kemungkinan dan nilai Dampak pada Matriks Risiko.

Dengan demikian, nilai risiko tidak dihitung semata-mata melalui perkalian antara Kemungkinan dan Dampak, melainkan ditetapkan berdasarkan nilai prioritas risiko pada matriks yang telah ditentukan.

Nilai Risiko = Nilai pada Matriks Risiko berdasarkan kombinasi Kemungkinan dan Dampak

Dengan ketentuan:

- nilai Kemungkinan berada pada rentang 1 sampai dengan 5;
- nilai Dampak berada pada rentang 1 sampai dengan 5;
- nilai Risiko berada pada rentang 1 sampai dengan 25;
- nilai Risiko ditentukan berdasarkan perpotongan antara Kemungkinan dan Dampak pada Matriks Risiko;

- semakin tinggi nilai Risiko, semakin tinggi prioritas penanganannya;
- tingkat risiko ditetapkan berdasarkan zona warna pada Matriks Risiko.

Metode ini digunakan agar penilaian risiko tidak hanya memperhatikan besaran angka, tetapi juga mempertimbangkan pola distribusi risiko yang lebih natural, yaitu:

- risiko dengan Dampak sangat tinggi tetap memperoleh perhatian meskipun Kemungkinannya rendah;
- risiko dengan Kemungkinan tinggi tetap diprioritaskan karena menunjukkan kejadian yang sering atau hampir pasti terjadi;
- kombinasi Kemungkinan dan Dampak tertentu dapat memiliki tingkat risiko yang berbeda walaupun secara perkalian sederhana menghasilkan nilai yang berdekatan;
- prioritas penanganan risiko ditentukan berdasarkan urutan nilai risiko pada matriks, bukan hanya berdasarkan hasil perkalian matematis.

1. Skala Kemungkinan (*Likelihood*)

Nilai	Tingkat	Deskripsi
1	Hampir Tidak Terjadi	Belum pernah terjadi; kemungkinan < 1 kali dalam 5 tahun terakhir di lingkungan Pemkab Kendal
2	Jarang Terjadi	Pernah terjadi; kemungkinan 1 kali dalam 3–5 tahun
3	Kadang-Kadang Terjadi	Terjadi sesekali; kemungkinan 1–2 kali per tahun
4	Sering Terjadi	Terjadi secara rutin; kemungkinan 3–11 kali setahun
5	Hampir Pasti Terjadi	Terjadi hampir pasti; kemungkinan ≥ 12 kali setahun

Tabel 1. Skala kemungkinan risiko

Panduan Penentuan Nilai Dampak:

- Gunakan **data historis insiden** dari sistem pencatatan OPD sebagai acuan utama.
- Jika tidak ada data historis, gunakan **penilaian ahli** dari tim teknis IT OPD.
- Pertimbangkan **keberadaan kontrol saat ini** — kontrol yang lemah atau tidak ada meningkatkan nilai kemungkinan.
- Konsultasikan dengan Tim Manajemen Keamanan Informasi Kabupaten Kendal untuk referensi insiden lintas OPD.

2. Skala Dampak (*Impact*)

Nilai	Tingkat	Deskripsi
1	Tidak Signifikan	Gangguan minimal; diselesaikan internal OPD tanpa dampak layanan publik; kerugian tidak signifikan
2	Kurang Signifikan	Gangguan terbatas pada unit kerja; layanan public terganggu < 2 jam; pemulihan mudah dilakukan
3	Cukup Signifikan	Beberapa OPD terdampak; layanan publik terganggu 2–8 jam; memerlukan koordinasi lintas OPD
4	Signifikan	Gangguan luas; layanan publik terganggu > 8 jam; potensi kebocoran data pribadi atau kerugian keuangan daerah yang signifikan

5	Sangat Signifikan	Gangguan kritis pada seluruh layanan SPBE; potensi pelanggaran UU PDP skala besar; kerugian reputasi dan hukum bagi Pemerintah Kabupaten Kendal

Tabel 2. Skala dampak risiko

Panduan Penentuan Nilai Kemungkinan:

- Gunakan akibat terhadap layanan publik, proses bisnis OPD, sistem elektronik, aset informasi, data, reputasi, hukum, dan keuangan sebagai dasar penilaian.
- Nilai dampak ditentukan berdasarkan akibat terburuk yang wajar terjadi apabila risiko benar-benar terjadi.
- Apabila terdapat lebih dari satu jenis dampak, gunakan nilai dampak tertinggi.
- Dampak terhadap layanan publik menjadi pertimbangan utama apabila gangguan menyebabkan layanan tidak tersedia, tertunda, salah proses, atau tidak dapat digunakan.
- Dampak terhadap data dinilai berdasarkan potensi kebocoran, perubahan tanpa kewenangan, kehilangan, atau tidak tersedianya data.
- Dampak hukum dan kepatuhan harus diperhitungkan apabila risiko berpotensi melanggar peraturan perundang-undangan, standar keamanan informasi, atau ketentuan perlindungan data pribadi.
- Dampak reputasi dan keuangan diperhitungkan apabila risiko dapat menurunkan kepercayaan publik atau menimbulkan kerugian bagi Pemerintah Kabupaten Kendal.
- Dalam hal terdapat keraguan antara dua nilai dampak, gunakan nilai yang lebih tinggi sebagai bentuk prinsip kehati-hatian.
- Risiko dengan dampak tinggi tetap harus menjadi perhatian meskipun kemungkinan kejadiannya rendah.
- Hasil penentuan nilai dampak wajib dicatat dalam Register Risiko beserta dasar pertimbangannya.

3. Kriteria Penerimaan Risiko (*Risk Acceptance Criteria*)

Kriteria penerimaan risiko ditetapkan sebagai berikut:

- Risiko dengan tingkat **Sangat Rendah** dapat diterima tanpa tindakan penanganan tambahan, dengan syarat tetap dipantau paling sedikit 1 kali dalam 1 tahun.
- Risiko dengan tingkat **Rendah** dapat diterima dengan pengendalian dasar dan wajib didokumentasikan dalam Register Risiko.
- Risiko dengan tingkat **Sedang** wajib memiliki rencana penanganan risiko yang proporsional.
- Risiko dengan tingkat **Tinggi** wajib dimitigasi secara segera dan dilaporkan kepada Pimpinan OPD.
- Risiko dengan tingkat **Sangat Tinggi** wajib dieskalasi kepada Pimpinan OPD dan Tim Manajemen Keamanan Informasi Kabupaten Kendal untuk penanganan prioritas.

Penerimaan risiko hanya dapat dilakukan apabila risiko telah dinilai, didokumentasikan, disetujui oleh pejabat yang berwenang, dan tidak bertentangan dengan ketentuan peraturan perundang-undangan.

C. Matriks Risiko

1. Tabel Matriks 5x5

			DAMPAK				
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
			1	2	3	4	5
KEMUNGKINAN	Hampir pasti terjadi	5	9	15	18	23	25
	Sering terjadi	4	6	12	16	19	24
	Kadang-kadang terjadi	3	4	10	14	17	22
	Jarang terjadi	2	2	7	11	13	21
	Hampir tidak terjadi	1	1	3	5	8	20

Tabel 3. Tabel matriks risiko 5x5

2. Klasifikasi Tingkat Risiko dan Respons Wajib

Nilai Risiko	Tingkat Risiko	Warna	Ketentuan Umum	Respons Wajib
1-5	Sangat Rendah	Biru	Risiko dapat diterima dengan pemantauan berkala.	Diterima dan dipantau paling sedikit 1 kali dalam 1 tahun.
6-10	Rendah	Hijau	Risiko masih dapat diterima dengan pengendalian dasar.	Didokumentasikan dalam Register Risiko dan dipantau secara berkala.
11-15	Sedang	Kuning	Risiko memerlukan pengendalian dan rencana penanganan yang proporsional.	Wajib disusun rencana penanganan risiko dan dilaporkan kepada Pimpinan OPD.
16-20	Tinggi	Oranye	Risiko memerlukan tindakan mitigasi segera.	Wajib dimitigasi, ditetapkan penanggung jawab, dan dipantau oleh Pimpinan OPD serta Tim Manajemen Keamanan Informasi.

21-25	Sangat Tinggi	Merah	Risiko memerlukan eskalasi dan penanganan prioritas.	Wajib dieskalasi kepada Pimpinan OPD dan Penanggung Jawab Keamanan Informasi Kabupaten Kendal untuk mendapatkan arahan penanganan segera.

Tabel 4. Klasifikasi risiko dan respons wajib

D. Proses Manajemen Risiko

Proses manajemen risiko keamanan informasi di lingkungan Pemerintah Kabupaten Kendal dilaksanakan melalui 6 (enam) langkah berurutan sebagai berikut:

LANGKAH 1 — IDENTIFIKASI ASET INFORMASI

Setiap OPD wajib menyusun dan memutakhirkan Daftar Aset Informasi yang berada dalam tanggung jawabnya. Daftar tersebut mencakup minimal: nama aset, kategori aset (data/sistem/infrastruktur/SDM), pemilik aset, lokasi/media penyimpanan, tingkat klasifikasi informasi, dan nilai aset bagi organisasi.

Klasifikasi aset informasi mengacu pada tingkat kerahasiaan:

a. Rahasia — hanya dapat diakses oleh pihak yang berwenang;
b. Terbatas — dapat diakses oleh personel OPD tertentu;
c. Biasa — dapat diakses oleh seluruh ASN Pemkab Kendal;
d. Publik — dapat diakses oleh masyarakat umum.

LANGKAH 2 — IDENTIFIKASI ANCAMAN DAN KERENTANAN

Untuk setiap aset informasi, OPD wajib mengidentifikasi:

a. Ancaman yang relevan, meliputi: serangan siber (malware, phishing, ransomware), akses tidak sah, bencana alam, kegagalan sistem, kesalahan manusia, dan kebocoran informasi;
b. Kerentanan yang melekat pada aset, meliputi: kelemahan konfigurasi sistem, ketiadaan prosedur, kurangnya kompetensi SDM, dan kelemahan kontrol fisik.

LANGKAH 3 — ANALISIS RISIKO

OPD menghitung Nilai Risiko untuk setiap kombinasi aset–ancaman menggunakan rumus: Nilai Risiko = Kemungkinan × Dampak, berdasarkan skala yang ditetapkan dalam Pasal B dokumen ini.

CONTOH KASUS NYATA PEMKAB KENDAL:

Skenario: Kegagalan Server Utama Akibat Patch Keamanan Tertunda	
Aset	Server aplikasi layanan SPBE di Data Center Diskominfo Kabupaten Kendal
Klasifikasi Aset	Terbatas
Ancaman	Eksploitasi kerentanan sistem operasi server oleh peretas (*ransomware*/*remote code execution*) melalui jaringan publik
Kerentanan	Pembaruan patch keamanan sistem operasi server tertunda lebih dari 90 hari karena tidak ada jadwal pemeliharaan terjadwal

Kemungkinan	2 (Kadang-kadang Terjadi - kerentanan CVE tinggi pada versi OS yang digunakan telah dipublikasi dan dieksploitasi secara aktif)
Dampak	4 (Signifikan - gangguan layanan SPBE lintas OPD, potensi kebocoran data layanan publik, pemulihan membutuhkan waktu lebih dari 24 jam)
Nilai Risiko	2 × 4 = 8 → SEDANG (Kuning)
Respons Wajib	Mitigasi dalam 3 bulan; lapor Pimpinan OPD
Rencana Penanganan	1. Terapkan patch keamanan kritis dalam jam sejak rilis; patch mayor dalam 30 hari (sesuai BAB VI, A.8.8) 2. Tetapkan Jadwal Pemeliharaan Preventif server minimal setiap 6 bulan (A.8.8) 1. Aktifkan pemantauan CVE otomatis dari BSSN dan vendor OS yang digunakan

Tabel 5. Contoh analisis risiko

LANGKAH 4 — EVALUASI RISIKO

OPD membandingkan Nilai Risiko hasil analisis dengan Kriteria Penerimaan Risiko (Pasal B angka 3). Risiko yang melampaui kriteria penerimaan wajib diprioritaskan untuk ditangani berdasarkan urutan nilai risiko dari yang tertinggi.

LANGKAH 5 — PENANGANAN RISIKO

Terhadap setiap risiko yang memerlukan penanganan, OPD memilih satu atau kombinasi opsi berikut:

a. Mitigasi (*Risk Mitigation*) — Menerapkan kontrol keamanan informasi untuk mengurangi kemungkinan dan/atau dampak risiko. Ini adalah opsi yang paling diutamakan;

b. Transfer (*Risk Transfer*) — Memindahkan sebagian risiko kepada pihak lain melalui asuransi, kontrak jasa, atau perjanjian layanan (SLA). Wajib mendapat persetujuan Pimpinan OPD;

c. Terima (*Risk Acceptance*) — Menerima risiko yang berada dalam kriteria penerimaan tanpa tindakan tambahan, disertai dokumentasi pertimbangan dan persetujuan tertulis dari Pimpinan OPD;

d. Hindari (*Risk Avoidance*) — Menghentikan aktivitas yang menimbulkan risiko tersebut apabila risiko tidak dapat dimitigasi secara efektif dan proporsional.

Setiap keputusan penanganan risiko wajib dituangkan dalam Rencana Penanganan Risiko yang ditandatangani oleh Pimpinan OPD.

LANGKAH 6 — PEMANTAUAN DAN TINJAUAN

Pemantauan risiko dilaksanakan secara berkala dan berkelanjutan:

a. Tinjauan rutin: minimal 1 (satu) kali dalam 1 (satu) tahun pada setiap OPD, dikoordinasikan oleh Tim Teknis Diskominfo;

b. Tinjauan insidental: wajib dilaksanakan dalam waktu 14 (empat belas) hari kerja setelah terjadinya insiden keamanan informasi yang signifikan;

c. Tinjauan perubahan: wajib dilaksanakan apabila terdapat perubahan signifikan pada infrastruktur TIK, sistem informasi, atau struktur organisasi yang memengaruhi profil risiko OPD;

d. Hasil tinjauan wajib didokumentasikan dalam Laporan Tinjauan Risiko Tahunan dan dilaporkan melalui Diskominfo kepada pejabat yang bertanggung jawab atas keamanan informasi tingkat pemerintah daerah.

E. Dokumen dan Rekaman Wajib

No	Dokumen/Rekaman	Frekuensi Pembaruan
1	Daftar Aset Informasi OPD	Minimal setahun sekali atau setiap ada perubahan aset
2	Register Risiko (*Risk Register*)	Minimal setahun sekali atau pasca insiden keamanan informasi yang signifikan
3	Rencana Penanganan Risiko (*Risk Treatment Plan*)	Diperbarui setiap siklus penilaian risiko atau saat ada risiko baru
4	Laporan Tinjauan Risiko Tahunan	Setahun sekali

Tabel 6. Dokumen dan rekaman risiko

Seluruh dokumen dan rekaman wajib disimpan dalam jangka waktu minimal 5 (lima) tahun sesuai ketentuan kearsipan yang berlaku dan harus tersedia untuk keperluan audit internal maupun eksternal.

BAB III
PENGENDALIAN ORGANISASI

A. Maksud dan Tujuan

Memastikan tersedianya kerangka tata kelola keamanan informasi yang menyeluruh di lingkungan Pemerintah Kabupaten Kendal, meliputi penetapan kebijakan, pembagian peran dan tanggung jawab, pemisahan tugas, dukungan manajemen, hubungan dengan otoritas, inventarisasi dan penggunaan aset informasi, pengendalian transfer dan akses informasi, kesiapan manajemen insiden, serta perlindungan data pribadi — sehingga tercipta landasan organisasi yang kuat bagi seluruh pengendalian keamanan informasi yang diatur dalam dokumen ini.

B. Ruang Lingkup

Seluruh Organisasi Perangkat Daerah (OPD) di lingkungan Pemerintah Kabupaten Kendal, mencakup pejabat struktural, Aparatur Sipil Negara (ASN), Pegawai Pemerintah dengan Perjanjian Kerja (PPPK), tenaga kontrak, konsultan, dan pihak ketiga yang mengakses, mengelola, atau memproses aset informasi dan sistem Teknologi Informasi dan Komunikasi (TIK) milik Pemerintah Kabupaten Kendal.

C. Ketentuan

1. Pemisahan Tugas

a. Fungsi pengembangan, pengujian, dan pengoperasian sistem informasi wajib dipisahkan dan tidak boleh dilaksanakan oleh personel yang sama.
b. Fungsi permintaan akses, persetujuan akses, dan implementasi akses wajib dilaksanakan oleh personel yang berbeda.
c. Fungsi pengelolaan data keuangan wajib dipisahkan antara pihak yang menginput, memverifikasi, dan menyetujui transaksi.
d. Pengelola sistem dilarang menjadi auditor internal untuk sistem yang dikelolanya sendiri.
e. Dalam hal keterbatasan sumber daya manusia pada OPD tertentu yang menyebabkan pemisahan tugas tidak dapat dilakukan secara penuh, pimpinan OPD wajib menetapkan kontrol kompensasi berupa mekanisme pengawasan tambahan dan pencatatan log audit yang memadai.

2. Tanggung Jawab Manajemen

a. Pimpinan OPD wajib memastikan seluruh ASN dan pihak ketiga di lingkungan OPD memahami dan mematuhi kebijakan keamanan informasi yang berlaku.
b. Pimpinan OPD wajib mengalokasikan sumber daya yang memadai untuk pelaksanaan pengendalian keamanan informasi di OPD.
c. Pimpinan OPD wajib menyelenggarakan atau memfasilitasi kegiatan sosialisasi keamanan informasi bagi seluruh ASN di OPD minimal 1 (satu) kali dalam 1 (satu) tahun.
d. Pimpinan OPD wajib memastikan bahwa pelanggaran keamanan informasi ditindaklanjuti sesuai prosedur yang berlaku.
e. Pejabat yang bertanggung jawab atas keamanan informasi tingkat pemerintah daerah wajib melakukan evaluasi kepatuhan OPD terhadap kebijakan keamanan informasi minimal 1 (satu) kali dalam 1 (satu) tahun.

3. Hubungan dengan Otoritas

a. Unit kerja yang membidangi TIK wajib menyusun dan memutakhirkan Daftar Kontak Otoritas yang mencakup minimal: Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika, Kepolisian (*unit cybercrime*), CSIRT Nasional/Sektoral, dan penyedia layanan internet yang digunakan.
b. Daftar Kontak Otoritas wajib mencantumkan nama lembaga, nama kontak, nomor telepon, alamat email, dan prosedur pelaporan yang berlaku.
c. Daftar Kontak Otoritas wajib ditinjau dan diperbarui minimal 1 (satu) kali dalam 6 (enam) bulan.
d. Seluruh OPD wajib mengetahui prosedur pelaporan insiden kepada otoritas melalui koordinasi unit kerja yang membidangi TIK.
e. Pelaporan insiden keamanan informasi kepada otoritas eksternal wajib dikoordinasikan melalui unit kerja yang membidangi TIK, kecuali ditentukan lain oleh peraturan perundang-undangan.

4. Inventarisasi Aset Informasi

a. Setiap OPD wajib menyusun Daftar Aset Informasi yang mencakup minimal: identitas aset, kategori (data, perangkat keras, perangkat lunak, layanan), pemilik aset, lokasi atau media penyimpanan, klasifikasi kerahasiaan, dan nilai kritikalitas.
b. Setiap aset informasi wajib memiliki pemilik (*asset owner*) yang ditunjuk secara resmi oleh pimpinan OPD. Pemilik aset bertanggung jawab atas perlindungan, klasifikasi, dan pengendalian akses terhadap aset yang dimilikinya.
c. Daftar Aset Informasi wajib diperbarui minimal 1 (satu) kali dalam 1 (satu) tahun atau setiap terjadi penambahan, perubahan, atau penghapusan aset.
d. Unit kerja yang membidangi TIK wajib mengkonsolidasikan Daftar Aset Informasi seluruh OPD menjadi Inventaris Aset Informasi Pemerintah Kabupaten Kendal.
e. Penghapusan aset informasi dari daftar wajib mendapat persetujuan pimpinan OPD dan didokumentasikan.

5. Penggunaan Aset Informasi yang Dapat Diterima

a. Aset informasi dan fasilitas TIK milik Pemerintah Kabupaten Kendal hanya boleh digunakan untuk kepentingan dinas dan pelayanan publik.
b. Pengguna dilarang menggunakan fasilitas TIK dinas untuk:
    1) mengakses, menyimpan, atau mendistribusikan konten ilegal;
    2) melakukan kegiatan yang melanggar hak kekayaan intelektual;
    3) menginstal perangkat lunak tidak berlisensi atau yang tidak disetujui;
    4) mengakses sistem atau data di luar kewenangan yang diberikan.
c. Pengguna wajib menjaga kerahasiaan kredensial akses dan dilarang membagikannya kepada pihak lain.
d. Penggunaan perangkat pribadi (BYOD) untuk mengakses sistem informasi dinas wajib mendapat persetujuan pimpinan OPD dan memenuhi persyaratan keamanan minimum yang ditetapkan.
e. Seluruh pengguna wajib menandatangani Pernyataan Penggunaan Aset yang Dapat Diterima sebelum diberikan hak akses.
f. Pelanggaran ketentuan penggunaan aset wajib dilaporkan kepada pengelola sistem dan pimpinan OPD.

6. Transfer Informasi

a. Transfer informasi dengan klasifikasi Rahasia dan Terbatas wajib menggunakan mekanisme enkripsi atau perlindungan yang setara.
b. Pengiriman informasi Rahasia melalui email wajib menggunakan email dinas resmi dengan enkripsi dan/atau lampiran terproteksi kata sandi.
c. Transfer informasi ke pihak eksternal wajib berdasarkan perjanjian kerahasiaan (*Non-Disclosure Agreement*/NDA) yang ditandatangani kedua belah pihak, kecuali untuk informasi berkategori Publik.
d. Penggunaan media penyimpanan portabel (USB, *external drive*) untuk mentransfer informasi Rahasia wajib mendapat persetujuan tertulis dari pimpinan OPD dan dicatat dalam log transfer informasi.
e. Pengiriman dokumen fisik berkategori Rahasia wajib menggunakan amplop tersegel dengan tanda klasifikasi dan dikirim melalui kurir resmi atau diserahkan secara langsung dengan bukti serah terima.
f. Seluruh transfer informasi berkategori Rahasia dan Terbatas wajib dicatat dalam Log Transfer Informasi.

7. Pengendalian Akses

a. Kebijakan pengendalian akses wajib ditetapkan berdasarkan prinsip *need-to-know* dan *least privilege* (hak akses minimum yang diperlukan untuk menjalankan tugas).
b. Setiap pemberian hak akses wajib melalui proses formal yang mencakup: permohonan tertulis, persetujuan pimpinan OPD atau pejabat yang ditunjuk, dan pencatatan oleh pengelola sistem.
c. Hak akses wajib ditinjau minimal 1 (satu) kali dalam 6 (enam) bulan oleh pengelola sistem dan dilaporkan kepada pimpinan OPD.
d. Hak akses ASN yang mutasi, pensiun, atau berhenti wajib dicabut dalam waktu maksimal 1 (satu) hari kerja setelah tanggal efektif perubahan status kepegawaian.
e. Akses terhadap data kependudukan dan data pribadi wajib dibatasi hanya kepada ASN yang memiliki kewenangan berdasarkan tugas dan fungsinya, sesuai ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
f. Seluruh aktivitas akses terhadap sistem kritis wajib dicatat dalam log akses.
g. Penggunaan akun bersama (*shared account*) dilarang, kecuali untuk akun layanan (*service account*) yang dikelola dengan prosedur khusus dan mendapat persetujuan dari pejabat yang berwenang.

8. Perencanaan dan Kesiapan Manajemen Insiden

a. Pimpinan daerah atau pejabat yang diberi wewenang wajib menetapkan Kebijakan Manajemen Insiden Keamanan Informasi yang mencakup minimal: definisi dan klasifikasi insiden, struktur tanggap insiden siber, alur eskalasi, dan kewajiban pelaporan.
b. Klasifikasi insiden keamanan informasi ditetapkan sebagai berikut:
    1) Prioritas 1 (Kritis) — insiden yang mengakibatkan gangguan total layanan publik, kebocoran data pribadi skala besar, atau ancaman terhadap keselamatan; penanganan wajib dimulai dalam 1 (satu) jam;
    2) Prioritas 2 (Tinggi) — insiden yang mengakibatkan gangguan signifikan pada layanan atau potensi kebocoran data terbatas; penanganan wajib dimulai dalam 4 (empat) jam;
    3) Prioritas 3 (Sedang) — insiden yang berdampak terbatas pada operasional internal OPD; penanganan wajib dimulai dalam 1 (satu) hari kerja;

4) Prioritas 4 (Rendah) — peristiwa keamanan yang memerlukan pencatatan dan pemantauan tanpa dampak operasional langsung; penanganan dalam 3 (tiga) hari kerja.

c. Unit kerja yang membidangi TIK wajib membentuk Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*/CSIRT) Pemerintah Kabupaten Kendal yang bertugas mengoordinasikan respons insiden lintas OPD.
d. Setiap OPD wajib menunjuk minimal 1 (satu) personel sebagai Agen Siber yang bertanggung jawab melaporkan setiap insiden atau dugaan insiden kepada CSIRT Pemerintah Kabupaten Kendal melalui kanal pelaporan resmi yang ditetapkan.
e. Seluruh ASN wajib melaporkan setiap peristiwa yang diduga merupakan insiden keamanan informasi kepada Agen Siber di OPD masing-masing dalam waktu maksimal 1×24 jam setelah diketahui.
f. Alur eskalasi insiden:
   1) Prioritas 4 dan 3: ditangani oleh pengelola sistem OPD, dilaporkan kepada pimpinan OPD;
   2) Prioritas 2: dieskalasi kepada CSIRT Pemerintah Kabupaten Kendal dan pimpinan unit kerja yang membidangi TIK;
   3) Prioritas 1: dieskalasi langsung kepada pejabat yang bertanggung jawab atas keamanan informasi tingkat pemerintah daerah dan dilaporkan kepada Bupati; wajib berkoordinasi dengan BSSN dan otoritas terkait.
g. Simulasi penanganan insiden (*incident response drill*) wajib diselenggarakan minimal 1 (satu) kali dalam 1 (satu) tahun untuk menguji kesiapan dan efektivitas prosedur penanganan insiden.
h. Setiap insiden yang telah ditangani wajib dilengkapi Laporan Pasca Insiden yang memuat: kronologi, dampak, tindakan penanganan, akar penyebab, dan rekomendasi pencegahan.
i. Hasil pembelajaran dari insiden (lessons learned) wajib diintegrasikan ke dalam proses tinjauan risiko sebagaimana diatur dalam BAB II dokumen ini.

9. Privasi dan Perlindungan Data Pribadi

a. Pemerintah Kabupaten Kendal selaku Pengendali Data Pribadi wajib memenuhi seluruh kewajiban yang ditetapkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
b. Setiap OPD yang memproses data pribadi wajib menyusun Rekaman Kegiatan Pemrosesan Data Pribadi (*Record of Processing Activities*/RoPA) yang mencakup minimal: jenis data yang diproses, tujuan pemrosesan, dasar hukum pemrosesan, kategori subjek data, pihak penerima data, jangka waktu penyimpanan, dan langkah perlindungan yang diterapkan.
c. Pemrosesan data pribadi wajib dilakukan berdasarkan dasar hukum yang sah sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022, yang meliputi: persetujuan subjek data, pemenuhan kewajiban perjanjian, pemenuhan kewajiban hukum, perlindungan kepentingan vital, pelaksanaan tugas dalam rangka kepentingan umum atau pelayanan publik, dan pemenuhan kepentingan yang sah.
d. Pimpinan daerah atau pejabat yang diberi wewenang wajib menunjuk Pejabat Pelindungan Data Pribadi (*Data Protection Officer*/DPO) di lingkungan Pemerintah Kabupaten Kendal yang bertugas memberikan saran mengenai kewajiban pelindungan data, memantau kepatuhan, dan menjadi kontak utama bagi subjek data dan otoritas pengawas.

e. Setiap OPD wajib melaksanakan Penilaian Dampak Pelindungan Data Pribadi (*Data Protection Impact Assessment*/DPIA) sebelum menerapkan pemrosesan data pribadi baru yang berisiko tinggi, meliputi: pemrosesan data spesifik (ras, agama, data kesehatan, data biometrik, data genetika, data anak, data keuangan pribadi), pemrosesan otomatis dengan pengambilan keputusan berdampak signifikan, dan pemrosesan data pribadi skala besar.
f. Penyimpanan data pribadi wajib dibatasi sesuai jangka waktu yang diperlukan berdasarkan tujuan pemrosesan. Data pribadi yang telah melampaui jangka waktu penyimpanan wajib dihapus atau dianonimkan dengan cara yang tidak dapat dikembalikan ke bentuk semula, dan dibuktikan dengan Berita Acara Pemusnahan Data Pribadi.
g. Transfer data pribadi kepada pihak ketiga wajib memenuhi persyaratan:
    1) berdasarkan perjanjian pemrosesan data pribadi (*Data Processing Agreement*/DPA) yang memuat kewajiban pelindungan data;
    2) pihak ketiga penerima wajib memberikan tingkat pelindungan data pribadi yang setara atau lebih tinggi;
    3) mendapat persetujuan tertulis dari pimpinan OPD pemilik data.
h. Dalam hal terjadi kegagalan pelindungan data pribadi (*data breach*), unit kerja yang membidangi TIK wajib:
    1) memberitahukan kepada subjek data pribadi yang terdampak secara tertulis dalam waktu maksimal 3×24 jam;
    2) memberitahukan kepada lembaga pengawas pelindungan data pribadi dalam waktu maksimal 3×24 jam;
    3) memuat minimal: jenis data yang terungkap, kronologi, upaya penanganan, dan langkah mitigasi.
i. Seluruh ASN yang memproses data pribadi wajib menandatangani Perjanjian Kerahasiaan Data Pribadi dan mengikuti pelatihan kesadaran pelindungan data pribadi minimal 1 (satu) kali dalam 1 (satu) tahun.
j. Hak subjek data pribadi yang wajib dipenuhi oleh setiap OPD meliputi: hak mendapatkan informasi tentang pemrosesan, hak mengakses dan memperoleh salinan data pribadinya, hak memperbarui dan memperbaiki data pribadi, serta hak mengakhiri pemrosesan dan menghapus data pribadi sesuai ketentuan yang berlaku.

BAB IV
PENGENDALIAN SUMBER DAYA MANUSIA

A. Maksud dan Tujuan

Memastikan seluruh personel yang mengakses aset informasi dan sistem TIK Pemerintah Kabupaten Kendal memahami, menyetujui, dan menjalankan tanggung jawab keamanan informasi — mulai dari proses penerimaan hingga setelah berakhirnya hubungan kerja — serta memiliki kompetensi yang memadai melalui program kesadaran dan pelatihan yang terencana.

B. Ruang Lingkup

Seluruh ASN, PPPK, tenaga kontrak, konsultan, dan personel pihak ketiga di lingkungan Pemerintah Kabupaten Kendal yang diberikan akses terhadap sistem informasi, infrastruktur TIK, atau fasilitas pengolahan data.

C. Ketentuan

1. Verifikasi Latar Belakang

a. Setiap calon personel yang akan diberikan akses ke sistem informasi wajib menjalani verifikasi latar belakang sesuai ketentuan peraturan perundang-undangan yang berlaku sebelum diberikan akses ke sistem informasi dinas.
b. Tenaga kontrak dan personel pihak ketiga yang akan mengakses sistem informasi dengan klasifikasi Rahasia atau Terbatas wajib menjalani verifikasi yang mencakup minimal: validasi identitas, konfirmasi kualifikasi, dan pemeriksaan rekam jejak kerja.
c. Pimpinan OPD wajib memastikan bahwa pemberian akses kepada tenaga kontrak dan pihak ketiga baru hanya dilakukan setelah proses verifikasi selesai dan hasilnya dinyatakan memenuhi syarat.
d. Seluruh hasil verifikasi latar belakang wajib didokumentasikan dan disimpan dalam berkas kepegawaian dengan perlindungan yang sesuai dengan klasifikasi data pribadi.
e. Verifikasi latar belakang ulang wajib dilaksanakan apabila terdapat perubahan signifikan pada akses atau tanggung jawab personel yang menyangkut aset informasi kritis.

2. Persyaratan Keamanan dalam Hubungan Kerja

a. Kewajiban keamanan informasi wajib dicantumkan secara eksplisit dalam perjanjian kerja, kontrak, atau dokumen penugasan untuk seluruh personel sebelum diberikan akses ke sistem informasi dinas.
b. Ketentuan keamanan informasi wajib mencakup minimal:
    1) kewajiban menjaga kerahasiaan informasi yang diakses;
    2) larangan penggunaan aset informasi di luar kepentingan dinas;
    3) kewajiban melaporkan insiden atau dugaan insiden keamanan informasi;
    4) konsekuensi atas pelanggaran ketentuan keamanan informasi;
    5) kewajiban perlindungan data pribadi sesuai Undang-Undang Nomor 27 Tahun 2022.
c. Setiap personel wajib menandatangani Perjanjian Kerahasiaan (Non-Disclosure Agreement/NDA) sebelum diberikan akses ke informasi dengan klasifikasi Rahasia atau Terbatas.
d. NDA tetap berlaku setelah berakhirnya hubungan kerja atau penugasan selama jangka waktu yang ditetapkan dalam perjanjian dan tidak kurang dari 2 (dua) tahun.

e. Template standar NDA wajib disediakan oleh unit kerja yang membidangi TIK dan dapat diadaptasi oleh setiap OPD sesuai kebutuhan.

3. Kesadaran, Pendidikan, dan Pelatihan Keamanan Informasi

a. Program Pelatihan dan Kesadaran Keamanan Informasi Tahunan wajib disusun yang mencakup: tujuan, sasaran peserta, materi, metode, jadwal, dan mekanisme evaluasi.
b. Seluruh ASN wajib mengikuti pelatihan atau sosialisasi kesadaran keamanan informasi minimal 1 (satu) kali dalam 1 (satu) tahun kalender.
c. Materi pelatihan wajib mencakup minimal:
   1) kebijakan dan prosedur keamanan informasi yang berlaku;
   2) ancaman keamanan informasi terkini yang relevan (phishing, *malware*, rekayasa sosial);
   3) kewajiban perlindungan data pribadi;
   4) prosedur pelaporan insiden dan dugaan insiden;
   5) tanggung jawab dan sanksi pelanggaran keamanan informasi.
a. ASN yang mengemban peran sebagai pengelola sistem wajib mengikuti pelatihan teknis keamanan informasi yang relevan dengan perannya, minimal 1 (satu) kali dalam 1 (satu) tahun, dengan muatan teknis yang lebih mendalam dari pelatihan kesadaran umum.
b. Seluruh ASN baru wajib mengikuti orientasi keamanan informasi dalam waktu maksimal 30 (tiga puluh) hari kerja sejak tanggal mulai bertugas, sebelum atau bersamaan dengan pemberian akses ke sistem informasi dinas.
c. Simulasi serangan phishing atau uji kesadaran keamanan informasi wajib dilaksanakan minimal 1 (satu) kali dalam 1 (satu) tahun untuk mengukur efektivitas program pelatihan.
d. Efektivitas program pelatihan wajib dievaluasi dan hasilnya digunakan sebagai dasar penyempurnaan program pelatihan tahun berikutnya.
e. Pimpinan OPD wajib memastikan seluruh ASN di OPD menghadiri kegiatan pelatihan dan mencatat kehadiran sebagai rekaman wajib.

4. Proses Disiplin atas Pelanggaran Keamanan Informasi

a. Setiap dugaan pelanggaran kebijakan keamanan informasi wajib ditindaklanjuti melalui proses investigasi yang objektif, terdokumentasi, dan menjamin hak klarifikasi bagi pihak yang diduga melanggar, sebelum dijatuhkan sanksi.
b. Proses disiplin bagi ASN yang melanggar ketentuan keamanan informasi dilaksanakan sesuai mekanisme disiplin Pegawai Negeri Sipil sebagaimana diatur dalam Peraturan Pemerintah Nomor 94 Tahun 2021, dengan mempertimbangkan:
   1) tingkat kesengajaan atau kelalaian;
   2) dampak nyata atau potensi dampak terhadap organisasi;
   3) rekam jejak disiplin sebelumnya.
c. Matriks Sanksi Keamanan Informasi wajib disusun yang memetakan jenis pelanggaran ke tingkat hukuman disiplin yang sesuai, sebagai acuan yang konsisten bagi seluruh OPD.
d. Tingkat hukuman disiplin mengacu pada Peraturan Pemerintah Nomor 94 Tahun 2021:
   1) hukuman disiplin ringan: teguran lisan, teguran tertulis, atau pernyataan tidak puas secara tertulis;

2) hukuman disiplin sedang: pemotongan tunjangan kinerja, penundaan kenaikan gaji berkala, atau penundaan kenaikan pangkat;
3) hukuman disiplin berat: penurunan jabatan, pembebasan dari jabatan, pemberhentian dengan hormat tidak atas permintaan sendiri, atau pemberhentian tidak dengan hormat.

e. Pelanggaran yang memenuhi unsur pidana diproses sesuai ketentuan hukum yang berlaku tanpa meniadakan proses disiplin internal.
f. Proses disiplin terhadap tenaga kontrak dan pihak ketiga dilaksanakan sesuai ketentuan dalam perjanjian kerja atau kontrak yang berlaku.
g. Seluruh proses disiplin terkait keamanan informasi wajib didokumentasikan, termasuk bukti investigasi, temuan, putusan, dan tindak lanjut.

5. Tanggung Jawab Pasca Penugasan (Offboarding)

a. Penonaktifan Akses Sistem:
1) seluruh hak akses ke sistem informasi, aplikasi, email dinas, dan infrastruktur TIK wajib dinonaktifkan dalam waktu maksimal 1 (satu) hari kerja setelah tanggal efektif berakhirnya penugasan, mutasi, pensiun, atau pemberhentian;
2) pengelola sistem OPD wajib membuat daftar periksa penonaktifan akses yang mencakup seluruh sistem yang pernah diakses oleh personel yang bersangkutan;
3) penonaktifan akses wajib dikonfirmasi secara tertulis oleh pengelola sistem kepada pimpinan OPD.

b. Pengembalian Aset:
1) seluruh aset TIK dan aset informasi milik dinas wajib dikembalikan pada hari kerja terakhir, meliputi: perangkat keras (laptop, ponsel dinas, token akses), media penyimpanan, kunci fisik ruang server atau ruang arsip, dan dokumen atau berkas dinas;
2) pengembalian aset wajib dibuktikan dengan Berita Acara Serah Terima Aset yang ditandatangani oleh personel yang bersangkutan dan pejabat yang ditunjuk;
3) seluruh data dinas pada perangkat pribadi (BYOD) yang digunakan selama penugasan wajib dihapus secara permanen dan dibuktikan dengan pernyataan tertulis.

c. Kewajiban Kerahasiaan Pasca Penugasan:
1) kewajiban menjaga kerahasiaan informasi yang diperoleh selama masa penugasan tetap berlaku setelah berakhirnya hubungan kerja selama jangka waktu yang ditetapkan dalam NDA dan tidak kurang dari 2 (dua) tahun;
2) personel yang bersangkutan wajib menandatangani Surat Pernyataan Kerahasiaan Pasca Penugasan pada saat serah terima aset;
3) pelanggaran kewajiban kerahasiaan pasca penugasan dapat dikenakan sanksi hukum sesuai ketentuan peraturan perundang-undangan yang berlaku.

d. Proses *Offboarding* Terstruktur:
1) Formulir *Offboarding* Keamanan Informasi standar wajib disediakan untuk digunakan oleh seluruh OPD;
2) pimpinan OPD wajib memastikan proses *offboarding* keamanan informasi diselesaikan sebelum penerbitan surat keterangan bebas administrasi kepegawaian;

3) pengelola sistem OPD wajib melaporkan penyelesaian penonaktifan akses kepada unit kerja yang membidangi TIK dalam waktu 3 (tiga) hari kerja.

6. Pelaporan Kejadian Keamanan Informasi

a. Kanal pelaporan kejadian keamanan informasi wajib disediakan dan dipublikasikan, mencakup minimal:
   1) email khusus pelaporan insiden yang dipantau setiap hari kerja;
   2) nomor telepon atau aplikasi pesan singkat tim teknis keamanan informasi;
   3) sistem pelaporan internal OPD melalui Agen Siber sebagaimana ditetapkan dalam BAB III dokumen ini.

b. Mekanisme pelaporan anonim wajib disediakan yang memungkinkan pelapor menyampaikan informasi kejadian keamanan tanpa mengungkapkan identitasnya. Laporan anonim wajib ditindaklanjuti dengan proses investigasi yang sama dengan laporan beridentitas.

c. Setiap personel yang melaporkan kejadian atau dugaan kejadian keamanan informasi dengan itikad baik wajib mendapat perlindungan dari tindakan pembalasan, intimidasi, atau sanksi. Pimpinan OPD dilarang mengambil tindakan yang merugikan pelapor atas dasar laporan yang disampaikan dengan itikad baik. Identitas pelapor bersifat rahasia dan hanya boleh diakses oleh personel yang berwenang dalam rangka investigasi.

d. Seluruh ASN wajib segera melaporkan kejadian atau dugaan kejadian keamanan informasi, termasuk namun tidak terbatas pada:
   1) dugaan infeksi *malware* atau ransomware pada perangkat atau sistem;
   2) kehilangan atau pencurian perangkat yang menyimpan data dinas;
   3) akses tidak sah atau mencurigakan ke akun atau sistem;
   4) email *phishing* yang diterima melalui email dinas;
   5) kebocoran atau dugaan kebocoran data/informasi dinas.

e. Pelaporan wajib disampaikan dalam waktu maksimal 1×24 jam setelah kejadian diketahui atau diduga terjadi.

f. Setiap laporan kejadian wajib mendapat konfirmasi penerimaan dalam waktu maksimal 4 (empat) jam kerja dan informasi tindak lanjut awal dalam waktu 1 (satu) hari kerja.

g. Seluruh laporan kejadian wajib dicatat dalam Log Insiden Keamanan Informasi sebagaimana diatur dalam BAB III dokumen ini.

BAB V
PENGENDALIAN FISIK

A. Maksud dan Tujuan

Melindungi fasilitas pengolahan informasi, peralatan TIK, infrastruktur pendukung, dan aset informasi fisik Pemerintah Kabupaten Kendal dari akses fisik yang tidak sah, ancaman lingkungan, kerusakan peralatan, dan kebocoran informasi melalui media fisik — dengan menetapkan zona keamanan, mekanisme pengendalian akses fisik, pemantauan, perlindungan peralatan, pemeliharaan, serta prosedur pembuangan yang aman.

B. Ruang Lingkup

Seluruh lokasi fisik yang menyimpan, memproses, atau mendukung operasional sistem informasi dan aset TIK di lingkungan Pemerintah Kabupaten Kendal, meliputi: data center, ruang server, ruang telekomunikasi, ruang arsip, ruang perangkat jaringan (*wiring closet*), ruang rapat yang membahas informasi sensitif, ruang kerja ASN, serta infrastruktur pendukung (kelistrikan, pendingin, kabel).

C. Ketentuan

1. Perimeter dan Zona Keamanan Fisik

a. Zona keamanan fisik fasilitas TIK wajib ditetapkan dan didokumentasikan berdasarkan tingkat keamanan yang diperlukan, minimal terdiri dari:
   1) Zona Terbuka — area publik dan area penerimaan tamu;
   2) Zona Terbatas — area kerja ASN, ruang rapat, dan koridor OPD;
   3) Zona Aman — ruang telekomunikasi, ruang peralatan TIK, ruang penyimpanan arsip digital, dan *wiring closet*;
   4) Zona Kritis — ruang server, data center, dan ruang penyimpanan media backup.

b. Setiap batas zona keamanan fisik wajib ditandai secara jelas dan dilengkapi mekanisme pengendalian akses yang sesuai dengan tingkat keamanannya.

c. Perimeter fisik Zona Kritis wajib memenuhi persyaratan konstruksi minimal:
   1) dinding, lantai, dan langit-langit yang kokoh dari lantai ke lantai sebenarnya (bukan sekat partisi);
   2) pintu masuk tunggal atau terbatas dengan sistem kunci ganda;
   3) jendela pada area yang dapat diakses dari luar dilengkapi pengamanan fisik yang memadai.

d. Setiap OPD yang menyimpan aset informasi dengan klasifikasi Rahasia wajib memastikan ruang penyimpanan tersebut memiliki minimal: akses terkunci dan tidak dapat diakses oleh pengunjung tanpa pendampingan personel yang berwenang.

e. Akses tamu atau kontraktor ke Zona Aman dan Zona Kritis wajib direncanakan terlebih dahulu, mendapat persetujuan pimpinan yang berwenang, dan dilaksanakan dengan pendampingan personel yang ditunjuk selama berada di area tersebut.

2. Pengendalian Akses Fisik

a. Akses fisik ke Zona Kritis wajib dikendalikan dengan sistem autentikasi berlapis, minimal menggunakan 2 (dua) dari mekanisme berikut:
   1) kartu akses elektronik atau kode PIN;

2) kunci mekanis;
3) autentikasi biometrik.

b. Daftar Personel Berotorisasi Akses Fisik ke Zona Kritis wajib disusun, disahkan oleh pimpinan yang berwenang, dan ditinjau minimal setiap 6 (enam) bulan.
c. Pemberian hak akses fisik wajib melalui proses formal: permohonan tertulis, persetujuan pimpinan yang berwenang, dan pencatatan dalam Daftar Personel Berotorisasi.
d. Hak akses fisik personel yang mutasi, pensiun, atau berhenti wajib dicabut (kartu akses dinonaktifkan, kode PIN diubah) dalam waktu maksimal 1 (satu) hari kerja setelah tanggal efektif perubahan status.
e. Seluruh akses fisik ke Zona Kritis wajib dicatat dalam Log Akses Fisik yang memuat: identitas personel, tanggal dan waktu masuk/keluar, dan tujuan kunjungan.
f. Pengunjung dan kontraktor yang memasuki Zona Aman atau Zona Kritis wajib didampingi, memakai tanda pengenal tamu yang terlihat jelas, dan dicatat dalam Log Kunjungan Tamu.
g. Audit akses fisik wajib dilaksanakan minimal 1 (satu) kali dalam 6 (enam) bulan untuk memverifikasi kesesuaian Daftar Personel Berotorisasi dengan kondisi aktual.

3. Pemantauan Keamanan Fisik

a. Sistem CCTV (*Closed-Circuit Television*):
   1) CCTV wajib dipasang dan beroperasi mencakup seluruh titik akses masuk dan keluar Zona Kritis serta koridor utama menuju area tersebut;
   2) CCTV wajib beroperasi 24 jam sehari, 7 hari seminggu;
   3) kualitas rekaman wajib memadai untuk identifikasi wajah dan aktivitas;
   4) rekaman CCTV wajib disimpan dalam media penyimpanan yang terpisah dari ruang yang dipantau, dengan jangka waktu penyimpanan minimal 90 (sembilan puluh) hari;
   5) akses terhadap rekaman hanya diberikan kepada personel berotorisasi dan setiap akses wajib dicatat.
b. Log Akses Elektronik:
   1) sistem pengendalian akses fisik elektronik wajib menghasilkan log otomatis untuk setiap kejadian masuk dan keluar dari Zona Kritis;
   2) log akses wajib disimpan minimal 90 hari dan dilindungi dari modifikasi;
   3) log akses wajib ditinjau minimal 1 (satu) kali per bulan untuk mendeteksi pola yang mencurigakan.
c. Sistem *Alarm*:
   1) Zona Kritis wajib dilengkapi sistem *alarm* yang aktif saat area tidak berpenghuni, termasuk sensor gerak dan/atau sensor pintu;
   2) alarm wajib terhubung ke petugas keamanan atau personel yang dapat merespons dalam waktu memadai.
d. Pemantauan Lingkungan:
   1) ruang server wajib dilengkapi pemantauan kondisi lingkungan yang mencakup minimal: suhu, kelembapan, dan detektor asap;
   2) hasil pemantauan wajib dicatat secara otomatis dan ditinjau berkala;
   3) nilai ambang batas yang tidak aman wajib dikonfigurasi untuk mengaktifkan notifikasi otomatis.

e. Dalam hal sistem pemantauan mengalami gangguan, tindakan pemantauan manual sementara wajib diterapkan dan dilaporkan kepada pimpinan yang berwenang.

4. Kebijakan Meja Bersih dan Layar Bersih

a. Seluruh perangkat komputer dan laptop dinas wajib dikonfigurasi dengan *screen lock* otomatis yang aktif setelah masa tidak aktif maksimal 5 (lima) menit; konfigurasi ini tidak boleh dinonaktifkan oleh pengguna.
b. Pengguna wajib mengunci layar secara manual setiap kali meninggalkan perangkat meskipun dalam waktu singkat.
c. Dokumen fisik dengan klasifikasi Rahasia atau Terbatas tidak boleh ditinggalkan di meja kerja tanpa pengawasan dan wajib disimpan dalam lemari atau laci terkunci saat tidak digunakan.
d. Media penyimpanan portabel yang berisi data dinas wajib disimpan dalam lemari atau laci terkunci saat tidak digunakan.
e. Pada akhir jam kerja, seluruh ASN wajib memastikan meja kerjanya bebas dari dokumen dan media penyimpanan yang mengandung informasi dinas.
f. Dokumen yang dicetak wajib segera diambil dari baki printer; dokumen Rahasia atau Terbatas tidak boleh dibiarkan di printer tanpa pengawasan. Dokumen cetak yang tidak diperlukan lagi wajib dihancurkan menggunakan mesin penghancur dokumen.
g. Pemeriksaan kepatuhan kebijakan meja bersih dan layar bersih wajib dilaksanakan secara berkala, minimal 1 (satu) kali dalam 3 (tiga) bulan.

5. Penempatan dan Perlindungan Peralatan

a. Server dan perangkat jaringan kritis wajib ditempatkan dalam lemari server (*rack*) yang terkunci di dalam Zona Kritis, dengan mempertimbangkan sirkulasi udara yang memadai.
b. Kabel daya dan kabel data wajib dikelola dengan rapi, diberi label yang jelas, dan dilindungi dari kerusakan fisik.
c. Ruang server wajib dilengkapi sistem pendingin udara yang beroperasi berkelanjutan dengan unit cadangan; suhu wajib dijaga dalam rentang 18–27°C.
d. Ruang server wajib dilengkapi sistem deteksi dan pemadam kebakaran yang sesuai untuk peralatan elektronik.
e. Peralatan TIK tidak boleh ditempatkan di area yang rentan terhadap banjir, bocor, atau paparan langsung sinar matahari.
f. Seluruh peralatan server dan jaringan kritis wajib terhubung dengan *Uninterruptible Power Supply* (UPS) yang mampu memberikan daya cadangan minimal untuk prosedur penghentian sistem yang aman (graceful shutdown); kapasitas UPS wajib diperiksa dan diuji minimal setiap 6 (enam) bulan.
g. Komputer dan laptop dinas wajib ditempatkan sedemikian rupa sehingga layar tidak mudah terlihat oleh pihak yang tidak berkepentingan.
h. Perangkat TIK portabel yang tidak digunakan wajib disimpan di tempat yang aman dan terkunci di luar jam kerja.
i. Inventaris Peralatan TIK wajib disusun dan dimutakhirkan, mencakup spesifikasi, lokasi, status, dan jadwal pemeliharaan.

6. Pengamanan Ruangan dan Fasilitas Khusus

a. Ruangan yang menyimpan informasi Rahasia atau Terbatas wajib dikunci saat tidak digunakan dan aksesnya dibatasi hanya kepada personel berotorisasi.
b. Ruang arsip yang menyimpan dokumen fisik Rahasia wajib memenuhi: pintu dengan kunci ganda atau akses elektronik, dinding dan langit-langit yang memadai, serta pencatatan log akses keluar-masuk.
c. Ruang rapat yang digunakan untuk membahas informasi Rahasia wajib diperiksa dari perangkat perekam tidak sah sebelum digunakan, cukup terisolasi agar pembicaraan tidak terdengar dari luar, dan tidak menggunakan papan tulis yang terlihat dari luar.
d. Ruang penyimpanan backup wajib terpisah secara fisik dari data center utama dan memenuhi perlindungan lingkungan yang memadai.
e. Wiring closet di setiap gedung OPD wajib dikunci dan aksesnya dicatat; hanya personel berotorisasi yang boleh mengakses.

7. Perlindungan terhadap Ancaman Fisik dan Lingkungan

a. Perlindungan Kebakaran:
   1) data center dan ruang server wajib dilengkapi sistem deteksi dan pemadam kebakaran otomatis (*gas clean agent*);
   2) Alat Pemadam Api Ringan (APAR) wajib tersedia dan diperiksa setiap 6 (enam) bulan;
   3) material mudah terbakar dilarang disimpan di ruang server.
b. Perlindungan Banjir:
   1) data center tidak boleh ditempatkan di lantai dasar atau basement gedung di area rawan banjir;
   2) sensor deteksi air (*water leak detector*) wajib dipasang di bawah raised floor data center;
   3) saluran drainase di sekitar ruang server wajib dipelihara.
c. Perlindungan Petir:
   1) gedung yang menampung data center wajib dilengkapi sistem penangkal petir yang terstandar;
   2) perangkat TIK kritis wajib dilindungi *surge protector*.
d. Perlindungan Gempa:
   1) rak server wajib dipasang dengan penguat anti-gempa dan diikat ke lantai;
   2) perangkat kritis pada rak wajib diamankan agar tidak jatuh.
e. Evaluasi risiko ancaman fisik dan lingkungan wajib dilaksanakan minimal setiap 2 (dua) tahun atau setelah kejadian bencana.

8. Bekerja di Area Aman

a. Personel yang memasuki area aman wajib mengetahui keberadaan area tersebut hanya seperlunya (*need-to-know basis*).
b. Kegiatan di area aman tanpa pengawasan dilarang untuk personel yang tidak memiliki akses reguler.
c. Larangan di area aman meliputi:
   1) membawa perangkat perekam (kamera, ponsel dengan kamera) tanpa persetujuan pimpinan yang berwenang;
   2) mengonsumsi makanan dan minuman;
   3) merokok;
   4) menyimpan material yang tidak terkait operasional.
d. Kontraktor dan teknisi eksternal yang bekerja di area aman:
   1) wajib didampingi personel berotorisasi setiap saat;
   2) wajib menandatangani log pengunjung;

3) peralatan kerja wajib diperiksa sebelum masuk dan sebelum keluar;
4) akses diberikan hanya untuk durasi pekerjaan yang dibutuhkan.

e. Area aman wajib dikunci dan diperiksa secara berkala saat tidak berpenghuni.

9. Utilitas Pendukung

a. Kelistrikan:
1) data center wajib memiliki suplai listrik dari minimal 2 (dua) sumber independen;
2) UPS wajib menyediakan daya cadangan minimal 30 (tiga puluh) menit untuk seluruh perangkat kritis;
3) generator cadangan wajib mampu beroperasi minimal 24 (dua puluh empat) jam dan diuji setiap 3 (tiga) bulan;
4) peralihan daya wajib melalui *Automatic Transfer Switch* (ATS) yang diuji secara berkala.

b. Pendingin:
1) suhu ruang server wajib dijaga pada rentang 18–27°C dengan kelembaban 40–60%;
2) sistem pendingin wajib memiliki unit cadangan (N+1 *redundancy*);
3) sensor suhu dan kelembaban wajib dipasang dan terintegrasi dengan sistem monitoring.

c. Pemeriksaan dan pemeliharaan utilitas pendukung wajib dilaksanakan sesuai jadwal yang ditetapkan dan didokumentasikan.

d. Gangguan utilitas pendukung wajib dilaporkan segera dan ditangani sebagai prioritas tinggi.

10. Keamanan Kabel

a. Kabel jaringan backbone antar-gedung OPD wajib melalui jalur yang terlindungi (*conduit/duct* tertutup) dan didokumentasikan jalurnya pada peta kabel.

b. Kabel daya dan kabel data wajib dipisahkan secara fisik untuk mencegah interferensi elektromagnetik.

c. Seluruh kabel di ruang server dan *wiring closet* wajib diberi label yang jelas sesuai standar pelabelan yang ditetapkan.

d. *Patch* panel dan *port* jaringan yang tidak digunakan wajib dinonaktifkan atau ditutup secara fisik.

e. Akses ke jalur kabel wajib dikunci dan dibatasi kepada personel berotorisasi.

f. Inspeksi fisik kabel wajib dilaksanakan minimal 1 (satu) kali per tahun untuk mendeteksi kerusakan atau pemasangan perangkat tidak sah.

11. Pemeliharaan Peralatan

a. Jadwal Pemeliharaan Preventif wajib disusun untuk seluruh perangkat kritis, minimal:
1) server dan storage: setiap 6 (enam) bulan;
2) perangkat jaringan: setiap 6 (enam) bulan;
3) UPS dan generator: setiap 3 (tiga) bulan;
4) sistem pendingin: setiap 3 (tiga) bulan;
5) perangkat keamanan fisik (CCTV, akses kontrol): setiap 6 (enam) bulan.

b. Seluruh pemeliharaan wajib dicatat dalam Rekaman Pemeliharaan yang memuat: perangkat, tanggal, jenis pemeliharaan, pelaksana, dan temuan/tindakan.

c. Pemeliharaan oleh teknisi eksternal/vendor:
   1) wajib mendapat persetujuan dari pimpinan yang berwenang;
   2) teknisi wajib didampingi personel berotorisasi;
   3) media dan perangkat yang dibawa masuk/keluar wajib diperiksa;
   4) data sensitif pada perangkat yang akan diperbaiki di luar lokasi wajib dihapus terlebih dahulu atau dienkripsi.
d. Perangkat yang gagal diperbaiki wajib ditangani sesuai prosedur pembuangan aman sebagaimana diatur pada ketentuan angka 12 bab ini.

12. Pembuangan dan Penggunaan Ulang Peralatan Secara Aman

a. Klasifikasi Peralatan Sebelum Pembuangan:
   1) sebelum dibuang atau dialihfungsikan, peralatan wajib diklasifikasikan berdasarkan level klasifikasi tertinggi data yang pernah tersimpan atau diproses;
   2) metode sanitasi data wajib sesuai dengan klasifikasi tersebut.
b. Prosedur Sanitasi Data per Jenis Media:

Jenis Media	Prosedur Sanitasi
HDD (Rahasia)	Degaussing atau penghancuran fisik (shredding/crushing/drilling)
HDD (Terbatas)	Overwrite minimal 3 pass atau degaussing
SSD (Rahasia)	*Cryptographic erase* + penghancuran fisik
SSD (Terbatas)	*Cryptographic erase* atau *Secure Erase*
USB/Kartu Memori	*Overwrite* + format atau penghancuran
Perangkat cetak (*printer*/MFP)	Reset pabrik; hapus memori dan hard disk internal
Ponsel/Tablet	*Factory reset* + hapus kartu SIM dan kartu memori; verifikasi penghapusan
Perangkat jaringan	Reset konfigurasi ke *default* pabrik; hapus log dan kredensial tersimpan

Tabel 7. Prosedur sanitasi data per jenis media

c. Sertifikat Penghancuran:
   1) untuk peralatan yang dimusnahkan secara fisik, wajib diterbitkan Sertifikat Penghancuran yang memuat: deskripsi perangkat (*serial number*), metode penghancuran, tanggal, dan pelaksana;
   2) apabila penghancuran dilaksanakan oleh pihak ketiga, Sertifikat Penghancuran dari vendor wajib diperoleh;
   3) penghancuran media data Rahasia direkomendasikan disaksikan oleh minimal 2 (dua) personel berotorisasi.
d. Penggunaan Ulang:
   1) peralatan yang akan digunakan ulang oleh OPD lain wajib melalui sanitasi data lengkap dan instalasi ulang sistem operasi yang bersih;

2) peralatan yang akan didonasikan ke pihak luar wajib melalui sanitasi data sesuai level Rahasia untuk jaminan keamanan maksimum.

e. Pembuangan peralatan yang pernah memproses data pribadi wajib memastikan seluruh data pribadi telah terhapus secara permanen sesuai ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

f. Pembuangan peralatan wajib mengikuti prosedur penghapusan Barang Milik Daerah (BMD) yang berlaku.

BAB VI
PENGENDALIAN TEKNOLOGI DAN INFRASTRUKTUR

A. Maksud dan Tujuan

Menetapkan pengendalian teknis pada perangkat pengguna akhir, hak akses sistem, mekanisme autentikasi, perlindungan terhadap malware, manajemen kerentanan, pencegahan kebocoran data, pencadangan informasi, pencatatan log, keamanan jaringan, serta penggunaan kriptografi dan tanda tangan elektronik - guna melindungi kerahasiaan, integritas, dan ketersediaan aset informasi Pemerintah Kabupaten Kendal secara menyeluruh.

B. Ruang Lingkup

Seluruh perangkat keras, perangkat lunak, jaringan, server, basis data, dan sistem informasi yang digunakan untuk penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di lingkungan Pemerintah Kabupaten Kendal, meliputi perangkat endpoint milik dinas maupun perangkat pribadi (*BYOD*) yang mengakses sistem dinas.

C. Ketentuan

1. Keamanan Perangkat Pengguna Akhir

a. Standar Konfigurasi Keamanan Perangkat *Endpoint* wajib ditetapkan untuk seluruh perangkat yang terhubung ke jaringan dan/atau sistem informasi Pemerintah Kabupaten Kendal, mencakup minimal:
   1) sistem operasi pada versi yang masih mendapat dukungan keamanan dari pabrikan;
   2) pembaruan keamanan (*security patch*) diterapkan dalam waktu maksimal 14 (empat belas) hari kalender sejak dirilis, atau segera untuk *patch* kritis;
   3) perangkat lunak *antivirus/antimalware* terpasang dan aktif dengan definisi yang diperbarui secara otomatis;
   4) *firewall* lokal diaktifkan;
   5) enkripsi penyimpanan (*full disk encryption*) diaktifkan pada perangkat portabel yang menyimpan data dinas.

b. Perangkat portabel milik dinas yang dibawa ke luar kantor wajib mendapat persetujuan tertulis dari pimpinan OPD dan dicatat dalam Log Peminjaman Perangkat.

c. Penggunaan perangkat pribadi (*BYOD*) untuk mengakses sistem informasi dinas hanya diizinkan apabila:
   1) mendapat persetujuan pimpinan OPD;
   2) perangkat memenuhi standar konfigurasi keamanan minimum;
   3) pengguna menandatangani Pernyataan Kepatuhan *BYOD* yang mencakup kesediaan penghapusan data dinas secara jarak jauh (*remote wipe*) apabila diperlukan.

d. Kehilangan atau pencurian perangkat yang menyimpan data dinas wajib dilaporkan kepada pengelola sistem dan pimpinan OPD dalam waktu maksimal 1×24 jam dan ditindaklanjuti sesuai prosedur manajemen insiden.

e. Perangkat yang tidak lagi digunakan (*end-of-life*) wajib melalui prosedur sanitasi data yang aman sebelum dimusnahkan atau dialihfungsikan sebagaimana diatur dalam BAB V dokumen ini.

f. Inventarisasi dan verifikasi kepatuhan perangkat endpoint terhadap standar konfigurasi wajib dilaksanakan minimal 1 (satu) kali dalam 6 (enam) bulan.

2. Hak Akses Istimewa

a. Prinsip pemberian hak akses istimewa:
   1) hak akses istimewa hanya diberikan berdasarkan kebutuhan tugas (*need-to-use*) dan bersifat sementara apabila dimungkinkan;
   2) setiap personel yang memiliki hak akses istimewa wajib memiliki akun reguler terpisah untuk aktivitas harian non-administratif;
   3) jumlah personel yang memiliki hak akses istimewa pada setiap sistem wajib dibatasi seminimal mungkin.

b. Prosedur pemberian hak akses istimewa:
   1) permohonan wajib diajukan secara tertulis dengan menyebutkan sistem tujuan, justifikasi, dan jangka waktu;
   2) persetujuan untuk sistem tingkat OPD diberikan oleh pimpinan OPD;
   3) persetujuan untuk infrastruktur kritis terpusat (*data center*, jaringan *backbone*, server utama) diberikan oleh pimpinan unit kerja yang membidangi TIK;
   4) setiap pemberian wajib dicatat dalam Register Hak Akses Istimewa.

c. Pengelolaan akun istimewa:
   1) kata sandi akun istimewa: minimal 14 (empat belas) karakter, kombinasi huruf besar, huruf kecil, angka, dan karakter khusus, diganti setiap 60 (enam puluh) hari;
   2) penggunaan akun bersama (*shared privileged account*) dilarang;
   3) akun layanan (*service account*) dengan hak istimewa wajib dikelola dengan kata sandi terenkripsi dan akses terbatas pada fungsi otomatis yang ditentukan.

d. Pemantauan dan peninjauan:
   1) seluruh aktivitas akun istimewa wajib dicatat dalam log yang dilindungi dari modifikasi;
   2) log aktivitas akun istimewa wajib ditinjau minimal 1 (satu) kali per bulan;
   3) peninjauan hak akses istimewa wajib dilaksanakan setiap 3 (tiga) bulan;
   4) hak akses istimewa personel yang mutasi, pensiun, atau berhenti wajib dicabut dalam waktu maksimal 4 (empat) jam setelah tanggal efektif perubahan status.

3. Pembatasan Akses Informasi

a. Setiap sistem informasi wajib menerapkan mekanisme pembatasan akses berbasis peran (*role-based access control/RBAC*) yang membatasi pengguna hanya pada fungsi dan data yang diperlukan sesuai tugasnya.

b. Matriks peran dan hak akses (*role-access matrix*) wajib didefinisikan, didokumentasikan, dan disahkan oleh pimpinan OPD untuk setiap sistem informasi.

c. Akses terhadap data dengan klasifikasi Rahasia wajib dibatasi hanya kepada personel yang tercantum dalam daftar akses yang disahkan, dan setiap akses wajib dicatat dalam log.

d. Sistem informasi wajib menampilkan hanya menu, fungsi, dan data yang relevan dengan peran pengguna yang sedang login.

e. Perubahan terhadap konfigurasi pembatasan akses wajib melalui prosedur manajemen perubahan dan didokumentasikan.

4. Autentikasi Aman

a. Standar kata sandi minimum untuk akun reguler:
   1) panjang minimal 8 (delapan) karakter;
   2) kombinasi minimal 3 dari 4 kategori: huruf besar, huruf kecil, angka, dan karakter khusus;
   3) diganti setiap 90 (sembilan puluh) hari;
   4) sistem wajib mencegah penggunaan ulang 5 (lima) kata sandi terakhir;
   5) akun terkunci otomatis setelah 5 (lima) kali percobaan login gagal berturut-turut, dengan periode kunci minimal 15 (lima belas) menit.

b. Autentikasi Multi-Faktor (*MFA*):
   1) wajib diterapkan pada akun istimewa untuk seluruh sistem kritis;
   2) wajib diterapkan pada akses jarak jauh (*remote access/ VPN*);
   3) direkomendasikan untuk akses ke sistem yang memproses data pribadi dan data keuangan.

c. Seluruh sistem informasi wajib menampilkan peringatan keamanan pada halaman login yang memuat pernyataan bahwa sistem hanya untuk pengguna berotorisasi dan aktivitas dapat dipantau.

d. Batas waktu sesi otomatis (session timeout) wajib diterapkan: maksimal 15 (lima belas) menit untuk sistem kritis dan 30 (tiga puluh) menit untuk sistem non-kritis.

e. Transmisi kredensial autentikasi wajib dilindungi dengan enkripsi (*HTTPS/ TLS*) dan kata sandi wajib disimpan dalam bentuk *hash* yang aman pada basis data.

5. Perlindungan terhadap Malware

a. Seluruh perangkat endpoint dan server wajib dilengkapi perangkat lunak *anti-malware* yang:
   4) berlisensi resmi dan berasal dari penyedia terpercaya;
   5) definisi *malware* diperbarui secara otomatis minimal 1 (satu) kali per hari;
   6) pemindaian real-time diaktifkan;
   7) pemindaian menyeluruh (*full scan*) terjadwal minimal 1 (satu) kali per minggu.

b. Pengguna dilarang menonaktifkan perangkat lunak *anti-malware* tanpa persetujuan tertulis dari pengelola sistem dengan alasan teknis yang terdokumentasi.

c. Perlindungan *anti-malware* pada tingkat jaringan (*gateway*) wajib diterapkan untuk menyaring lalu lintas masuk, termasuk pemindaian email dan unduhan berkas dari internet.

d. Dalam hal terdeteksi infeksi malware:
   1) perangkat yang terinfeksi wajib segera diisolasi dari jaringan;
   2) kejadian wajib dilaporkan sebagai insiden keamanan informasi sesuai prosedur manajemen insiden;
   3) pemulihan perangkat hanya boleh dilakukan setelah dipastikan bersih dari *malware*.

e. Efektivitas solusi *anti-malware* wajib dievaluasi minimal 1 (satu) kali per tahun.

f. Seluruh ASN wajib mendapat edukasi tentang ancaman malware sebagai bagian dari program pelatihan keamanan informasi.

6. Manajemen Kerentanan Teknis

a. Sumber informasi kerentanan yang tepercaya wajib dipantau secara aktif, meliputi: pemberitahuan dari BSSN, CVE (*Common*

Vulnerabilities and Exposures), dan buletin keamanan dari vendor/pabrikan.

b. Pemindaian kerentanan (*vulnerability scanning*) terhadap infrastruktur kritis dan sistem yang terekspos ke internet wajib dilaksanakan minimal 1 (satu) kali dalam 3 (tiga) bulan, atau segera setelah adanya pemberitahuan kerentanan kritis.
c. Prioritas penanganan kerentanan berdasarkan tingkat keparahan:
   1) Kritis (*CVSS* ≥ 9.0): perbaikan dalam 7 (tujuh) hari kalender;
   2) Tinggi (*CVSS* 7.0–8.9): perbaikan dalam 14 (empat belas) hari;
   3) Sedang (*CVSS* 4.0–6.9): perbaikan dalam 30 (tiga puluh) hari;
   4) Rendah (*CVSS* < 4.0): perbaikan pada siklus pembaruan berikutnya.
d. Penerapan *patch* wajib melalui tahap pengujian pada lingkungan uji sebelum diterapkan pada lingkungan produksi, kecuali dalam kondisi darurat yang disetujui pimpinan yang berwenang.
e. Apabila *patch* belum tersedia atau tidak dapat segera diterapkan, kontrol kompensasi sementara wajib diterapkan dan didokumentasikan.
f. Laporan Status Kerentanan wajib disusun secara triwulanan.

7. Pencegahan Kebocoran Data

a. Langkah pencegahan kebocoran data wajib diterapkan, mencakup minimal:
   1) pembatasan penggunaan media penyimpanan portabel (*USB*) pada perangkat dinas melalui kebijakan teknis;
   2) pemantauan lalu lintas email dinas untuk mendeteksi pengiriman data Rahasia ke alamat email eksternal yang tidak berotorisasi;
   3) pembatasan akses ke layanan penyimpanan awan publik yang tidak disetujui dari jaringan dinas.
b. Pengiriman data Rahasia ke luar jaringan wajib menggunakan mekanisme perlindungan (enkripsi, kata sandi lampiran).
c. Sistem wajib dikonfigurasi untuk mencegah pencetakan, penyalinan layar, atau pengunduhan massal data Rahasia tanpa otorisasi, sejauh dimungkinkan secara teknis.
d. Kebutuhan penerapan solusi *Data Loss Prevention* (DLP) wajib dievaluasi secara berkala berdasarkan hasil penilaian risiko.
e. Seluruh insiden kebocoran data atau dugaan kebocoran wajib dilaporkan dan ditangani sesuai prosedur manajemen insiden.

8. Pencadangan Informasi (Backup)

a. Frekuensi backup:
   1) backup harian (*incremental*) untuk seluruh basis data sistem kritis;
   2) backup mingguan (*full backup*) untuk seluruh sistem informasi kritis;
   3) backup bulanan (*full backup* arsip) sebagai backup jangka panjang;
   4) backup konfigurasi setiap kali terdapat perubahan pada server, perangkat jaringan, firewall, dan sistem kritis.
b. Lokasi penyimpanan backup:
   1) backup utama pada media yang terpisah secara fisik dari server produksi;
   2) salinan backup (*off-site backup*) pada lokasi terpisah secara geografis dari lokasi utama;

3) lokasi *off-site* wajib memenuhi persyaratan keamanan fisik dan pengendalian akses yang setara;
4) apabila digunakan penyimpanan awan (*cloud backup*), data wajib dienkripsi sebelum diunggah.

c. Perlindungan backup:
1) seluruh media backup wajib dienkripsi;
2) akses terhadap media dan sistem backup hanya untuk personel berotorisasi;
3) media *backup* fisik wajib disimpan dalam ruang yang terkunci di area aman;
4) integritas *backup* wajib diverifikasi setelah setiap proses pencadangan.

d. Uji pemulihan (*restore test*) wajib dilaksanakan minimal 2 (dua) kali dalam 1 (satu) tahun untuk setiap sistem kritis, mencakup pemulihan penuh dan pemulihan parsial. Hasil wajib didokumentasikan.

e. Retensi backup:
1) *backup* harian: minimal 30 (tiga puluh) hari;
2) *backup* mingguan: minimal 3 (tiga) bulan;
3) *backup* bulanan: minimal 1 (satu) tahun;
4) *backup* yang tunduk pada ketentuan retensi khusus mengikuti peraturan perundang-undangan yang berlaku.

f. Seluruh aktivitas *backup* dan *restore* wajib dicatat dalam Log *Backup*.

9. Pencatatan Log

a. Jenis aktivitas yang wajib dicatat dalam log mencakup minimal:
1) login berhasil dan gagal;
2) aktivitas akun istimewa;
3) akses terhadap data Rahasia dan Terbatas;
4) perubahan konfigurasi sistem dan keamanan;
5) aktivitas *backup* dan *restore*;
6) kejadian keamanan yang terdeteksi oleh perangkat keamanan;
7) *start-up* dan *shutdown* sistem.

b. Setiap entri log wajib mencakup minimal: tanggal dan waktu kejadian (tersinkronisasi *NTP*), identitas pengguna atau proses, jenis aktivitas, sumber (alamat IP/*hostname*), objek yang diakses, dan status (berhasil/gagal).

c. Retensi log:
1) log sistem kritis: minimal 12 (dua belas) bulan;
2) log sistem non-kritis: minimal 6 (enam) bulan;
3) log yang berkaitan dengan insiden keamanan informasi disimpan hingga investigasi dan tindak lanjut selesai.

d. Perlindungan integritas log:
1) log wajib dilindungi dari modifikasi, penghapusan, dan akses tidak sah;
2) pengelola sistem yang dimonitor tidak boleh memiliki kemampuan memodifikasi atau menghapus log aktivitasnya sendiri;
3) log dari sistem kritis wajib dikirim ke *server log* terpusat yang dikelola secara terpisah;
4) sinkronisasi waktu (*NTP*) wajib diterapkan pada seluruh perangkat untuk konsistensi *timestamp*.

e. Peninjauan log:
1) log sistem kritis ditinjau minimal 1 (satu) kali per minggu;
2) log akun istimewa ditinjau minimal 1 (satu) kali per bulan;

3) anomali yang ditemukan wajib dilaporkan dan ditangani sebagai insiden.

10. Keamanan Jaringan

a. Segmentasi jaringan:
   1) jaringan wajib disegmentasi minimal menjadi: zona server/ *data center*, zona kerja internal OPD, zona layanan publik (*DMZ*), dan zona tamu/internet;
   2) lalu lintas antar-zona wajib dikendalikan melalui *firewall* dengan prinsip *deny-by-default*;
   3) sistem yang memproses data Rahasia wajib ditempatkan pada segmen jaringan yang terisolasi.

b. Perangkat keamanan jaringan:
   1) *firewall* wajib terpasang pada setiap titik perbatasan jaringan dan antar-zona;
   2) sistem deteksi dan/atau pencegahan intrusi (*IDS/IPS*) wajib dioperasikan pada jaringan utama;
   3) aturan *firewall* dan *IDS/IPS* wajib ditinjau minimal 1 (satu) kali dalam 6 (enam) bulan.

c. Keamanan jaringan nirkabel (*Wi-Fi*):
   1) jaringan *Wi-Fi* dinas wajib menggunakan protokol enkripsi minimal *WPA3* atau *WPA2-Enterprise*;
   2) jaringan *Wi-Fi* untuk tamu wajib dipisahkan dari jaringan internal;
   3) *SSID* jaringan internal tidak dipublikasikan apabila dimungkinkan secara teknis.

d. Akses jarak jauh (*remote access*):
   1) akses jarak jauh ke jaringan dan sistem informasi hanya diizinkan melalui *VPN* terenkripsi;
   2) *VPN* wajib dikombinasikan dengan autentikasi multi-faktor;
   3) pemberian akses *VPN* wajib mendapat persetujuan pimpinan yang berwenang dan dicatat.

e. Pemantauan jaringan:
   1) lalu lintas jaringan wajib dipantau secara berkelanjutan untuk mendeteksi anomali dan serangan;
   2) log perangkat jaringan wajib dikirim ke *server log* terpusat;
   3) laporan status keamanan jaringan wajib disusun minimal setiap bulan.

f. Diagram topologi jaringan wajib disusun, dimutakhirkan, dan diklasifikasikan sebagai informasi Terbatas.

11. Penggunaan Kriptografi dan Tanda Tangan Elektronik

a. Kebijakan penggunaan kriptografi wajib ditetapkan yang mengatur jenis algoritma, panjang kunci, dan protokol enkripsi yang disetujui. Algoritma wajib mengacu pada standar yang diakui secara internasional dan/atau direkomendasikan oleh BSSN. Kebijakan ditinjau minimal 1 (satu) kali per tahun.

b. Penerapan enkripsi wajib pada:
   1) transmisi data melalui jaringan publik menggunakan protokol *TLS* versi 1.2 atau lebih baru;
   2) penyimpanan data Rahasia pada server dan basis data;
   3) media penyimpanan portabel yang berisi data dinas;
   4) media backup;
   5) koneksi *VPN*.

c. Seluruh aplikasi SPBE yang dapat diakses publik wajib menggunakan sertifikat *SSL/TLS* yang valid.

d. Tanda Tangan Elektronik (TTE):
    1) TTE yang digunakan oleh pejabat struktural wajib merupakan Tanda Tangan Elektronik Tersertifikasi sebagaimana dimaksud dalam peraturan perundang-undangan yang berlaku, yang diterbitkan oleh Penyelenggara Sertifikasi Elektronik yang diakui;
    2) setiap pejabat yang diwajibkan menggunakan TTE wajib memiliki sertifikat elektronik aktif;
    3) sertifikat elektronik pejabat yang mutasi, pensiun, atau berhenti wajib dicabut dalam waktu maksimal 1 (satu) hari kerja setelah tanggal efektif perubahan status.
e. Pengelolaan kunci kriptografi:
    1) kunci dihasilkan menggunakan metode yang aman dan acak;
    2) kunci privat wajib dilindungi dari akses tidak sah dan disimpan dalam media yang aman;
    3) kunci wajib diganti sesuai masa berlaku atau segera apabila terdapat indikasi kompromi;
    4) kunci yang tidak digunakan wajib dihancurkan secara aman;
    5) Inventaris Kunci Kriptografi dan Sertifikat Elektronik wajib dikelola.

BAB VII
MANAJEMEN INSIDEN KEAMANAN INFORMASI

A. Maksud dan Tujuan

Menetapkan prosedur yang terstruktur untuk menilai, merespons, mendokumentasikan, dan mengambil pembelajaran dari setiap insiden keamanan informasi di lingkungan Pemerintah Kabupaten Kendal, termasuk prosedur pengumpulan dan pengelolaan bukti digital yang dapat dipertanggungjawabkan secara hukum — guna meminimalkan dampak insiden dan mencegah terulangnya kejadian serupa.

B. Ruang Lingkup

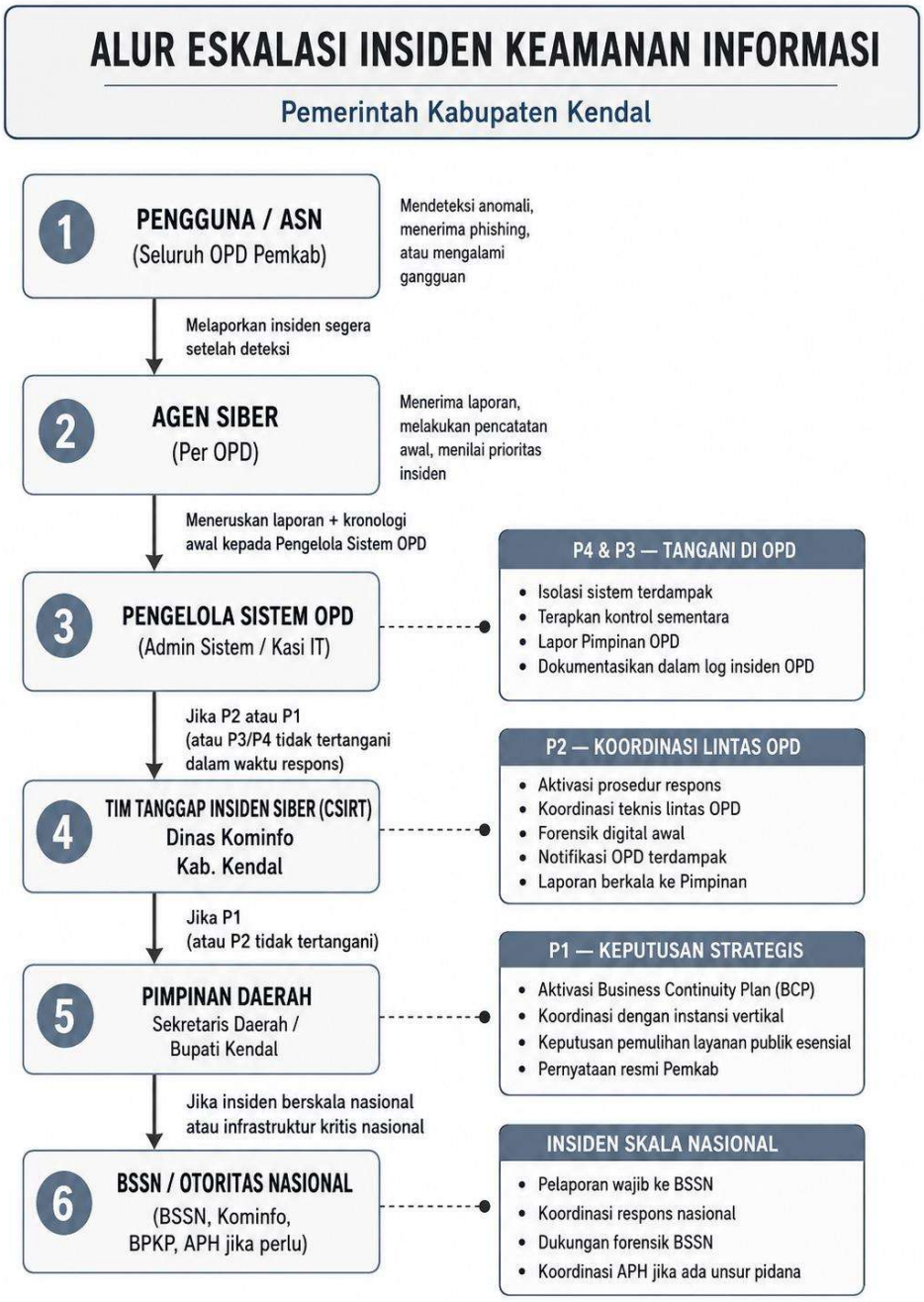
Seluruh kejadian dan insiden keamanan informasi yang terjadi pada sistem informasi, infrastruktur TIK, dan aset informasi di lingkungan Pemerintah Kabupaten Kendal, baik yang dilaporkan oleh personel, terdeteksi oleh sistem pemantauan, maupun diinformasikan oleh pihak eksternal.

C. Ketentuan

1. Penilaian dan Klasifikasi Kejadian Keamanan Informasi

a. Setiap kejadian keamanan informasi yang diterima melalui kanal pelaporan wajib dinilai oleh personel yang kompeten untuk menentukan apakah kejadian tersebut memenuhi kriteria sebagai insiden keamanan informasi.
b. Batas waktu penilaian awal sejak laporan diterima:
    1) kejadian yang diduga berdampak kritis: penilaian dalam 30 (tiga puluh) menit;
    2) kejadian lainnya: penilaian dalam 4 (empat) jam kerja.
c. Kriteria penilaian mencakup minimal:
    1) jenis dan sifat kejadian (teknis, non-teknis, disengaja, tidak disengaja);
    2) aset informasi yang terdampak atau berpotensi terdampak;
    3) cakupan dampak (satu pengguna, satu OPD, lintas OPD, atau seluruh Pemerintah Kabupaten Kendal);
    4) potensi keterlibatan data pribadi;
    5) potensi gangguan terhadap layanan publik.
d. Klasifikasi tingkat keparahan insiden:
    1) Prioritas 1 (Kritis) — gangguan total layanan publik, kebocoran data pribadi skala besar, atau ancaman keselamatan;
    2) Prioritas 2 (Tinggi) — gangguan signifikan atau potensi kebocoran data terbatas;
    3) Prioritas 3 (Sedang) — dampak terbatas pada operasional internal;
    4) Prioritas 4 (Rendah) — peristiwa yang memerlukan pencatatan tanpa dampak operasional langsung.

e. Alur eskalasi berdasarkan tingkat keparahan:



Gambar 1. Alur eskalasi insiden keamanan informasi

f. Kejadian yang dinilai bukan merupakan insiden (*false positive*) wajib tetap dicatat dalam Log Kejadian beserta alasan keputusan.
g. Apabila tingkat keparahan aktual berbeda dari penilaian awal, reklasifikasi wajib dilakukan segera dan eskalasi disesuaikan.

2. Respons terhadap Insiden Keamanan Informasi

a. Batas waktu respons berdasarkan tingkat keparahan:

Prioritas	Batas Respons	Keterangan
1 (Kritis)	Maks. 1 jam	Mobilisasi CSIRT segera; eskalasi ke pimpinan
2 (Tinggi)	Maks. 4 jam	CSIRT mulai penanganan
3 (Sedang)	Maks. 24 jam	Pengelola sistem OPD

4 (Rendah)	Maks. 3 hari kerja	Pencatatan dan penanganan rutin

Tabel 8. Respons insiden keamanan informasi

b. Fase penanganan insiden (6 fase berurutan):

Fase 1 — Identifikasi dan Konfirmasi: mengonfirmasi insiden berdasarkan hasil penilaian; mendokumentasikan informasi awal meliputi waktu, sistem terdampak, dan gejala yang teramati.

Fase 2 — Penahanan (Containment): melaksanakan tindakan segera untuk membatasi penyebaran dan dampak insiden, termasuk: isolasi sistem atau segmen jaringan, penonaktifan akun yang terkompromi, dan pemblokiran alamat IP atau domain berbahaya.

Fase 3 — Pemberitahuan dan Eskalasi: melaksanakan pemberitahuan dan eskalasi sesuai alur yang ditetapkan. Untuk insiden yang melibatkan data pribadi, notifikasi kepada subjek data dan otoritas pengawas wajib dilaksanakan dalam waktu maksimal 3×24 jam.

Fase 4 — Eradikasi: menghilangkan akar penyebab insiden, termasuk: pembersihan malware, penutupan kerentanan, penghapusan akses tidak sah, dan perbaikan konfigurasi.

Fase 5 — Pemulihan (Recovery): memulihkan sistem dan layanan ke kondisi operasional normal, termasuk: restore data dari backup yang bersih, verifikasi integritas sistem, pengaktifan kembali layanan secara bertahap, dan pemantauan intensif pasca pemulihan selama minimal 72 (tujuh puluh dua) jam.

Fase 6 — Penutupan dan Dokumentasi: menutup penanganan insiden setelah memastikan seluruh dampak telah ditangani; menyusun Laporan Pasca Insiden.

c. Selama penanganan insiden Prioritas 1 dan 2, laporan perkembangan (status update) wajib disampaikan setiap 2 (dua) jam hingga insiden terkendali.
d. Komunikasi tentang insiden kepada pihak eksternal (media, masyarakat) hanya boleh dilakukan oleh pejabat yang ditunjuk.
e. Seluruh aktivitas penanganan insiden wajib dicatat secara kronologis dalam Log Penanganan Insiden.

3. Pembelajaran dari Insiden Keamanan Informasi

a. Setiap insiden dengan Prioritas 1, 2, dan 3 wajib diikuti Tinjauan Pasca Insiden (*Post-Incident Review*) dalam waktu maksimal 14 (empat belas) hari kerja setelah insiden dinyatakan selesai.
b. Laporan Pasca Insiden wajib mencakup minimal:
   1) kronologi insiden secara lengkap;
   2) akar penyebab (*root cause analysis*);
   3) aset dan layanan yang terdampak;
   4) efektivitas respons dan penanganan;
   5) dampak aktual (operasional, finansial, reputasi, hukum);
   6) kelemahan kontrol yang teridentifikasi;
   7) rekomendasi perbaikan spesifik dan terukur;
   8) penanggung jawab dan tenggat waktu implementasi rekomendasi.
c. Rekomendasi perbaikan wajib diintegrasikan ke dalam Register Risiko dan Rencana Penanganan Risiko sebagaimana diatur dalam BAB II dokumen ini.

d. Laporan Ringkasan Insiden Tahunan wajib disusun yang mengkonsolidasikan seluruh insiden, tren ancaman, dan status implementasi rekomendasi perbaikan.
e. Pembelajaran dari insiden (*lessons learned*) wajib digunakan untuk:
   1) memperbarui materi pelatihan kesadaran keamanan informasi;
   2) memperbaiki prosedur penanganan insiden;
   3) memperkuat skenario simulasi insiden;
   4) memperbarui penilaian risiko pada aset dan ancaman terkait.
f. Insiden Prioritas 4 wajib didokumentasikan dalam Log Insiden dan ditinjau secara agregat dalam laporan tahunan.

4. Pengumpulan dan Pengelolaan Bukti Digital

a. Prinsip pengumpulan bukti digital:
   1) Legalitas — sesuai peraturan perundang-undangan yang berlaku;
   2) Integritas — bukti dijaga keutuhan dan keasliannya;
   3) Rantai Pengamanan (*Chain of Custody*) — setiap perpindahan, akses, dan penyimpanan bukti dicatat secara kronologis;
   4) Reprodusibilitas — proses pengumpulan dapat diulang dengan hasil yang konsisten.
b. Prosedur pengumpulan bukti:
   1) pengumpulan dilakukan oleh personel yang memiliki kompetensi forensik digital atau di bawah supervisi personel yang kompeten;
   2) langkah minimal: dokumentasi kondisi awal sistem, pembuatan salinan forensik menggunakan write-blocker, penghitungan nilai *hash* (*SHA-256* atau lebih kuat), dan pencatatan metadata;
   3) bukti asli wajib diamankan dan tidak digunakan untuk analisis; seluruh analisis dilakukan pada salinan forensik;
   4) apabila bukti bersifat volatil (RAM, koneksi jaringan aktif), pengamanan bukti volatil wajib diprioritaskan sebelum tindakan penahanan.
c. Rantai Pengamanan Bukti (*Chain of Custody*):
   1) setiap bukti digital wajib dilengkapi Formulir Rantai Pengamanan yang mencatat: identitas bukti, pelaksana pengumpulan, tanggal/waktu perpindahan, penerima, tujuan akses, dan kondisi penyimpanan;
   2) bukti digital wajib disimpan dalam media penyimpanan yang terkunci dan terlindungi;
   3) setiap akses terhadap bukti wajib dicatat dan disetujui oleh penanggung jawab investigasi.
d. Koordinasi dengan pihak berwenang:
   1) untuk insiden yang diduga mengandung unsur pidana, wajib berkoordinasi dengan Inspektorat dan/atau aparat penegak hukum sebelum tindakan yang dapat memengaruhi bukti;
   2) penyerahan bukti dilakukan secara resmi dengan Berita Acara Serah Terima Bukti Digital;
   3) salinan seluruh bukti yang diserahkan wajib disimpan.
e. Retensi bukti digital:
   1) disimpan minimal hingga proses investigasi dan tindak lanjut selesai;
   2) untuk insiden tanpa implikasi hukum: minimal 2 (dua) tahun;
   3) pemusnahan bukti wajib mendapat persetujuan pimpinan yang berwenang dan didokumentasikan.
f. Peralatan dan perangkat lunak forensik digital dasar wajib tersedia, dan minimal 2 (dua) personel teknis wajib memiliki kompetensi dasar forensik digital.

BAB VIII
KEAMANAN PIHAK KETIGA

A. Maksud dan Tujuan

Memastikan bahwa aset informasi dan sistem TIK Pemerintah Kabupaten Kendal tetap terlindungi dari risiko yang ditimbulkan oleh hubungan dengan pihak ketiga, melalui identifikasi dan penilaian risiko sebelum perjanjian, penetapan klausul keamanan dalam kontrak, pengelolaan keamanan rantai pasokan, serta pemantauan dan tinjauan berkala selama masa perjanjian berlangsung.

B. Ruang Lingkup

Seluruh hubungan dengan pihak ketiga yang memiliki akses atau berpotensi memengaruhi keamanan informasi dan infrastruktur TIK Pemerintah Kabupaten Kendal, meliputi: vendor pengembang aplikasi, penyedia layanan cloud, kontraktor pemeliharaan, mitra integrasi data antar-instansi, konsultan, dan auditor eksternal.

C. Ketentuan

1. Penilaian Risiko dan Klasifikasi Pihak Ketiga

a. Sebelum menjalin hubungan kerja dengan pihak ketiga yang akan memiliki akses ke sistem informasi atau aset informasi, penilaian risiko pihak ketiga wajib dilaksanakan yang mencakup minimal:
   1) identifikasi jenis akses yang diperlukan (fisik, logis, atau akses terhadap data pribadi);
   2) penilaian kapabilitas keamanan informasi pihak ketiga;
   3) identifikasi risiko rantai pasokan dan ketergantungan pada sub-kontraktor.

b. Klasifikasi pihak ketiga berdasarkan tingkat risiko:
   1) Risiko Tinggi — pihak ketiga yang memiliki akses langsung ke data Rahasia, sistem kritis, atau infrastruktur utama;
   2) Risiko Sedang — pihak ketiga yang memiliki akses ke sistem dengan data Terbatas atau menyediakan layanan pendukung;
   3) Risiko Rendah — pihak ketiga yang tidak memiliki akses langsung ke sistem atau data sensitif.

c. Pihak ketiga dengan klasifikasi Risiko Tinggi wajib menunjukkan bukti penerapan keamanan informasi yang memadai sebelum perjanjian ditandatangani, berupa: sertifikasi ISO 27001, laporan audit keamanan, atau dokumen kebijakan keamanan yang relevan.

d. Register Pihak Ketiga wajib disusun dan dimutakhirkan yang mencatat seluruh pihak ketiga beserta klasifikasi risiko, jenis akses, dan status kontrak.

e. Seluruh pihak ketiga yang diberikan akses wajib menjalani proses penerimaan (onboarding) keamanan informasi yang mencakup: sosialisasi kebijakan keamanan, penandatanganan NDA, dan penetapan batas akses yang diizinkan.

2. Klausul Keamanan Informasi dalam Perjanjian

a. Setiap kontrak atau perjanjian dengan pihak ketiga yang memiliki akses ke sistem informasi atau data wajib memuat klausul keamanan informasi sebagai bagian tidak terpisahkan dari dokumen kontrak.

b. Klausul keamanan informasi wajib mencakup minimal:

1) Kewajiban Kerahasiaan — pihak ketiga wajib menjaga kerahasiaan seluruh informasi yang diperoleh, berlaku tidak kurang dari 3 (tiga) tahun setelah berakhirnya kontrak.
2) Pembatasan Penggunaan Data — data hanya boleh digunakan untuk keperluan pelaksanaan perjanjian.
3) Perlindungan Data Pribadi — pihak ketiga yang memproses data pribadi wajib mematuhi ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
4) Standar Keamanan Minimum — pihak ketiga wajib menerapkan pengendalian keamanan yang memadai sesuai standar yang ditetapkan.
5) Pembatasan Sub-Kontrak — pengalihan pekerjaan kepada sub-kontraktor wajib mendapat persetujuan tertulis; sub-kontraktor tunduk pada ketentuan keamanan yang sama.
6) Kewajiban Pelaporan Insiden — pihak ketiga wajib melaporkan insiden dalam waktu maksimal 1×24 jam setelah diketahui.
7) Hak Audit — hak untuk melaksanakan audit keamanan informasi terhadap pihak ketiga.
8) Pengembalian atau Pemusnahan Data — pada saat berakhirnya perjanjian, seluruh data wajib dikembalikan dan/atau dihapus secara permanen, dengan konfirmasi tertulis.
9) Sanksi dan Kompensasi — pelanggaran klausul keamanan dapat menjadi dasar pemutusan kontrak dan/atau tuntutan ganti rugi.

c. Template klausul keamanan informasi standar wajib disediakan untuk digunakan seluruh OPD dalam proses pengadaan.
d. Bagian pengadaan OPD wajib berkoordinasi dengan unit kerja yang membidangi TIK untuk memastikan klausul keamanan termuat sebelum kontrak ditandatangani.

3. Keamanan Rantai Pasokan TIK

a. Pengadaan perangkat lunak dan aplikasi:
   1) vendor wajib menyertakan dokumentasi keamanan yang mencakup: arsitektur keamanan, daftar komponen pihak ketiga (*Software Bill of Materials*/*SBOM*), dan hasil pengujian keamanan;
   2) seluruh aplikasi yang dikembangkan pihak ketiga wajib melalui pengujian keamanan sebelum diterapkan pada lingkungan produksi;
   3) kode sumber aplikasi yang dikembangkan khusus wajib diserahkan pada saat serah terima.
b. Pengelolaan komponen sumber terbuka (open source):
   1) penggunaan komponen open source wajib didokumentasikan dalam *SBOM*;
   2) vendor wajib memantau kerentanan dan menerapkan pembaruan keamanan sesuai SLA.
c. Pengadaan perangkat keras:
   1) perangkat keras kritis wajib diperoleh dari distributor resmi atau pabrikan terverifikasi;
   2) integritas fisik perangkat wajib diverifikasi sebelum dioperasikan.
d. Layanan cloud:
   1) penyedia layanan cloud wajib melalui penilaian keamanan yang mencakup: lokasi data center, sertifikasi keamanan, mekanisme enkripsi, dan SLA keamanan;
   2) data Rahasia tidak boleh disimpan pada layanan cloud publik tanpa enkripsi ujung ke ujung dan persetujuan tertulis dari pimpinan yang berwenang.

e. Daftar Produk dan Layanan TIK yang Disetujui wajib disusun sebagai referensi pengadaan bagi seluruh OPD.

4. Pemantauan, Tinjauan, dan Penghentian Hubungan Pihak Ketiga

a. Pemantauan kinerja keamanan:
   1) kinerja keamanan informasi pihak ketiga wajib dipantau secara berkelanjutan melalui mekanisme yang disepakati dalam SLA;
   2) pihak ketiga Risiko Tinggi wajib menyampaikan laporan kepatuhan keamanan minimal setiap 3 (tiga) bulan;
   3) insiden keamanan yang melibatkan pihak ketiga wajib ditangani sesuai BAB VII dokumen ini.

b. Tinjauan dan audit tahunan:
   1) tinjauan kinerja keamanan terhadap seluruh pihak ketiga aktif wajib dilaksanakan minimal 1 (satu) kali per tahun;
   2) tinjauan dapat berupa: audit dokumen, kuesioner keamanan, atau audit lapangan berdasarkan profil risiko;
   3) pihak ketiga yang tidak memenuhi persyaratan wajib diberikan Rencana Perbaikan yang dipantau.

c. Manajemen perubahan layanan:
   1) pihak ketiga wajib memberitahukan setiap perubahan yang berpotensi memengaruhi keamanan layanan, minimal 30 (tiga puluh) hari kalender sebelumnya;
   2) perubahan darurat wajib diberitahukan dalam 1×24 jam;
   3) penundaan atau pembatalan perubahan dapat diminta apabila risiko dinilai tidak dapat diterima.

d. Penghentian hubungan (offboarding pihak ketiga):
   1) seluruh hak akses logis dan fisik wajib dicabut dalam waktu maksimal 1 (satu) hari kerja;
   2) pengembalian atau pemusnahan data wajib dikonfirmasi;
   3) pengembalian perangkat atau media penyimpanan yang dipinjamkan;
   4) rekaman proses offboarding disimpan minimal 3 (tiga) tahun.

e. Register Pihak Ketiga wajib diperbarui setiap terjadi perubahan dan ditinjau secara menyeluruh minimal 1 (satu) kali per tahun.

BAB IX
MANAJEMEN ASET DAN KLASIFIKASI INFORMASI

A. Maksud dan Tujuan

Memastikan seluruh aset informasi Pemerintah Kabupaten Kendal teridentifikasi, diklasifikasikan, dilabeli, dan dilindungi secara proporsional sesuai tingkat sensitivitasnya — termasuk pengelolaan pengembalian aset, perlindungan aset di luar lokasi, pengelolaan media penyimpanan, penghapusan informasi, dan penyamaran data — sehingga risiko kehilangan, kebocoran, dan penyalahgunaan informasi dapat diminimalkan.

B. Ruang Lingkup

Seluruh aset informasi (data, dokumen, perangkat keras, perangkat lunak, layanan) yang dimiliki, dikelola, atau diproses oleh seluruh OPD di lingkungan Pemerintah Kabupaten Kendal, baik dalam format digital maupun fisik.

C. Ketentuan

1. Pengembalian Aset

a. Seluruh aset informasi dan aset TIK milik Pemerintah Kabupaten Kendal yang dipinjamkan atau dipercayakan kepada personel wajib dikembalikan pada saat berakhirnya hubungan kerja, mutasi, atau selesainya penugasan, selaras dengan prosedur offboarding sebagaimana diatur dalam BAB IV dokumen ini.
b. Pengembalian aset wajib dibuktikan dengan Berita Acara Serah Terima Aset yang ditandatangani oleh kedua belah pihak.
c. Data dinas yang tersimpan pada perangkat pribadi (BYOD) wajib dihapus secara permanen dan dibuktikan dengan pernyataan tertulis.
d. Aset yang tidak dikembalikan wajib dilaporkan kepada pimpinan OPD dan ditindaklanjuti sesuai ketentuan pengelolaan Barang Milik Daerah yang berlaku.

2. Klasifikasi Informasi

a. Seluruh informasi yang dimiliki dan dikelola oleh Pemerintah Kabupaten Kendal wajib diklasifikasikan ke dalam 4 (empat) level berdasarkan tingkat sensitivitas dan dampak apabila terungkap tanpa otorisasi:

Level	Definisi dan contoh
RAHASIA	Informasi yang pengungkapannya dapat membahayakan kepentingan negara, keamanan publik, atau menimbulkan kerugian besar. Contoh: data kependudukan massal, data biometrik, kunci kriptografi, strategi keamanan nasional.
TERBATAS	Informasi yang pengungkapannya dapat mengganggu operasional atau merugikan organisasi. Contoh: data keuangan internal, data kepegawaian, laporan audit, hasil penilaian risiko.
BIASA	Informasi internal yang tidak dimaksudkan untuk publik namun pengungkapannya tidak menimbulkan dampak signifikan. Contoh: memo internal, jadwal rapat, notulen umum.

PUBLIK	Informasi yang secara sah ditujukan untuk konsumsi publik. Contoh: pengumuman resmi, data statistik yang dipublikasikan, profil OPD.

Tabel 9. Klasifikasi informasi

b. Pemilik aset (*asset owner*) bertanggung jawab menetapkan klasifikasi informasi berdasarkan tingkat sensitivitas dan dampak pengungkapan.
c. Tabel penanganan informasi berdasarkan klasifikasi:

Aspek	RAHASIA	TERBATAS	BIASA	PUBLIK
Penyimpanan	Enkripsi wajib	Akses terbatas	Akses internal	Tanpa batasan
Transfer	Enkripsi + NDA	Enkripsi/ proteksi	Email dinas	Tanpa batasan
Pencetakan	Terkendali + hancurkan	Terkendali	Bebas	Bebas
Pembuangan	Sanitasi level maksimal	Sanitasi standar	Format standar	Hapus biasa
Akses	*Need-to-know* + persetujuan	*Need-to-know*	Internal	Umum

Tabel 10. Penanganan informasi berdasarkan klasifikasi

d. Klasifikasi wajib ditinjau secara berkala oleh pemilik aset, minimal 1 (satu) kali per tahun, dan disesuaikan apabila tingkat sensitivitas berubah.

3. Pelabelan Informasi

a. Seluruh informasi dengan klasifikasi Rahasia, Terbatas, dan Biasa wajib diberi label yang jelas dan konsisten.
b. Pelabelan dokumen fisik:
   1) label klasifikasi wajib dicantumkan pada *header* dan/atau *footer* setiap halaman dokumen;
   2) sampul dokumen wajib memuat label klasifikasi yang terlihat jelas;
   3) format label: [**RAHASIA**], [**TERBATAS**], atau [**BIASA**].
c. Pelabelan dokumen digital:
   1) label klasifikasi wajib dicantumkan pada *header* dan/atau *footer* dokumen (*Microsoft Word*, PDF);
   2) metadata file digital wajib memuat informasi klasifikasi (*custom properties*);
   3) subjek email yang mengandung lampiran Rahasia atau Terbatas wajib mencantumkan label klasifikasi pada baris subjek.
d. Informasi berkategori Publik tidak wajib dilabeli namun direkomendasikan untuk menghindari kerancuan.
e. Pimpinan OPD wajib memastikan seluruh ASN memahami dan menerapkan aturan pelabelan.

4. Keamanan Aset di Luar Lokasi

a. Perangkat portabel dinas (laptop, tablet, ponsel dinas) yang dibawa ke luar lingkungan kantor wajib:
   1) mendapat persetujuan tertulis dari pimpinan OPD;
   2) memiliki enkripsi penyimpanan (*full disk encryption*) aktif;
   3) dilindungi dengan kata sandi atau biometrik yang kuat;
   4) tidak boleh ditinggalkan tanpa pengawasan di tempat umum.

b. Media penyimpanan portabel (USB, *external drive*) yang membawa data Terbatas atau Rahasia ke luar kantor wajib dienkripsi.
c. Kehilangan atau pencurian perangkat di luar lokasi wajib dilaporkan dalam waktu maksimal 1×24 jam dan ditindaklanjuti sesuai prosedur manajemen insiden.
d. Penggunaan perangkat dinas di luar negeri wajib mendapat persetujuan khusus dengan mempertimbangkan risiko keamanan informasi di negara tujuan.

5. Pengelolaan Media Penyimpanan

a. Media penyimpanan yang berisi data Rahasia atau Terbatas wajib disimpan di tempat yang terkunci dengan akses terbatas.
b. Penggunaan media penyimpanan portabel untuk menyimpan data Rahasia wajib mendapat persetujuan pimpinan OPD dan dicatat.
c. Media penyimpanan yang rusak atau tidak terpakai wajib melalui prosedur sanitasi data yang aman sebelum dibuang, sebagaimana diatur dalam BAB V dokumen ini.
d. Inventaris media penyimpanan yang berisi data Rahasia wajib disusun dan dimutakhirkan.
e. Pengiriman media penyimpanan yang berisi data Rahasia wajib menggunakan layanan pengiriman yang aman, terenkripsi, dan dilengkapi bukti serah terima.

6. Penghapusan Informasi

a. Informasi yang tidak lagi diperlukan atau telah melampaui jangka waktu retensi wajib dihapus secara aman sesuai klasifikasi:
    1) data Rahasia: menggunakan metode penghapusan yang tidak dapat dipulihkan (*secure wipe*, *degaussing*, atau penghancuran fisik);
    2) data Terbatas: *overwrite* minimal 3 pass atau secure erase;
    3) data Biasa: penghapusan standar yang memadai;
    4) data Publik: penghapusan biasa.
b. Penghapusan data pribadi wajib mematuhi ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, termasuk hak subjek data untuk menghapus data pribadinya.
c. Setiap penghapusan informasi Rahasia wajib didokumentasikan dalam Berita Acara Penghapusan yang memuat: jenis data, media penyimpanan, metode penghapusan, tanggal, dan pelaksana.
d. Penghapusan data pada sistem basis data yang masih aktif wajib memastikan bahwa data juga terhapus dari seluruh salinan backup sesuai siklus retensi backup.
e. Verifikasi penghapusan wajib dilaksanakan untuk data Rahasia guna memastikan data tidak dapat dipulihkan.

7. Penyamaran Data (*Data Masking*)

a. Teknik penyamaran data wajib diterapkan apabila data produksi perlu digunakan di luar lingkungan produksi, termasuk:
    1) lingkungan pengembangan dan pengujian;
    2) pelatihan dan demonstrasi;
    3) analisis statistik yang tidak memerlukan identitas individu.
b. Teknik penyamaran data yang dapat digunakan meliputi:
    1) pseudonimisasi — mengganti identitas asli dengan pengenal buatan (*pseudonym*), dengan kunci pemetaan disimpan terpisah dan terproteksi;
    2) anonimisasi — menghilangkan seluruh atribut yang dapat mengidentifikasi individu secara tidak dapat dikembalikan;

3) tokenisasi — mengganti data sensitif dengan token acak;
4) substitusi — mengganti data asli dengan data sintetis yang mempertahankan format dan karakteristik.

c. Data kependudukan dan data pribadi yang digunakan untuk pengembangan atau pengujian sistem wajib dianonimkan atau menggunakan data sintetis; penggunaan data produksi riil dilarang.
d. Tingkat penyamaran data wajib disesuaikan dengan klasifikasi informasi dan tujuan penggunaan.

BAB X
MANAJEMEN IDENTITAS DAN AKSES

A. Maksud dan Tujuan

Menetapkan pengendalian atas siklus hidup identitas digital, pengelolaan informasi autentikasi, proses pemberian dan pencabutan hak akses (provisioning dan de-provisioning), perjanjian kerahasiaan, serta keamanan bekerja jarak jauh — guna memastikan bahwa akses terhadap sistem informasi Pemerintah Kabupaten Kendal selalu sesuai dengan kebutuhan tugas, terlindungi, dan dapat dipertanggungjawabkan.

B. Ruang Lingkup

Seluruh identitas digital (akun pengguna) dan hak akses pada sistem informasi, aplikasi, dan layanan TIK yang dikelola oleh Pemerintah Kabupaten Kendal, meliputi akun ASN, PPPK, tenaga kontrak, dan pihak ketiga, baik yang bekerja di kantor maupun dari lokasi jarak jauh.

C. Ketentuan

1. Manajemen Identitas Digital

a. Siklus hidup identitas digital:
   1) Pendaftaran — identitas digital hanya diterbitkan berdasarkan permohonan formal dari pimpinan OPD atau pejabat yang berwenang, disertai identifikasi positif pemilik akun;
   2) Verifikasi — identitas pemohon wajib diverifikasi terhadap data kepegawaian atau kontrak sebelum akun diterbitkan;
   3) Penerbitan — akun diterbitkan oleh pengelola sistem sesuai konvensi penamaan dan hak akses yang disetujui;
   4) Penangguhan — akun wajib ditangguhkan (disabled) apabila pemilik cuti panjang (lebih dari 30 hari), dalam proses investigasi disiplin, atau atas permintaan pimpinan OPD;
   5) Pencabutan — akun wajib dinonaktifkan secara permanen sesuai ketentuan offboarding dalam BAB IV dokumen ini.

b. Konvensi penamaan akun:
   1) standar konvensi penamaan akun wajib ditetapkan dan berlaku seragam untuk seluruh sistem informasi;
   2) penggunaan akun anonim atau akun generik (misal: "user1", "admin") dilarang; setiap akun wajib dapat dikaitkan dengan satu individu yang bertanggung jawab.

c. Setiap individu wajib memiliki identitas digital yang unik; satu akun tidak boleh digunakan oleh lebih dari satu orang.

d. Direktori Identitas terpusat wajib dikelola yang mencatat seluruh akun aktif, pemilik, OPD, dan status.

e. Akun yang tidak aktif selama lebih dari 90 (sembilan puluh) hari tanpa justifikasi wajib ditangguhkan secara otomatis atau manual.

2. Pengelolaan Informasi Autentikasi

a. Distribusi kredensial awal:
   1) kata sandi awal wajib dibuat secara acak, unik per akun, dan bersifat sementara;
   2) distribusi kata sandi awal wajib melalui kanal yang aman dan terpisah dari distribusi informasi akun (username);
   3) pengguna wajib mengubah kata sandi awal pada saat login pertama; sistem wajib memaksa perubahan ini secara teknis.

b. Pengelolaan kata sandi oleh pengguna:
   1) pengguna dilarang membagikan kata sandi kepada siapa pun;

2) pengguna dilarang mencatat kata sandi dalam bentuk yang dapat dibaca tanpa perlindungan;
3) penggunaan pengelola kata sandi (password manager) yang disetujui sangat direkomendasikan;
4) standar kompleksitas dan rotasi kata sandi mengacu pada ketentuan autentikasi dalam BAB VI dokumen ini.

c. Penyimpanan kredensial pada sistem:
1) kata sandi dilarang disimpan dalam format plaintext pada basis data, berkas konfigurasi, atau kode sumber;
2) kata sandi wajib disimpan dalam bentuk *hash* menggunakan algoritma yang aman (*bcrypt*, *Argon2*, atau setara);
3) kunci API dan kredensial layanan wajib disimpan dalam penyimpanan aman yang terenkripsi (vault).

d. Reset kata sandi wajib melalui prosedur yang memverifikasi identitas pemohon sebelum kata sandi baru diterbitkan.

e. Seluruh percobaan autentikasi gagal wajib dicatat sesuai ketentuan pencatatan log dalam BAB VI dokumen ini.

3. Hak Akses — Provisioning dan De-provisioning

a. Prinsip pemberian hak akses:
1) hak akses diberikan berdasarkan prinsip *least privilege*;
2) hak akses diberikan berdasarkan peran (*role-based*) sesuai matriks peran yang ditetapkan;
3) pemberian melalui permohonan formal yang disetujui oleh pimpinan OPD atau pejabat yang berwenang.

b. Proses *Joiner-Mover-Leaver*:
1) *Joiner* (Personel Baru): pimpinan OPD mengajukan permohonan akses sesuai peran, pengelola sistem menerbitkan akun dan hak akses, aktif paling lambat pada hari pertama kerja.
2) *Mover* (Mutasi/Perubahan Jabatan): pimpinan OPD asal wajib menginformasikan mutasi paling lambat 3 (tiga) hari kerja sebelum tanggal efektif; hak akses pada OPD asal wajib dicabut atau disesuaikan; hak akses baru diberikan sesuai peran baru; proses ini mencegah akumulasi hak akses berlebihan (*privilege creep*).
3) *Leaver* (Pensiun/Berhenti/Akhir Kontrak): seluruh hak akses reguler dicabut dalam 1 (satu) hari kerja; hak akses istimewa dicabut dalam 4 (empat) jam; akun dinonaktifkan selama minimal 90 (sembilan puluh) hari untuk keperluan *audit trail*, kemudian dihapus.

c. Tinjauan hak akses berkala:
1) hak akses reguler ditinjau minimal setiap 6 (enam) bulan;
2) hak akses istimewa ditinjau setiap 3 (tiga) bulan;
3) tinjauan memverifikasi: akun masih sesuai dengan personel aktif, hak akses sesuai dengan peran terkini, dan tidak ada akumulasi berlebihan;
4) hasil tinjauan wajib didokumentasikan dalam Laporan Tinjauan Hak Akses yang ditandatangani pimpinan OPD.

d. Hak akses sementara (*temporary access*) wajib memiliki tanggal kedaluwarsa yang ditetapkan pada saat pemberian dan dicabut pada tanggal tersebut.

4. Perjanjian Kerahasiaan

a. Template NDA standar wajib disusun dan berlaku untuk seluruh OPD, dengan ketentuan minimal:
1) definisi informasi yang bersifat rahasia;

2) kewajiban penerima untuk menjaga kerahasiaan;
3) larangan pengungkapan tanpa persetujuan tertulis;
4) jangka waktu berlaku minimal 2 (dua) tahun setelah berakhirnya hubungan kerja/kontrak;
5) konsekuensi pelanggaran;
6) pengecualian untuk informasi yang menjadi milik publik bukan karena pelanggaran NDA.

b. NDA wajib ditandatangani oleh:
1) ASN yang memiliki akses ke data Rahasia;
2) tenaga kontrak sebelum memulai pekerjaan;
3) pihak ketiga sebagai bagian dari kontrak;
4) auditor sebelum pelaksanaan audit.

c. NDA yang ditandatangani wajib disimpan sesuai ketentuan retensi yang berlaku.

d. Pimpinan OPD bertanggung jawab memastikan seluruh personel yang mengakses informasi sensitif telah menandatangani NDA.

5. Keamanan Bekerja Jarak Jauh

a. Kelayakan dan persetujuan:
1) bekerja jarak jauh hanya diizinkan dengan persetujuan tertulis dari pimpinan OPD;
2) jenis tugas dan data yang boleh diakses secara jarak jauh wajib ditetapkan; pemrosesan data Rahasia dalam volume besar dari jarak jauh tidak disarankan kecuali mendapat persetujuan khusus.

b. Persyaratan koneksi jaringan:
1) akses ke sistem informasi dari lokasi jarak jauh wajib melalui VPN yang terenkripsi;
2) VPN wajib dikombinasikan dengan autentikasi multi-faktor;
3) penggunaan jaringan Wi-Fi publik untuk mengakses data Rahasia atau Terbatas dilarang meskipun melalui VPN; gunakan koneksi data seluler pribadi sebagai alternatif;
4) apabila Wi-Fi publik tidak dapat dihindari untuk informasi Biasa, pengguna wajib terhubung melalui VPN.

c. Keamanan perangkat:
1) perangkat wajib memenuhi seluruh standar konfigurasi keamanan sebagaimana diatur dalam BAB VI dokumen ini;
2) perangkat wajib dikonfigurasi dengan *screen lock* otomatis maksimal 5 (lima) menit;
3) fitur *remote wipe* wajib aktif pada perangkat portabel.

d. Keamanan fisik lokasi kerja jarak jauh:
1) layar perangkat tidak boleh terlihat oleh pihak yang tidak berwenang saat mengakses informasi sensitif;
2) dokumen fisik berisi informasi dinas wajib disimpan aman;
3) pembicaraan yang membahas informasi sensitif wajib dilakukan di ruangan yang tertutup.

e. Pengelolaan data:
1) data dinas yang diakses selama bekerja jarak jauh tidak boleh disimpan permanen pada perangkat pribadi;
2) pencetakan dokumen Rahasia di lokasi jarak jauh dilarang;
3) setelah selesai bekerja jarak jauh, data dinas pada cache dan folder unduhan wajib dihapus.

f. Insiden keamanan selama bekerja jarak jauh wajib dilaporkan segera sesuai prosedur BAB VII tanpa menunggu kembali ke kantor.

g. Panduan Bekerja Jarak Jauh yang Aman wajib disusun dan didistribusikan kepada seluruh ASN.

BAB XI
KEAMANAN PENGEMBANGAN SISTEM

A. Maksud dan Tujuan

Memastikan bahwa seluruh pengembangan, modifikasi, dan pengadaan sistem informasi di lingkungan Pemerintah Kabupaten Kendal menerapkan prinsip keamanan informasi secara terintegrasi pada setiap fase — mulai dari perencanaan proyek, analisis kebutuhan, desain arsitektur, pengkodean, pengujian, hingga pemeliharaan — termasuk pengendalian terhadap pengembangan yang dialihdayakan, pemisahan lingkungan, perlindungan data pengujian, dan pembatasan akses terhadap kode sumber.

B. Ruang Lingkup

Seluruh proyek pengembangan, modifikasi, dan pemutakhiran sistem informasi serta aplikasi SPBE yang dilaksanakan oleh unit kerja internal maupun pihak ketiga (vendor) di lingkungan Pemerintah Kabupaten Kendal.

C. Ketentuan

1. Keamanan Informasi dalam Manajemen Proyek

a. Setiap proyek TIK wajib menyertakan Penilaian Risiko Keamanan Informasi sebagai bagian dari dokumen perencanaan proyek, yang mengidentifikasi ancaman, kerentanan, dan pengendalian yang diperlukan sesuai metodologi BAB II dokumen ini.
b. Kerangka Acuan Kerja (KAK) atau Terms of Reference proyek TIK wajib mencantumkan persyaratan keamanan informasi, meliputi:
   1) klasifikasi data yang akan diproses oleh sistem;
   2) persyaratan keamanan teknis;
   3) kewajiban pengujian keamanan sebelum go-live;
   4) kewajiban dokumentasi keamanan.
c. Pada setiap *milestone* proyek, pemenuhan persyaratan keamanan wajib dievaluasi dan didokumentasikan.
d. Serah terima proyek tidak boleh dilaksanakan apabila persyaratan keamanan belum terpenuhi atau kerentanan kritis belum ditangani.
e. Untuk proyek yang melibatkan pihak ketiga, persyaratan keamanan wajib tercakup dalam kontrak sesuai BAB VIII dokumen ini.

2. Siklus Hidup Pengembangan Sistem yang Aman (*Secure SDLC*)

a. Pedoman *Secure Software Development Life Cycle* (*Secure SDLC*) wajib ditetapkan yang mengatur aktivitas keamanan pada setiap fase pengembangan. Seluruh pengembangan aplikasi SPBE wajib mengikuti pedoman ini.
b. Fase dan aktivitas keamanan wajib:

   Fase 1 — Analisis Kebutuhan:

   1) identifikasi data yang akan diproses beserta klasifikasinya;
   2) penilaian risiko keamanan awal;
   3) penyusunan persyaratan keamanan aplikasi;
   4) identifikasi kepatuhan regulasi yang berlaku.

   Fase 2 — Desain:

   1) penerapan prinsip arsitektur aman;
   2) pemodelan ancaman (*threat modeling*);
   3) desain mekanisme autentikasi, otorisasi, dan *audit trail*;
   4) perencanaan mekanisme enkripsi untuk data sensitif.

Fase 3 — Pengkodean:

1) penerapan standar pengkodean aman;
2) tinjauan kode (*code review*) oleh personel berbeda dari pengembang;
3) penggunaan alat analisis kode statis apabila tersedia;
4) pengelolaan dependensi dan komponen pihak ketiga.

Fase 4 — Pengujian:

1) pengujian keamanan mencakup *vulnerability assessment* dan penetration testing;
2) uji kerentanan terhadap *OWASP Top 10*;
3) pengujian menggunakan data non-produksi;
4) verifikasi pemenuhan seluruh persyaratan keamanan.

Fase 5 — *Deployment*:

1) deployment hanya pada lingkungan produksi yang terpisah;
2) pengerasan (*hardening*) konfigurasi;
3) penonaktifan akun debug dan konfigurasi default yang tidak aman;
4) pemindaian kerentanan final sebelum *go-live*.

Fase 6 — Pemeliharaan:

1) pemantauan kerentanan berkelanjutan;
2) penerapan *patch* keamanan sesuai SLA;
3) modifikasi signifikan wajib melalui siklus *Secure SDLC* yang sama.

c. Seluruh aktivitas keamanan pada setiap fase wajib didokumentasikan.
d. Pengembangan oleh pihak ketiga wajib mematuhi Pedoman *Secure SDLC* dan kepatuhannya wajib dipantau.
e. Pedoman *Secure SDLC* wajib ditinjau minimal 1 (satu) kali per tahun.

3. Persyaratan Keamanan Aplikasi

a. Setiap aplikasi wajib memenuhi persyaratan keamanan minimum:
   1) Autentikasi — sesuai standar yang ditetapkan dalam BAB VI;
   2) Otorisasi — *role-based access control* (RBAC);
   3) Validasi Input — seluruh masukan pengguna divalidasi pada sisi server untuk mencegah serangan injeksi;
   4) Enkripsi — data sensitif dienkripsi saat transmisi dan penyimpanan;
   5) Manajemen Sesi — *session timeout*, *token* aman, *logout* eksplisit;
   6) *Logging* dan *Audit Trail* — aktivitas kritis dicatat;
   7) Penanganan Kesalahan — pesan kesalahan tidak boleh mengungkapkan informasi teknis internal;
   8) Perlindungan CSRF — mekanisme *anti-CSRF* pada formulir;
   9) Pengunggahan Berkas — pembatasan jenis dan ukuran, pemindaian *malware*;
   10) *API Security* — autentikasi *token*, *rate limiting*, validasi *input/ output*.
b. Persyaratan keamanan wajib menjadi kriteria penerimaan saat serah terima proyek.
c. Dokumen Persyaratan Keamanan Standar wajib disusun untuk digunakan seluruh OPD sebagai lampiran KAK.

4. Arsitektur Sistem Aman

a. Setiap desain arsitektur sistem wajib menerapkan prinsip:
   1) *Defense-in-Depth* — keamanan berlapis pada lapisan jaringan, aplikasi, dan data;
   2) *Least Privilege* — hak akses minimum untuk setiap komponen;
   3) *Fail-Secure* — kondisi default menolak akses saat terjadi kegagalan;
   4) *Separation of Concerns* — pemisahan arsitektural antara komponen presentasi, logika bisnis, dan data.
b. Desain arsitektur sistem kritis wajib melalui tinjauan keamanan (*security design review*) sebelum memasuki fase pengkodean.
c. Dokumentasi arsitektur wajib mencakup diagram keamanan yang menunjukkan mekanisme pengendalian pada setiap lapisan.
d. Perubahan arsitektural wajib melalui proses tinjauan ulang.

5. Standar Pengkodean Aman

a. Standar Pengkodean Aman wajib ditetapkan yang mengacu pada *OWASP Secure Coding Practices*, mencakup pencegahan terhadap *OWASP Top 10*.
b. Larangan praktik pengkodean tidak aman:
   1) menyimpan kredensial secara *hardcoded* dalam kode sumber;
   2) membangun *query* basis data dari masukan pengguna secara langsung (*string concatenation*);
   3) menampilkan detail teknis internal dalam pesan kesalahan;
   4) menonaktifkan validasi sertifikat *SSL/TLS* dalam kode produksi;
   5) menggunakan fungsi kriptografi yang sudah usang;
   6) menyimpan kata sandi dalam format *plaintext* atau enkripsi reversibel;
   7) menggunakan komponen pihak ketiga dengan kerentanan kritis;
   8) mengaktifkan fitur *debug* pada lingkungan produksi.
c. Validasi input dan output:
   1) seluruh masukan pengguna divalidasi pada sisi server;
   2) pendekatan *whitelist* diterapkan apabila dimungkinkan;
   3) keluaran di-*encode* sesuai konteks untuk mencegah *XSS*.
d. Tinjauan kode (*code review*):
   1) kode yang akan di-*deploy* wajib melalui tinjauan oleh minimal 1 (satu) personel berbeda dari pengembang;
   2) tinjauan memperhatikan aspek keamanan;
   3) temuan keamanan wajib diperbaiki sebelum masuk ke cabang utama.
e. Penggunaan alat analisis kode statis (*SAST*) direkomendasikan.
f. Pengelolaan komponen pihak ketiga:
   1) setiap komponen tercatat dalam *SBOM*;
   2) pengembang wajib memantau kerentanan dan menerapkan pembaruan.

6. Pengujian Keamanan

a. Pengujian keamanan pra-operasional (sebelum *go-live*):
   1) wajib mencakup *Vulnerability Assessment* dan *Penetration Testing*;
   2) dilaksanakan oleh personel independen dari tim pengembang;
   3) kerentanan kritis dan tinggi wajib diperbaiki sebelum *go-live*; kerentanan sedang dan rendah boleh diterima dengan persetujuan tertulis dan rencana perbaikan.
b. Pengujian keamanan berkala pada sistem produksi:

1) *Vulnerability Assessment* minimal 1 (satu) kali per tahun untuk sistem terekspos ke internet dan sistem kritis;
2) *Penetration Testing* minimal 1 (satu) kali per tahun untuk sistem kritis;
3) pengujian tambahan setelah perubahan besar.

c. Hasil pengujian wajib didokumentasikan dalam Laporan Pengujian Keamanan.
d. Temuan wajib ditindaklanjuti sesuai SLA manajemen kerentanan sebagaimana diatur dalam BAB VI dokumen ini.

7. Pengembangan yang Dialihdayakan

a. Kontrak pengembangan yang dialihdayakan wajib memuat:
1) kewajiban vendor mematuhi Pedoman *Secure SDLC*, Standar Pengkodean Aman, dan Persyaratan Keamanan Aplikasi;
2) klausul keamanan informasi sesuai BAB VIII;
3) kewajiban penyerahan kode sumber dan dokumentasi teknis;
4) kewajiban penyerahan *SBOM*;
5) hak untuk melaksanakan audit keamanan dan *code review*.

b. Supervisi keamanan terhadap proses pengembangan vendor wajib dilaksanakan, meliputi: verifikasi pemenuhan persyaratan keamanan, *code review*, dan pengujian keamanan independen.
c. Vendor dilarang menyimpan salinan kode sumber, data, atau konfigurasi setelah serah terima, kecuali untuk dukungan teknis yang diatur dalam kontrak pemeliharaan terpisah.
d. Sub-kontraktor yang digunakan vendor wajib tunduk pada ketentuan keamanan yang sama.

8. Pemisahan Lingkungan

a. Setiap sistem dengan siklus pengembangan aktif wajib memiliki minimal 3 (tiga) lingkungan terpisah:
1) Lingkungan Pengembangan (*Development*);
2) Lingkungan Pengujian/*Staging*;
3) Lingkungan Produksi (*Production*).

b. Larangan:
1) pengembang dilarang melakukan pengkodean, kompilasi, atau *debug* langsung pada lingkungan produksi;
2) alat pengembangan dilarang terpasang pada server produksi;
3) data produksi riil dilarang disalin ke lingkungan pengembangan kecuali telah dianonimkan;
4) akun dan kredensial antar-lingkungan wajib berbeda.

c. Pemindahan kode antar-lingkungan wajib melalui prosedur *deployment* terkontrol.
d. Hak akses ke lingkungan produksi wajib dibatasi hanya kepada personel operasional berotorisasi.
e. Konfigurasi jaringan wajib memastikan lingkungan pengembangan dan pengujian tidak dapat mengakses data produksi secara langsung.

9. Perlindungan Data Pengujian

a. Penggunaan data produksi riil untuk pengujian dilarang kecuali telah melalui anonimisasi atau pseudonimisasi.
b. Data pengujian wajib diperoleh melalui:
1) data sintetis yang dibuat khusus;
2) data produksi yang telah dianonimkan;
3) data produksi yang telah di-pseudonimkan dengan kunci konversi yang disimpan terpisah.

c. Proses anonimisasi/pseudonimisasi wajib dilaksanakan oleh personel berotorisasi, menghapus seluruh atribut pengidentifikasi, dan didokumentasikan.
d. Apabila penggunaan data produksi tidak dapat dihindari:
    1) persetujuan tertulis dari pimpinan yang berwenang;
    2) pengendalian keamanan setara lingkungan produksi;
    3) data dihapus segera setelah pengujian selesai.
e. Vendor dilarang membawa data produksi keluar dari lingkungan yang dikendalikan.

10. Pembatasan Akses terhadap Kode Sumber

a. Kode sumber wajib disimpan dalam repositori terpusat dengan pengendalian akses berlapis.
b. Akses ke repositori hanya untuk:
    1) pengembang yang aktif ditugaskan pada proyek;
    2) personel teknis yang ditunjuk untuk supervisi dan reviu;
    3) auditor keamanan berotorisasi selama periode audit.
c. Hak akses ditinjau setiap 3 (tiga) bulan dan dicabut segera setelah tidak diperlukan.
d. Seluruh akses dan perubahan pada repositori wajib dicatat dalam log yang dilindungi dari modifikasi.
e. Kode sumber aset kritis wajib dicadangkan secara berkala.
f. Kode sumber tidak boleh disimpan pada perangkat pribadi atau media tidak terenkripsi, dan tidak boleh dibagikan melalui kanal komunikasi yang tidak aman.

BAB XII
MANAJEMEN OPERASI DAN PERUBAHAN

A. Maksud dan Tujuan

Menetapkan prosedur pengelolaan operasional TIK yang terdokumentasi, manajemen konfigurasi yang terkendali, manajemen perubahan yang formal, perencanaan kapasitas, pemantauan berkelanjutan, sinkronisasi waktu, pengendalian penggunaan program utilitas istimewa, dan pengendalian instalasi perangkat lunak — guna menjaga ketersediaan, integritas, dan keamanan seluruh sistem informasi Pemerintah Kabupaten Kendal.

B. Ruang Lingkup

Seluruh sistem informasi kritis, server, perangkat jaringan, basis data, aplikasi, dan infrastruktur pendukung yang dioperasikan oleh OPD di lingkungan Pemerintah Kabupaten Kendal.

C. Ketentuan

1. Prosedur Operasional Terdokumentasi

a. Setiap sistem informasi kritis wajib memiliki Standar Operasional Prosedur (SOP) yang terdokumentasi dan disetujui oleh pimpinan yang berwenang.
b. SOP wajib mencakup minimal:
   1) prosedur *start-up* dan *shutdown* sistem;
   2) prosedur pemantauan dan penanganan gangguan harian;
   3) prosedur *backup* dan *restore*;
   4) prosedur penanganan insiden awal;
   5) prosedur eskalasi;
   6) kontak darurat dan jadwal piket (jika berlaku).
c. SOP wajib ditulis dengan tingkat detail yang memungkinkan personel pengganti untuk melaksanakan prosedur tanpa pendampingan langsung dari pengelola sistem utama.
d. SOP wajib ditinjau dan diperbarui minimal 1 (satu) kali per tahun atau segera setelah perubahan signifikan pada sistem.
e. SOP wajib tersedia bagi personel berotorisasi; versi terkini dan 2 (dua) versi sebelumnya wajib dipertahankan.
f. Template SOP standar wajib disediakan sebagai acuan penyusunan bagi seluruh OPD.

2. Manajemen Konfigurasi

a. *Baseline* Konfigurasi Keamanan wajib ditetapkan untuk setiap kategori aset TIK utama, minimal:
   1) server (*Windows Server*, *Linux*);
   2) perangkat jaringan (*router*, *switch*, *firewall*);
   3) sistem operasi endpoint;
   4) basis data;
   5) aplikasi web server.
b. *Baseline* wajib mencakup: pengaturan keamanan yang harus diaktifkan, layanan/*port* yang harus dinonaktifkan, kebijakan akses, dan pengaturan *logging*; mengacu pada panduan pengerasan dari vendor, *CIS Benchmarks*, atau standar BSSN.
c. Basis Data Konfigurasi (*Configuration Management Database*/CMDB) wajib dikelola yang mencatat konfigurasi aktual seluruh aset TIK kritis, diperbarui setiap kali terjadi perubahan.

d. Seluruh perubahan konfigurasi pada lingkungan produksi wajib melalui prosedur manajemen perubahan. Konfigurasi sebelum perubahan wajib dicadangkan untuk keperluan *rollback*.
e. Audit kepatuhan konfigurasi terhadap *baseline* wajib dilaksanakan minimal 1 (satu) kali dalam 6 (enam) bulan untuk perangkat kritis. Penyimpangan wajib diperbaiki atau diberikan justifikasi pengecualian.
f. Konfigurasi default pabrikan (*default password*, akun *default*, layanan yang tidak diperlukan) wajib diubah atau dinonaktifkan sebelum perangkat dioperasikan.

3. Manajemen Perubahan

a. Klasifikasi perubahan:

Klasifikasi	Definisi dan Proses
Standar (*Pre-approved*)	Perubahan rutin, berisiko rendah, dengan prosedur terdokumentasi. Cukup didokumentasikan dan dilaporkan.
Normal	Perubahan yang memerlukan perencanaan, penilaian risiko, dan persetujuan. Diajukan melalui RFC dan disetujui CAB.
Darurat (*Emergency*)	Perubahan mendesak untuk mengatasi insiden aktif atau kerentanan kritis. Persetujuan lisan, didokumentasikan dalam 1 hari kerja setelah pelaksanaan.

Tabel 11. Klasifikasi perubahan

b. Prosedur perubahan normal (melalui RFC):
   1) Pengajuan — pemohon mengisi Formulir Permintaan Perubahan (*Request for Change*/RFC) yang memuat: deskripsi, justifikasi, sistem terdampak, penilaian risiko, rencana implementasi, dan rencana *rollback*;
   2) Penilaian — kelayakan teknis, risiko keamanan, dan dampak terhadap layanan dievaluasi;
   3) Persetujuan — RFC diajukan kepada *Change Advisory Board* (CAB);
   4) Implementasi — sesuai rencana yang disetujui, sebaiknya di luar jam operasional untuk perubahan berisiko;
   5) Verifikasi — perubahan diverifikasi berfungsi sesuai harapan;
   6) Penutupan — RFC ditutup dan CMDB diperbarui.
c. Rencana *Rollback* wajib ditetapkan untuk setiap perubahan Normal dan Darurat. Kriteria keputusan *rollback* wajib ditetapkan sebelum implementasi dimulai.
d. Perubahan pada sistem kritis memerlukan persetujuan eksplisit dari pimpinan yang berwenang.
e. Seluruh perubahan wajib dicatat dalam Register Perubahan.
f. CAB wajib melaksanakan rapat minimal 1 (satu) kali per bulan.

4. Manajemen Kapasitas

a. Kapasitas infrastruktur kritis wajib dipantau secara berkelanjutan, mencakup minimal: penggunaan CPU, memori, penyimpanan, dan *bandwidth* jaringan.
b. *Threshold* peringatan:
   1) Peringatan (*Warning*): pemanfaatan mencapai 75%;
   2) Kritis (*Critical*): pemanfaatan mencapai 90%.

c. Rencana Kapasitas Tahunan wajib disusun berdasarkan analisis tren penggunaan, proyeksi pertumbuhan, dan rencana pengembangan sistem.
d. Apabila kapasitas mendekati ambang kritis, langkah optimalisasi sementara wajib diterapkan.
e. Laporan kapasitas infrastruktur wajib disusun setiap bulan.

5. Aktivitas Pemantauan

a. Sistem pemantauan terpusat (*monitoring system*) wajib dioperasikan yang mencakup:
   1) pemantauan ketersediaan (*availability*) — status seluruh server dan layanan kritis;
   2) pemantauan kinerja (*performance*) — utilisasi sumber daya;
   3) pemantauan keamanan (*security monitoring*) — deteksi aktivitas mencurigakan.
b. Dashboard pemantauan wajib disediakan yang menampilkan status *real-time* infrastruktur dan layanan kritis.
c. Notifikasi anomali:
   1) sistem pemantauan wajib mengirimkan notifikasi otomatis apabila terdeteksi kondisi anomali;
   2) notifikasi melalui minimal 2 (dua) kanal komunikasi;
   3) setiap notifikasi wajib ditindaklanjuti dan dicatat.
d. Pemantauan infrastruktur kritis wajib beroperasi 24/7.
e. Laporan ringkasan pemantauan wajib disusun setiap bulan.

6. Sinkronisasi Waktu

a. Seluruh perangkat dan sistem wajib disinkronisasi waktunya menggunakan protokol *Network Time Protocol* (NTP).
b. Server NTP internal wajib ditetapkan sebagai sumber waktu utama, disinkronisasi dengan sumber waktu resmi (server NTP BSSN, BMKG, atau *stratum-1*/*stratum-2* terpercaya), dengan minimal 2 (dua) sumber eksternal untuk redundansi.
c. Zona waktu seluruh perangkat wajib diatur ke Waktu Indonesia Barat (WIB/*UTC+7*) kecuali terdapat kebutuhan teknis spesifik.
d. Verifikasi sinkronisasi waktu wajib dilaksanakan minimal 1 (satu) kali per bulan.
e. Sinkronisasi waktu merupakan prasyarat untuk keabsahan log, keabsahan bukti forensik, dan keabsahan Tanda Tangan Elektronik.

7. Penggunaan Program Utilitas Istimewa

a. Penggunaan program utilitas istimewa (*registry editor*, *packet sniffer*, *port scanner*, *disk editor*, *debugger* sistem, alat administrasi jarak jauh, dan sejenisnya) hanya diizinkan untuk personel dengan hak akses istimewa dan untuk keperluan tugas yang sah.
b. Daftar Program Utilitas Istimewa yang Diizinkan wajib disusun beserta ketentuan penggunaannya.
c. Program yang tidak termasuk dalam daftar dilarang dipasang atau digunakan tanpa persetujuan tertulis dari pimpinan yang berwenang.
d. Seluruh penggunaan program utilitas istimewa wajib dicatat dalam log.
e. Program yang tidak lagi diperlukan wajib segera dihapus.

8. Instalasi Perangkat Lunak pada Sistem Operasional

a. Instalasi perangkat lunak hanya diizinkan untuk perangkat lunak yang tercantum dalam Daftar Perangkat Lunak yang Disetujui.

b. Pengguna biasa (*non-administrator*) dilarang melakukan instalasi, penghapusan, atau modifikasi perangkat lunak secara mandiri.
c. Prosedur penambahan perangkat lunak baru:
    1) OPD mengajukan permohonan tertulis yang memuat: nama perangkat lunak, fungsi, justifikasi, dan informasi lisensi;
    2) evaluasi aspek keamanan, kompatibilitas, dan lisensi dilaksanakan;
    3) perangkat lunak yang disetujui ditambahkan ke Daftar yang Disetujui.
d. Perangkat lunak tidak berlisensi, bajakan, atau dari sumber tidak terpercaya dilarang.
e. Pemeriksaan perangkat lunak terpasang wajib dilaksanakan minimal 1 (satu) kali dalam 6 (enam) bulan. Perangkat lunak yang tidak tercantum dalam daftar wajib segera dihapus.
f. Daftar Perangkat Lunak yang Disetujui wajib diperbarui minimal 1 (satu) kali per tahun.

BAB XIII
KEAMANAN JARINGAN DAN LAYANAN CLOUD

A. Maksud dan Tujuan

Menetapkan pengendalian keamanan terhadap layanan jaringan yang disediakan oleh pihak ketiga, penguatan segregasi jaringan melalui segmentasi *VLAN* dan *microsegmentation*, penyaringan akses web, serta kebijakan penggunaan layanan *cloud* — guna melindungi infrastruktur jaringan dan data Pemerintah Kabupaten Kendal dari ancaman siber, kebocoran data, dan ketergantungan berlebihan pada penyedia layanan eksternal.

B. Ruang Lingkup

Seluruh infrastruktur jaringan (*LAN*, *WAN*, nirkabel), koneksi internet, layanan jaringan dari penyedia pihak ketiga, serta seluruh layanan *cloud* (*IaaS, PaaS, SaaS*) yang digunakan atau direncanakan untuk digunakan oleh OPD di lingkungan Pemerintah Kabupaten Kendal.

C. Ketentuan

1. Keamanan Layanan Jaringan

a. Setiap kontrak dengan penyedia layanan jaringan wajib memuat *Service Level Agreement* (SLA) keamanan yang mencakup minimal:
   1) jaminan ketersediaan layanan (*uptime*) minimal 99,5% per bulan untuk koneksi utama;
   2) waktu respons terhadap gangguan keamanan maksimal 4 (empat) jam;
   3) perlindungan terhadap serangan *DDoS* dasar;
   4) pelaporan insiden keamanan dalam waktu 1×24 jam;
   5) larangan penyedia mengakses konten lalu lintas data kecuali atas permintaan tertulis.

b. Persyaratan keamanan teknis dalam kontrak penyedia:
   1) koneksi wajib mendukung enkripsi untuk jalur yang membawa data Rahasia atau Terbatas;
   2) penyedia wajib memiliki sertifikasi keamanan yang relevan;
   3) penyedia wajib mengizinkan audit keamanan.

c. Kinerja dan kepatuhan SLA penyedia wajib dipantau setiap bulan dan dievaluasi secara menyeluruh setiap tahun.

d. Koneksi internet lokasi strategis wajib memiliki minimal 2 (dua) penyedia yang berbeda untuk redundansi.

2. Segregasi Jaringan

a. Segmentasi *VLAN* per OPD:
   1) setiap OPD wajib berada pada *VLAN* yang terpisah secara logis;
   2) lalu lintas antar-*VLAN* wajib dikendalikan melalui *firewall* atau *access control list* (ACL);
   3) kebijakan akses antar-*VLAN* mengikuti prinsip *deny-by-default*.

b. *Microsegmentation* untuk sistem kritis:
   1) sistem dengan prioritas tertinggi wajib ditempatkan pada segmen jaringan khusus yang terisolasi dari jaringan pengguna umum;
   2) akses ke segmen sistem kritis wajib melalui *firewall* berlapis;
   3) basis data sistem kritis wajib berada pada segmen terpisah dari server aplikasi (*database tier separation*).

c. *Network Access Control* (NAC):
   1) perangkat yang terhubung ke jaringan wajib diautentikasi dan diverifikasi kepatuhannya terhadap kebijakan keamanan sebelum diberikan akses;
   2) perangkat yang tidak memenuhi persyaratan wajib ditempatkan pada segmen karantina;
   3) implementasi NAC diprioritaskan untuk area dengan akses ke sistem kritis.
d. Jaringan tamu dan *Internet of Things* (IoT):
   1) jaringan tamu wajib terpisah dari jaringan operasional dan tidak memiliki akses ke sumber daya internal;
   2) perangkat IoT wajib ditempatkan pada *VLAN* terpisah dari jaringan data operasional.
e. Dokumentasi topologi jaringan wajib dipelihara dan diperbarui setiap terjadi perubahan.

3. Penyaringan Web

a. Sistem penyaringan web (*webfiltering*/*proxy*) wajib dioperasikan yang memblokir akses ke kategori situs:
   1) distribusi *malware* dan *exploit kits*;
   2) situs *phishing* dan penipuan;
   3) *command and control* (C2) *botnet*;
   4) konten dewasa/pornografi;
   5) perjudian daring;
   6) situs yang menyediakan alat peretasan;
   7) layanan berbagi berkas dan *torrent* publik.
b. Mekanisme *whitelist*:
   1) situs yang diblokir namun diperlukan untuk tugas kedinasan dapat di-*whitelist* melalui permohonan kepada unit kerja yang membidangi TIK;
   2) *whitelist* terbatas pada pengguna dan durasi tertentu;
   3) *whitelist* ditinjau setiap 3 (tiga) bulan.
c. Basis data kategori situs wajib diperbarui minimal setiap hari.
d. Akses yang diblokir wajib dicatat dalam log.
e. Upaya pengelabuan terhadap sistem penyaringan (VPN eksternal, *proxy* anonim, Tor) dari jaringan dinas dilarang.

4. Keamanan Layanan *Cloud*

a. Kebijakan penggunaan *cloud*:
   1) penggunaan layanan *cloud* oleh OPD wajib mendapat persetujuan dari unit kerja yang membidangi TIK melalui proses evaluasi keamanan;
   2) OPD dilarang menggunakan layanan *cloud* secara mandiri (*shadow IT*) tanpa persetujuan;
   3) Daftar Layanan *Cloud* yang Disetujui wajib disusun dan dimutakhirkan.

b. Klasifikasi data pada *cloud*:

Klasifikasi	**Ketentuan Penyimpanan di Cloud**
RAHASIA	Dilarang di cloud publik. Hanya diizinkan pada private cloud yang sepenuhnya dikendalikan atau cloud pemerintah.
TERBATAS	Diizinkan dengan: enkripsi end-to-end, data center di Indonesia, penyedia bersertifikasi.
BIASA	Diizinkan di cloud yang memenuhi standar keamanan minimum.

PUBLIK	Diizinkan tanpa persyaratan khusus.

Tabel 12. Klasifikasi data pada *cloud*

c. Kedaulatan data (*data sovereignty*):
   1) data Rahasia dan Terbatas yang disimpan di *cloud* wajib berada pada data center di wilayah Republik Indonesia;
   2) penyedia *cloud* wajib memberikan jaminan tertulis bahwa data tidak ditransfer ke luar Indonesia tanpa persetujuan;
   3) kunci enkripsi data Rahasia pada *cloud* wajib dikelola oleh Pemerintah Kabupaten Kendal (*customer-managed keys*).
d. Persyaratan penyedia cloud:
   1) penyedia untuk data Terbatas ke atas wajib memiliki minimal ISO 27001, *SOC 2 Type II*, atau Indeks KAMI dari BSSN;
   2) kontrak wajib memuat klausul keamanan sesuai BAB VIII;
   3) penyedia wajib mendukung MFA untuk akses administratif;
   4) penyedia wajib menyediakan log akses yang dapat diunduh dan diintegrasikan dengan sistem *logging*.
e. *Backup* dan kelangsungan:
   1) *backup* data pada cloud wajib mengikuti ketentuan BAB VI;
   2) salinan *backup* data kritis wajib disimpan secara independen dari penyedia *cloud*;
   3) uji *restore* dari *backup cloud* minimal 2 (dua) kali per tahun.
f. Strategi keluar (*exit strategy*):
   1) rencana migrasi keluar wajib tersedia untuk setiap layanan *cloud* sebelum kontrak ditandatangani;
   2) *exit strategy* mencakup: format dan prosedur ekspor data, *timeline* migrasi, konfirmasi penghapusan data oleh penyedia, dan alternatif layanan;
   3) *exit strategy* diuji validitasnya dan ditinjau setiap tahun;
   4) kontrak menjamin penyedia membantu proses migrasi keluar dan menyediakan data dalam format standar.
g. Insiden keamanan pada layanan *cloud* wajib ditangani sesuai prosedur BAB VII dengan koordinasi bersama penyedia *cloud*.

BAB XIV
KELANGSUNGAN BISNIS DAN PEMULIHAN BENCANA

A. Maksud dan Tujuan

Memastikan bahwa pengendalian keamanan informasi tetap dipertahankan selama terjadinya gangguan, infrastruktur TIK siap untuk dipulihkan sesuai target yang terukur, tersedia redundansi pada komponen kritis, serta terdapat Rencana Pemulihan Bencana (DRP) yang teruji — sehingga penyelenggaraan pemerintahan dan pelayanan publik Pemerintah Kabupaten Kendal dapat dilanjutkan dengan dampak minimal.

B. Ruang Lingkup

Seluruh sistem informasi, infrastruktur TIK, dan aset informasi kritis yang mendukung penyelenggaraan pemerintahan dan pelayanan publik di lingkungan Pemerintah Kabupaten Kendal, dalam menghadapi skenario gangguan meliputi: bencana alam, kegagalan infrastruktur, serangan siber masif, pandemi, dan gangguan sipil.

C. Ketentuan

1. Keamanan Informasi Selama Gangguan

a. Rencana Kelangsungan Keamanan Informasi (*Information Security Continuity Plan*) wajib disusun yang menetapkan langkah-langkah untuk mempertahankan pengendalian keamanan selama gangguan, mencakup minimal:
   1) identifikasi pengendalian keamanan minimum yang harus tetap aktif (autentikasi, pengendalian akses, *logging*, enkripsi, perlindungan *anti-malware*);
   2) prosedur alternatif apabila pengendalian teknis utama tidak berfungsi;
   3) kriteria aktivasi dan deaktivasi rencana kelangsungan.

b. Selama masa gangguan, prinsip berikut tetap berlaku tanpa pengecualian:
   1) data Rahasia tetap dilindungi dan tidak boleh diakses oleh pihak yang tidak berwenang;
   2) akses darurat ke sistem kritis hanya untuk personel yang tercantum dalam Daftar Personel Darurat;
   3) seluruh tindakan darurat wajib dicatat untuk audit pasca gangguan.

c. Apabila pemulihan memerlukan pelonggaran sementara terhadap kebijakan keamanan:
   1) pelonggaran wajib disetujui oleh pimpinan yang berwenang;
   2) dibatasi lingkup dan durasinya secara spesifik;
   3) seluruh aktivitasnya dicatat;
   4) dicabut segera setelah kondisi normal pulih.

d. Tim Manajemen Krisis wajib ditetapkan yang bertanggung jawab mengoordinasikan respons selama gangguan berskala besar.

e. Rencana Kelangsungan Keamanan Informasi wajib ditinjau minimal 1 (satu) kali per tahun atau setelah gangguan aktual.

2. Kesiapan TIK untuk Kelangsungan Bisnis

a. Analisis Dampak Bisnis (*Business Impact Analysis*/BIA):
   1) BIA wajib dilaksanakan minimal 1 (satu) kali per tahun untuk mengidentifikasi sistem kritis dan menetapkan prioritas pemulihan;

2) BIA wajib menetapkan *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) untuk setiap sistem kritis.

b. Target pemulihan sistem kritis:

Sistem / Layanan	RTO	RPO	Prioritas
Data center	4 Jam	1 Jam	1
Sistem Keuangan Daerah	4 Jam	1 Jam	1
Sistem Kepegawaian Daerah	4 Jam	1 Jam	1
Data Kependudukan	8 Jam	4 Jam	2
Portal Layanan publik	8 Jam	4 Jam	2
Website OPD	24 Jam	12 Jam	3
Email Dinas	24 Jam	12 Jam	3

Tabel 13. Target pemulihan sistem kritis

Keterangan:
- RTO: waktu maksimum yang diizinkan untuk memulihkan layanan;
- RPO: titik waktu terakhir data yang dapat diterima hilang;
- Target dapat disesuaikan berdasarkan BIA tahunan.

c. Strategi kelangsungan TIK wajib disusun yang memastikan target RTO dan RPO dapat dipenuhi, mencakup:
   1) frekuensi backup yang selaras dengan RPO;
   2) mekanisme *failover* untuk sistem prioritas tertinggi;
   3) lokasi pemulihan alternatif (*disaster recovery site*);
   4) prosedur pemulihan terdokumentasi untuk setiap sistem kritis.

d. Sumber daya pemulihan (perangkat cadangan, lisensi, konektivitas alternatif) wajib diidentifikasi, dianggarkan, dan tersedia dalam kondisi yang mendukung pencapaian target RTO.

e. Daftar Kontak Darurat TIK wajib disusun dan dipelihara.

3. Redundansi Fasilitas Pengolahan Informasi

a. Redundansi server:
   1) sistem dengan prioritas tertinggi wajib memiliki server cadangan yang dapat diaktifkan dalam waktu yang mendukung target RTO;
   2) konfigurasi server cadangan wajib identik atau setara dengan server utama;
   3) penerapan kluster server (*high availability*) wajib dievaluasi untuk sistem prioritas tertinggi.

b. Redundansi jaringan:
   1) jaringan *backbone* wajib memiliki jalur alternatif untuk rute kritis;
   2) koneksi internet lokasi strategis wajib memiliki minimal 2 (dua) penyedia yang berbeda;
   3) perangkat jaringan kritis wajib memiliki perangkat cadangan.

c. Redundansi daya listrik:
   1) UPS dengan kapasitas memadai;
   2) *generator* cadangan minimal 24 (dua puluh empat) jam operasi;
   3) pengujian generator dan *ATS* minimal setiap 3 (tiga) bulan.

d. Redundansi pendingin: unit cadangan wajib tersedia untuk diaktifkan saat unit utama mengalami kegagalan.

e. Seluruh komponen redundansi wajib diuji minimal setiap 6 (enam) bulan dan hasilnya didokumentasikan.

4. Rencana Pemulihan Bencana TIK (Disaster Recovery Plan)

a. Skenario bencana yang wajib dicakup dalam DRP minimal:
   1) Kebakaran — evakuasi, aktivasi backup *off-site*, pemulihan sesuai prioritas;

2) Banjir atau bencana alam — penyelamatan perangkat, aktivasi komunikasi alternatif, pemulihan bertahap;
3) Serangan siber masif (*ransomware*, *DDoS*) — isolasi jaringan, koordinasi dengan BSSN, pemulihan dari *backup* bersih, analisis forensik;
4) Kegagalan total lokasi utama — aktivasi *disaster recovery site*, *failover* layanan kritis.

b. Struktur DRP (6 fase):
1) Deteksi dan Notifikasi;
2) Penilaian Dampak;
3) Aktivasi DRP;
4) Pemulihan Sistem (sesuai prioritas dan target RTO);
5) Operasi Sementara;
6) Pemulihan Penuh dan Normalisasi.

c. DRP wajib menyertakan:
1) pohon komunikasi (*communication tree*);
2) lokasi penyimpanan DRP yang dapat diakses saat bencana (salinan fisik *off-site* dan digital terenkripsi);
3) daftar vendor dan kontak darurat;
4) prosedur eskalasi dan komunikasi publik.

d. DRP wajib ditinjau minimal 1 (satu) kali per tahun atau setelah perubahan signifikan pada infrastruktur.

5. Pengujian dan Latihan BCP/DRP

a. Pengujian wajib dilaksanakan minimal 1 (satu) kali per tahun dan setelah perubahan signifikan pada infrastruktur atau DRP.

b. Jenis pengujian:

Jenis Pengujian	Deskripsi
Tabletop Exercise (wajib setahun sekali)	Simulasi diskusi; meninjau Langkah DRP, alur komunikasi, dan pengambilan keputusan.
Walkthrough/ Functional Test (wajib setahun sekali)	Simulasi teknis parsial; *restore* dari *backup*, *failover* ke server cadangan tanpa gangguan produksi.
Full Simulation (wajib 2 tahun sekali)	Simulasi skala penuh di luar jam operasional dengan persetujuan pimpinan yang berwenang.

Tabel 14. Jenis pengujian BCP/DRP

c. Setiap pengujian wajib:
1) memiliki skenario tertulis;
2) mengukur: waktu pemulihan aktual vs RTO, kelengkapan data vs RPO, efektivitas komunikasi, dan kesiapan personel;
3) didokumentasikan dalam Laporan Pengujian BCP/DRP.

d. Temuan dan kelemahan wajib ditindaklanjuti dalam 30 (tiga puluh) hari kerja.

e. Hasil pengujian wajib dilaporkan kepada pimpinan yang berwenang dan digunakan sebagai masukan tinjauan risiko tahunan.

BAB XV
KEPATUHAN, AUDIT, DAN TINJAUAN KEAMANAN INFORMASI

A. Maksud dan Tujuan

Memastikan bahwa penyelenggaraan keamanan informasi di lingkungan Pemerintah Kabupaten Kendal memenuhi seluruh kewajiban hukum dan regulasi, menjaga kepatuhan terhadap hak kekayaan intelektual, melindungi rekaman SMKI, melaksanakan tinjauan independen, memantau kepatuhan internal melalui *self-assessment*, menjaga keamanan sistem selama audit, menjalin hubungan dengan forum keamanan, serta mengelola intelijen ancaman siber secara proaktif.

B. Ruang Lingkup

Seluruh OPD, sistem informasi, dan proses pengelolaan informasi di lingkungan Pemerintah Kabupaten Kendal yang tunduk pada peraturan perundang-undangan, kewajiban kontraktual, dan standar keamanan informasi yang berlaku.

C. Ketentuan

1. Kepatuhan terhadap Persyaratan Hukum dan Regulasi

a. Register Kewajiban Hukum dan Regulasi wajib disusun dan dimutakhirkan yang mengidentifikasi seluruh peraturan perundang-undangan yang relevan, minimal mencakup:

No	Regulasi	Kewajiban Utama
1	UU No. 11/2008 jo. UU No. 19/2016 tentang ITE	Keamanan sistem elektronik, TTE
2	UU No. 14/2008 tentang KIP	Keterbukaan informasi publik
3	UU No. 27/2022 tentang PDP	Pelindungan data pribadi, notifikasi breach 3x24 jam
4	PP No. 71/2019 tentang PTSE	Penyelenggaraan sistem elektronik
5	Perpres No. 95/2018 tentang SPBE	Keamanan SPBE
6	Peraturan BSSN No. 4/2021	Standar teknis keamanan SPBE
7	Perbup Kendal No. 35/2021 jo. Perbup Kendal No. 33/2024	Keamanan SPBE Pemkab Kendal
8	Perbup Kendal No. 57/2023	SMKI Pemkab Kendal

Tabel 15. Contoh register kewajiban hukum dan regulasi

b. Mekanisme pemantauan kepatuhan:
   1) personel atau unit yang bertanggung jawab memantau perkembangan regulasi wajib ditunjuk;
   2) evaluasi kepatuhan terhadap seluruh regulasi wajib dilaksanakan minimal 1 (satu) kali per tahun;
   3) hasil evaluasi dilaporkan kepada pimpinan yang berwenang;
   4) ketidakpatuhan wajib didokumentasikan dalam Rencana Tindakan Kepatuhan.

c. Register Kewajiban Hukum wajib diperbarui minimal setiap 6 (enam) bulan atau segera setelah regulasi baru terbit.

d. Kontrak dengan pihak ketiga wajib diperiksa kesesuaiannya dengan kewajiban hukum sesuai BAB VIII.

e. ASN yang menangani keamanan informasi wajib memahami kewajiban hukum yang relevan melalui program pelatihan.

2. Hak Kekayaan Intelektual

a. Seluruh perangkat lunak yang digunakan wajib memiliki lisensi yang sah; penggunaan perangkat lunak bajakan dilarang.
b. Register Lisensi Perangkat Lunak wajib dikelola yang mencatat: nama perangkat lunak, jenis lisensi, jumlah lisensi, masa berlaku, dan OPD pengguna.
c. Register Lisensi wajib ditinjau minimal setiap 6 (enam) bulan untuk memastikan:
   1) jumlah instalasi tidak melebihi jumlah lisensi;
   2) lisensi yang akan habis diperpanjang tepat waktu;
   3) perangkat lunak yang tidak digunakan dihapus dan lisensinya dioptimalkan.
d. Pengadaan perangkat lunak baru wajib mempertimbangkan perangkat lunak *open source* sebagai alternatif.
e. Hak kekayaan intelektual atas aplikasi dan karya digital yang dikembangkan oleh atau untuk Pemerintah Kabupaten Kendal wajib diatur dalam kontrak sesuai BAB VIII.
f. ASN dilarang menggandakan, mendistribusikan, atau menggunakan perangkat lunak berlisensi di luar ketentuan lisensi.

3. Perlindungan Rekaman SMKI

a. Jangka waktu retensi rekaman:

Jenis Rekaman	Retensi Minimum
Kebijakan dan prosedur (versi terkini + 2 versi)	Selama berlaku + 3 tahun setelah dicabut/diganti
Register Risiko dan Daftar Aset	5 tahun
Laporan Audit dan Tinjauan	5 tahun
Laporan Insiden dan Bukti Digital	5 tahun atau hingga proses hukum selesai
Log sistem	12 bulan (kritis) 6 bulan (non-kritis)
Bukti pelatihan dan NDA	5 tahun
Kontrak pihak ketiga	Selama berlaku + 5 tahun

Tabel 16. Jangka waktu retensi rekaman SMKI

b. Perlindungan rekaman:
   1) rekaman SMKI wajib dilindungi dari modifikasi tidak sah; rekaman digital menggunakan mekanisme yang menjamin integritas;
   2) akses terhadap rekaman dibatasi berdasarkan *need-to-know*;
   3) rekaman fisik disimpan di tempat yang terlindungi;
   4) rekaman digital wajib dicadangkan.
c. Indeks Rekaman SMKI wajib disusun yang mencantumkan: jenis rekaman, lokasi penyimpanan, penanggung jawab, masa retensi, dan prosedur pemusnahan.
d. Pemusnahan rekaman yang telah melampaui masa retensi wajib dilaksanakan secara aman dan didokumentasikan.
e. Rekaman yang berkaitan dengan proses hukum yang berjalan tidak boleh dimusnahkan hingga proses hukum selesai.

4. Tinjauan Independen Keamanan Informasi

a. Tinjauan independen terhadap SMKI wajib dilaksanakan minimal 1 (satu) kali per tahun oleh:
   1) Inspektorat Kabupaten Kendal;
   2) Auditor eksternal independen yang berkompeten; atau
   3) Kombinasi keduanya.

b. Tinjauan tambahan wajib dilaksanakan setelah insiden Prioritas 1 (Kritis) atau perubahan signifikan pada organisasi, teknologi, atau regulasi.

c. Kualifikasi auditor:
   1) kompetensi dan pengalaman di bidang keamanan informasi, dibuktikan dengan sertifikasi atau pengalaman memadai;
   2) independen dari area yang diaudit;
   3) menandatangani perjanjian kerahasiaan sebelum pelaksanaan.

d. Lingkup tinjauan minimal mencakup:
   1) kesesuaian kebijakan dengan standar ISO/IEC 27001:2022 dan regulasi yang berlaku;
   2) efektivitas implementasi kontrol pada sampel OPD;
   3) pengelolaan risiko;
   4) penanganan insiden;
   5) kepatuhan terhadap kewajiban hukum;
   6) tindak lanjut temuan audit sebelumnya.

e. Hasil tinjauan:
   1) didokumentasikan dalam Laporan Audit Keamanan Informasi;
   2) temuan ditindaklanjuti dengan Rencana Tindakan Perbaikan (kritis: 30 hari, mayor: 60 hari, minor: 90 hari);
   3) verifikasi implementasi dilaksanakan;
   4) temuan belum ditindaklanjuti sesuai tenggat wajib dieskalasi.

f. Program Audit Keamanan Informasi Tahunan wajib disusun.

5. Kepatuhan Internal (*Self-Assessment*)

a. Setiap OPD wajib melaksanakan *self-assessment* kepatuhan keamanan informasi minimal 1 (satu) kali per tahun menggunakan Daftar Periksa Kepatuhan standar.

b. Daftar Periksa Kepatuhan mencakup verifikasi terhadap kontrol utama, meliputi minimal:
   1) ketersediaan dan pemutakhiran Daftar Aset Informasi;
   2) pelaksanaan pelatihan kesadaran keamanan informasi;
   3) kepatuhan prosedur manajemen akses;
   4) pelaksanaan *backup* sesuai jadwal;
   5) penerapan kebijakan meja bersih dan layar bersih;
   6) ketersediaan dan pengujian prosedur penanganan insiden;
   7) kepatuhan penggunaan perangkat lunak berlisensi;
   8) pemutakhiran Register Risiko.

c. Hasil *self-assessment* wajib didokumentasikan dalam Laporan *Self-Assessment* Kepatuhan yang ditandatangani oleh pimpinan OPD.

d. Laporan dari seluruh OPD wajib dikonsolidasikan menjadi Laporan Kepatuhan Keamanan Informasi tahunan.

e. OPD dengan temuan ketidakpatuhan wajib menyertakan Rencana Perbaikan beserta tenggat waktu.

f. Verifikasi lapangan terhadap hasil *self-assessment* dapat dilaksanakan apabila diperlukan.

6. Perlindungan Sistem Informasi Selama Audit

a. Kegiatan audit terhadap sistem informasi produksi wajib dikomunikasikan minimal 5 (lima) hari kerja sebelum pelaksanaan.

b. Aktivitas audit teknis yang berpotensi mengganggu (*vulnerability scanning*, *penetration testing*, analisis log intensif) wajib dilaksanakan di luar jam operasional utama kecuali mendapat persetujuan tertulis.
c. Auditor dilarang melakukan perubahan konfigurasi, modifikasi data, atau instalasi perangkat lunak pada sistem produksi tanpa persetujuan eksplisit.
d. Akses auditor ke sistem produksi:
    1) dibatasi pada sistem dan data yang diperlukan;
    2) menggunakan akun audit khusus yang dinonaktifkan setelah audit;
    3) dicatat dalam log akses.
e. Alat dan perangkat lunak audit wajib disetujui terlebih dahulu untuk memastikan keamanan.
f. Pasca audit, seluruh akun audit khusus wajib dinonaktifkan dan berkas kerja auditor pada sistem produksi wajib dihapus.

7. Hubungan dengan Forum Keamanan Informasi

a. Hubungan aktif wajib dijalin dan dipelihara minimal dengan:
    1) BSSN — termasuk berlangganan notifikasi ancaman;
    2) ID-SIRTII sebagai komunitas respons insiden nasional;
    3) Forum keamanan siber antar-pemerintah daerah;
    4) Komunitas atau asosiasi keamanan informasi yang relevan.
b. Partisipasi meliputi:
    1) menerima dan mendistribusikan peringatan keamanan;
    2) berbagi informasi insiden yang tidak bersifat rahasia;
    3) mengikuti kegiatan pelatihan dan seminar keamanan.
c. Informasi yang diperoleh dari forum wajib dievaluasi relevansinya dan diintegrasikan ke dalam penilaian risiko.
d. Keanggotaan dan partisipasi wajib didokumentasikan dan dilaporkan dalam Laporan Keamanan Informasi Tahunan.

8. Intelijen Ancaman

a. Sumber intelijen ancaman yang dipantau:
    1) BSSN — peringatan keamanan, laporan ancaman siber nasional;
    2) Vendor keamanan — notifikasi kerentanan dan ancaman;
    3) CVE/NVD (*National Vulnerability Database*);
    4) Laporan insiden dari ID-SIRTII dan forum kepentingan khusus;
    5) Publikasi keamanan informasi terpercaya.
b. Proses pengelolaan intelijen ancaman:
    1) pemantauan sumber dilaksanakan minimal setiap minggu;
    2) setiap informasi ancaman dievaluasi relevansinya terhadap konteks Pemerintah Kabupaten Kendal;
    3) informasi yang relevan didistribusikan kepada pengelola sistem OPD terkait dalam 1×24 jam;
    4) informasi dengan indikasi risiko kritis dieskalasi segera.
c. Pemanfaatan intelijen ancaman:
    1) diintegrasikan ke dalam penilaian risiko;
    2) kerentanan yang teridentifikasi ditindaklanjuti sesuai prosedur manajemen kerentanan dalam BAB VI;
    3) tren ancaman digunakan untuk pembaruan materi pelatihan.

d. Laporan Intelijen Ancaman Triwulanan wajib disusun yang merangkum: ancaman terkini, kerentanan, tren serangan, dan rekomendasi tindakan pencegahan.

SEKRETARIS DAERAH
KABUPATEN KENDAL,

AGUS DWI LESTARI