



PEMERINTAH KABUPATEN KLATEN
DINAS KOMUNIKASI DAN INFORMATIKA

Jln. Pemuda No. 294 Klaten Blok C Kode Pos 57424
Telepon. 0272.321046 (Psw. 253), Faksimile.
0272.322567

Laman: <https://diskominfo.klaten.go.id>, email: diskominfo@klaten.go.id

KEPUTUSAN
KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
PEMERINTAH KABUPATEN KLATEN
NOMOR 000.6/43/2026
TENTANG
PEMBENTUKAN STRUKTUR ORGANISASI SISTEM MANAJEMEN
KEAMANAN INFORMASI DAN *DATA PROTECTION OFFICER*
BERBASIS SNI ISO / IEC 27001:2022

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN
KLATEN,

- Menimbang : a. bahwa sejalan dengan kebutuhan organisasi akan pengelolaan keamanan informasi secara terpadu sesuai dengan standarisasi SNI ISO / IEC 27001:2022 tentang Sistem Manajemen Keamanan Informasi/*Information Security Management System* (SMKI/ISMS) yang diakui secara Internasional;
- b. rencana Implementasi Sistem Manajemen Keamanan Informasi berbasis standardisasi SNI ISO / IEC 27001:2022 sebagai bentuk perwujudan komitmen organisasi atas keamanan informasi;
- c. bahwa proses dan aktivitas pengelolaan Sistem Manajemen Keamanan Informasi yang dipersyaratkan oleh SNI ISO / IEC 27001:2022 harus dijalankan oleh organisasi;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, b, dan c perlu menetapkan Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Klaten tentang Pembentukan Struktur Organisasi Sistem Manajemen Keamanan Informasi dan *Data Protection Officer* Berbasis SNI ISO / IEC 27001:2022;
- e. bahwa yang namanya tercantum pada keputusan ini dipandang memenuhi syarat untuk diangkat sebagai Tim Sistem Manajemen Keamanan Informasi dan *Data Protection Officer* Berbasis SNI ISO / IEC 27001:2022.

- Mengingat : 1. Undang-Undang Nomor 23 Tahun 2014, tentang Pemerintah Daerah;
2. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
3. Undang-Undang Nomor 14 Tahun 2008 tentang keterbukaan Informasi Publik;
4. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Perubahan atas Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah;
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE);
7. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
8. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik;
9. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber;
10. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;
11. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 9 Tahun 2021 tentang Perubahan Atas Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2021 Tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001:2022 Menggunakan Indeks Keamanan Informasi

12. Peraturan Daerah Kabupaten Klaten Nomor 18 Tahun 2018 tentang Penyelenggaraan e-Government;
13. Peraturan Daerah Kabupaten Klaten Nomor 7 Tahun 2021 tentang Perubahan atas Peraturan Daerah Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Klaten;
14. Peraturan Bupati Klaten Nomor 16 Tahun 2023 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Klaten.
15. Peraturan Bupati Klaten Nomor 57 Tahun 2024 tentang Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Klaten.

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA TENTANG PEMBENTUKAN STRUKTUR ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI DAN *DATA PROTECTION OFFICER* BERBASIS SNI ISO / IEC 27001:2022.

KESATU : Membentuk Struktur Organisasi Sistem Manajemen Keamanan Informasi (SMKI) dan *Data Protection Officer* (DPO) berbasis SNI ISO / IEC 27001:2022 dengan Susunan dan Personalia sebagaimana tercantum dalam Lampiran, yang merupakan bagian tidak terpisahkan dari Keputusan ini;

KEDUA Struktur Organisasi Sistem Manajemen Keamanan informasi (SMKI) dan *Data Protection Officer* (DPO) berbasis SNI ISO / IEC 27001:2022 sebagaimana dimaksud dalam diktum KESATU memiliki tugas dan tanggung jawab sebagai berikut:

A. Penanggung Jawab

Tugas dan Tanggung Jawab:

- 1) Memberikan arahan dan tujuan umum dari SMKI organisasi, dalam bentuk kebijakan sistem manajemen keamanan informasi (SMKI).
- 2) Memastikan bahwa tujuan dan rencana dari SMKI organisasi telah ditetapkan.
- 3) Menetapkan struktur organisasi beserta alokasi tugas dan tanggung jawab dalam SMKI

organisasi.

- 4) Mengkomunikasikan kepada personil terkait pentingnya pemenuhan aturan terkait keamanan informasi organisasi dan peraturan perundang-undangan yang berlaku serta perlunya peningkatan SMKI organisasi secara berkesinambungan.
- 5) Menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasi, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan SMKI organisasi.
- 6) Menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima.
- 7) Menyetujui tingkat risiko keamanan informasi
- 8) Memastikan pelaksanaan audit internal SMKI.
- 9) Melaksanakan tinjauan manajemen SMKI.

Wewenang:

- 1) Menyetujui kebijakan, sasaran, dan tingkat risiko sistem manajemen keamanan informasi.
- 2) Menyetujui struktur organisasi tim SMKI.
- 3) Memerintahkan Koordinator SMKI untuk memastikan bahwa implementasi SMKI telah dijalankan dengan baik.
- 4) Melimpahkan tanggung jawab pelaksanaan audit internal kepada Koordinator audit internal.
- 5) Menyetujui aktivitas yang terkait sistem manajemen keamanan informasi.

B. *Chief Information Security Officer (CISO)*

Target pengamanan informasi Chief Information Security Officer (CISO) yaitu aktifitas SMKI berjalan sesuai dengan program kerja yang telah ditetapkan, serta mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Menyusun, mengkoordinasikan serta memantau pelaksanaan program kerja SMKI.
- 2) Mengkoordinasikan pelaksanaan proses manajemen risiko SMKI organisasi.
- 3) Mengkoordinasikan pelaksanaan aktivitas SMKI serta pengamanan informasi di organisasi.
- 4) Mengkoordinasikan proses peninjauan secara

berkala terhadap implementasi SMKI di organisasi.

- 5) Mengkoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di organisasi.
- 6) Mengkoordinasikan aktivitas dan tindakan untuk meningkatkan efektivitas SMKI, yang mencakup antara lain tindakan perbaikan dan pencegahan untuk ketidaksesuaian yang ditemukan dalam proses audit serta pelaksanaan rencana penanganan risiko.
- 7) Memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi organisasi kepada penanggung jawab SMKI.

Wewenang:

- 1) Mengkoordinasikan Tim SMKI untuk menjalankan tugas dan tanggung jawab masing-masing dengan baik
- 2) Memberikan peringatan kepada personil Tim SMKI apabila melakukan pelanggaran
- 3) Membuat keputusan tindakan perbaikan apabila terjadi ketidaksesuaian
- 4) Membuat keputusan terhadap hal-hal yang berkaitan dengan keamanan informasi organisasi

C. *Data Protection Officer (DPO)*

Data Protection Officer memiliki tugas dan tanggung jawab sebagai berikut:

- 1) Menginformasikan dan memberikan saran untuk pengendali data pribadi atau prosesor data pribadi
- 2) Memantau dan memastikan kepatuhan terhadap Undang-undang ini dan kebijakan pengendali data pribadi atau prosesor data pribadi, termasuk penugasan, tanggung jawab, peningkatan kesadaran dan pelatihan pihak yang terlibat dalam pemrosesan data pribadi dan audit terkait
- 3) Memberikan saran mengenai penilaian dampak Pelindungan Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor

Data Pribadi

- 4) Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi

Wewenang:

- 1) Memberikan saran mengenai penilaian dampak perlindungan data pribadi dan memantau kinerja pengendali data pribadi dan prosesor data pribadi
- 2) Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan data pribadi, termasuk melakukan konsultasi mengenai mitigasi risiko dan/atau hal lainnya

D. Koordinator Audit Internal

Target pengamanan informasi koordinator auditor internal yaitu terlaksananya kegiatan internal audit ke seluruh organisasi dalam lingkup SMKI sesuai dengan program audit yang telah ditetapkan. Koordinator auditor internal mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Menyusun dan memantau program dan jadwal audit internal maupun eksternal SMKI.
- 2) Mengkoordinasikan pelaksanaan proses audit internal SMKI.
- 3) Merangkum dan melaporkan hasil audit internal SMKI kepada manajemen puncak.
- 4) Memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektivitas SMKI.
- 5) Mengkoordinasikan proses verifikasi tindakan perbaikan dan pencegahan terhadap ketidaksesuaian yang ditemukan dalam proses audit internal maupun eksternal SMKI.

Wewenang:

- 1) Memimpin kegiatan audit internal.
- 2) Memberi temuan-temuan atas ketidaksesuaian.
- 3) Memberi tugas kepada auditee untuk melakukan tindakan perbaikan.

E. Koordinator Pengendalian Dokumen

Target pengamanan informasi koordinator pengendalian dokumen yaitu memastikan terlaksananya proses pengklasifikasian, pelabelan, dan pengamanan seluruh informasi di organisasi yang menjadi tanggung jawabnya. Koordinasi unit mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Membantu para koordinator dalam menjalankan prosedur pengendalian dokumen, rekaman dan kepatuhan pada perundangan yang berlaku.
- 2) Memasukkan data dokumen ke dalam daftar dokumen dan memastikan bahwa informasi yang diberikan akurat dan terkini.
- 3) Memastikan dokumen disahkan sebelum didistribusikan
- 4) Melakukan perubahan dokumen bila diperlukan dengan berkoordinasi dengan Koordinator terkait
- 5) Memastikan seluruh dokumen telah disosialisasikan dan didistribusikan ke bagian yang berkepentingan
- 6) Memastikan seluruh dokumen disimpan dan dijaga dari kerusakan serta mudah untuk ditelusuri
- 7) Menarik atau memusnahkan dokumen yang sudah kadaluarsa.

Wewenang:

- 1) Menyetujui dokumen-dokumen yang dibuat oleh pemilik dokumen.
- 2) Memerintahkan personil terkait untuk melengkapi form dan rekaman yang diperlukan dalam implementasi SMKI.

F. Koordinator Manajemen Aset

Target pengamanan informasi koordinator manajemen aset yaitu semua aset informasi dan aset pemrosesan informasi tercatat dalam daftar aset informasi Dinas Komunikasi dan Informatika

secara akurat. Koordinator manajemen aset mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Mengkoordinasikan dan memantau pengelolaan aset penting terkait informasi dan sistem informasi organisasi. Hal ini mencakup proses registrasi, inventarisasi serta pemeliharaan inventarisasi aset.
- 2) Menyusun dan memelihara dokumen registrasi aset penting informasi dan sistem informasi organisasi
- 3) Melakukan peninjauan terkait proses penanganan aset penting terkait informasi dan sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan aset dalam SMKI organisasi.

Wewenang:

- 1) Menyetujui penggunaan aset mengenai keamanan informasi.
- 2) Memberi peringatan kepada pemilik aset apabila pemilik aset tidak melakukan perlindungan pada aset yang dimilikinya.

G. Koordinator Manajemen Risiko

Target pengamanan informasi koordinator manajemen risiko yaitu Proses risk assessment dan review dilakukan sesuai jadwal yang telah ditetapkan. Koordinator manajemen Risiko mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Menyusun dan mengkoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di organisasi.
- 2) Melakukan proses registrasi terhadap risiko SMKI di organisasi.
- 3) Melakukan pemutakhiran secara rutin terhadap risiko organisasi.
- 4) Menyusun dan memelihara dokumen dan memelihara profil risiko dan rencana pengendalian risiko SMKI organisasi.

Wewenang:

- 1) Menyetujui penanganan atau mitigasi risiko keamanan informasi.
- 2) Memberi himbauan kepada pemilik risiko agar memantau risiko secara berkala.

H. Koordinator Manajemen Keamanan Fisik dan Sistem Informasi

Target pengamanan informasi koordinator manajemen keamanan fisik dan sistem informasi yaitu tidak terjadi insiden keamanan informasi yang disebabkan oleh kelemahan pengamanan fisik dan sistem di Dinas Komunikasi dan Informatika Kabupaten Klaten. Koordinator manajemen keamanan fisik dan sistem informasi mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Mengkoordinasikan dan memantau proses dan aktivitas pengamanan fisik dan lingkungan dalam organisasi.
- 2) Melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan fisik organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi.
- 3) Melaksanakan proses pengelolaan dan pemeliharaan hak akses fisik ke fasilitas organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi.
- 4) Mengkoordinasikan dan memantau proses dan aktivitas pengelolaan akses logikal dari pengguna.
- 5) Melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan akses logikal ke sistem informasi organisasi secara internal berdasarkan kebijakan dan prosedur terkait keamanan akses logikal ke sistem informasi organisasi.
- 6) Mengkoordinasikan dan memantau pengelolaan keamanan operasional sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan

operasional sistem informasi organisasi.

- 7) Melaksanakan proses pengelolaan dan pemeliharaan akses logikal dari pengguna ke sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait keamanan akses logikal ke sistem informasi organisasi. Hal ini mencakup proses pendaftaran, pemeliharaan dan pencabutan hak akses logikal pengguna ke sistem informasi.
- 8) Mengakomodasi penyusunan dan pemeliharaan matriks pengendalian akses bersama-sama dengan unit bisnis pemilik aplikasi dan atau data.
- 9) Mengkoordinasikan dan memantau pengelolaan keamanan operasional sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan operasional sistem informasi organisasi.
- 10) Memastikan dan mengkoordinasikan proses keamanan informasi diimplementasikan secara menyeluruh sesuai dengan proses bisnis organisasi
- 11) Memastikan dan mengkoordinasikan penggunaan seluruh peralatan operasional yang digunakan adalah sesuai dengan persyaratan Sistem Manajemen Keamanan Informasi
- 12) Memonitor kegiatan pelaksanaan operasional teknis organisasi berlangsung dengan efektif dan sesuai Standar Sistem Manajemen Keamanan Informasi
- 13) Meninjau keberlangsungan pelaksanaan operasional teknis organisasi secara berkala dan menyeluruh
- 14) Memastikan dan mengkoordinasikan kontrol deteksi, pencegahan dan pemulihan untuk melindungi ancaman malware telah diterapkan.
- 15) Memastikan dan mengkoordinasikan penggunaan perangkat lunak yang digunakan adalah perangkat yang aman.
- 16) Meninjau kondisi perangkat lunak dan konten data secara berkala.

Wewenang:

- 1) Memberi persetujuan kepada pihak-pihak yang akan berkunjung.
- 2) Memberi peringatan kepada pemilik aset yang tidak memberi perlindungan pada aset yang diletakkan di luar kantor.
- 3) Menyetujui penggunaan peralatan operasional organisasi mengenai keamanan informasi
- 4) Memerintahkan personil untuk melengkapi form dan rekaman yang diperlukan dalam implementasi SMKI
- 5) Memonitor keberlangsungan implementasi operasional SMKI
- 6) Mengevaluasi keberlangsungan implementasi SMKI di dalam organisasi di departemen operasional
- 7) Menyetujui penggunaan perangkat lunak mengenai keamanan informasi.
- 8) Mengevaluasi kondisi penggunaan perangkat lunak dan konten data secara berkala

I. Koordinator Manajemen Insiden Keamanan Informasi dan Keberlangsungan Bisnis

Target pengamanan informasi koordinator manajemen insiden keamanan informasi yaitu permasalahan gangguan keamanan informasi dapat diselesaikan sesuai dengan perjanjian penanganan gangguan keamanan informasi.

Koordinator manajemen insiden keamanan informasi mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Mengkoordinasikan dan memantau pengelolaan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi.
- 2) Menerima serta mengelola laporan terkait kejadian, kelemahan dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi.
- 3) Mendokumentasikan proses pengelolaan

insiden keamanan informasi di organisasi.

- 4) Mengkoordinasikan dan memantau pengelolaan manajemen keberlangsungan bisnis di organisasi berdasarkan kebijakan dan prosedur terkait manajemen keberlangsungan bisnis organisasi.
- 5) Mengkoordinasikan penyusunan, pengujian dan pemeliharaan rencana kelangsungan bisnis dan rencana pemulihan bencana organisasi.
- 6) Memastikan terjaganya aspek keamanan informasi dalam proses manajemen pengelolaan bisnis.

Wewenang:

- 1) Menentukan tindakan penanganan insiden yang sedang terjadi.
- 2) Menentukan personil yang bertanggung jawab atas penanganan insiden.
- 3) Menyetujui rencana keberlangsungan bisnis.
- 4) Menentukan jadwal simulasi keberlangsungan bisnis.
- 5) Menentukan berlakunya Business Continuity Plan (BCP) apabila terjadi bencana yang telah ditetapkan dalam BCP.

J. Koordinator Keamanan Pemasok dan Kepatuhan Hukum

Target pengamanan informasi koordinator keamanan penyedia dan kepatuhan standar keamanan yaitu Teridentifikasinya seluruh persyaratan peraturan perundang-undangan terkait keamanan informasi dan terlaksananya proses pengukuran efektivitas SMKI dan kontrol keamanan informasi serta penyedia/pihak ketiga mengetahui standar SMKI organisasi. Koordinator keamanan penyedia dan kepatuhan standar keamanan mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Menganalisis risiko pekerjaan yang dilakukan supplier/pihak ketiga terhadap keamanan informasi.
- 2) Memastikan persyaratan keamanan informasi dalam menangani risiko terkait pekerjaan pemasok/pihak ketiga didokumentasikan dan

disetujui kedua belah pihak.

- 3) Memastikan kontrak pemasok/pihak ketiga terdapat kewajiban untuk menjaga keamanan informasi atau kontrak dapat dilengkapi dengan perjanjian kerahasiaan (NDA) yang ditandatangani semua personil pemasok/pihak ketiga yang akan melakukan aktivitas.
- 4) Memastikan kontrak pemasok/pihak ketiga terdapat kewajiban untuk memastikan rantai pasokan yang digunakan oleh pemasok/pihak ketiga dalam memberikan layanan untuk menjalankan prasyarat keamanan informasi yang berlaku.
- 5) Memastikan pemasok/pihak ketiga mendapatkan sosialisasi kebijakan dan prosedur terkait keamanan informasi sebelum mereka melakukan pekerjaan.
- 6) Melakukan peninjauan terhadap layanan yang diberikan pemasok/pihak ketiga sesuai dengan kontrak secara berkala.
- 7) Mengkoordinasikan kegiatan audit pemasok/pihak ketiga untuk mengetahui bagaimana proses pengamanan informasi milik organisasi yang dilakukan oleh pemasok/pihak ketiga.
- 8) Menganalisis risiko keamanan informasi yang mungkin terjadi apabila ada akan dilakukan pergantian pemasok/pihak ketiga yang bekerjasama dengan organisasi khususnya proses bisnis yang kritis yang didukung oleh pemasok/pihak ketiga.
- 9) Memantau undang-undang dan peraturan yang terkait dengan proses bisnis dan keamanan informasi.
- 10) Mengkoordinasikan proses pemenuhan undang-undang dan peraturan yang berlaku.
- 11) Memastikan organisasi memenuhi undang-undang dan peraturan yang berlaku.

Wewenang:

- 1) Menentukan tindakan atas hasil evaluasi pemasok/pihak ketiga.
- 2) Memberi persetujuan kontrak dan perjanjian

dengan pemasok/pihak ketiga dalam kaitan kepatuhan keamanan informasi.

- 3) Memberi saran dan perbaikan terkait proses pemenuhan undang-undang dan peraturan yang berlaku.

K. Koordinator Keamanan Sumber Daya Manusia

Target pengamanan informasi koordinator keamanan sumber daya manusia yaitu seluruh pegawai Dinas Komunikasi dan Informatika Kabupaten Klaten mendapatkan pengetahuan pengamanan informasi dan mencegah terjadi insiden keamanan informasi yang disebabkan oleh human error atau ketidaktahuan personil. Koordinator keamanan sumber daya manusia mempunyai tugas dan tanggung jawab sebagai berikut:

- 1) Memberikan sosialisasi kepada SDM baru terkait SMKI pada saat onboarding.
- 2) Menyusun dan mengkoordinasikan prosedur keamanan sumber daya manusia serta memastikan prosedur tersebut terimplementasi.
- 3) Mengkoordinasikan proses pengukuran efektivitas kegiatan keamanan sumber daya manusia.
- 4) Menyusun rencana jadwal dan melaksanakan kegiatan pelatihan yang berhubungan dengan peningkatan kualitas pengetahuan SDM secara berkala.
- 5) Memastikan keamanan informasi terkait atau milik SDM yang disimpan, dikendalikan dan diproses oleh organisasi
- 6) Mengkoordinasikan kepada seluruh pihak (SDM, pihak ketiga, dan SDM lainnya yang terkait) untuk meningkatkan kesadaran SMKI
- 7) Memastikan setiap SDM telah menandatangani perjanjian kerahasiaan (NDA).
- 8) Melaksanakan sosialisasi secara berkala untuk meningkatkan kesadaran kepada seluruh pihak akan pentingnya SMKI (SDM Organisasi dan pihak relevan lainnya)

Wewenang:

- 1) Merencanakan pelatihan, sertifikasi dan bimtek

kompetensi yang memadai untuk personil tim SMKI.

2) Memberi peringatan atas pelanggaran yang terkait dengan keamanan informasi.

KETIGA : Dalam melaksanakan tugas Tim Pelaksana Sistem Manajemen Keamanan Informasi (SMKI) berbasis SNI ISO / IEC 27001:2022 bertanggung jawab kepada Bupati Klaten melalui Kepala Dinas Komunikasi dan Informatika Kabupaten Klaten;

KEEMPAT : Untuk kelancaran pelaksanaan tugas Tim Pelaksana Sistem Manajemen Keamanan Informasi (SMKI) berbasis SNI ISO / IEC 27001:2022 dapat berhubungan dengan pihak-pihak lain yang dipandang perlu;

KELIMA : Keputusan ini berlaku sejak ditetapkan.

Ditetapkan di Klaten
Pada tanggal : 13 Agustus 2026
Kepala Dinas Komunikasi dan Informatika
Kabupaten Klaten



Aris Pramana, S.E., M.M
Pembina Tingkat I
NIP 197507182005011006

LAMPIRAN
KEPUTUSAN KEPALA DINAS
KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLATEN
NOMOR : 000.6/43/2026
TANGGAL : 13 Agustus 2026

SUSUNAN PENGELOLA SISTEM MANAJEMEN KEAMANAN
INFORMASI BERBASIS SNI ISO / IEC 27001:2022
DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KLATEN

No	Kedudukan	Jabatan	Nama
1	Penanggung Jawab	Kepala Dinas Komunikasi dan Informatika Kabupaten Klaten	Aris Pramana, S.E. M.M.
2	Chief Information Security Officer (CISO)	Sekretaris Dinas Komunikasi dan Informatika Kabupaten Klaten	Andi Hermanto,S.Kom., M.Eng
3	Koordinator Auditor Internal	Kepala Bidang Informatika dan Persandian	Heri Wismo Handono, S.E., M.M. Anggota : - Nazarudin, S.Kom.
4	Koordinator Pengendalian Dokumen	Pejabat Fungsional Pranata Komputer Terampil	Pramesti Ayupratiwi, A.Md.T
5	Koordinator Manajemen Aset	Pejabat Pengelola Barang Milik Daerah Diskominfo	Cyntia Wahyu Puspita, A.Md. Anggota: - Margi Handayani S.Sos
6	Koordinator Manajemen Risiko	Pejabat Fungsional Pranata Komputer Terampil	Riski Amalia A.Md. Anggota: - Danang Dewantoro
7	Koordinator Manajemen Keamanan Fisik dan Sistem Informasi	Pejabat Fungsional Pranata Komputer Ahli Pertama	Syaifulloh Amien Pandega Perdana, S.Kom., M.Eng Anggota: - Doddy Ashrib CP - M. Nurul Khomsa
8	Koordinator Manajemen Insiden Keamanan Informasi dan Keberlangsungan Bisnis	Pejabat Fungsional Sandiman	Suwarto, S.Sos Anggota: - Ervin Sandy Saputra S.Kom
9	Koordinator	Pejabat Pengadaan Dinas Komunikasi dan	I. Aji Indaryanto

	Keamanan Pemasok dan Kepatuhan Hukum	Informatika	Nugroho, S.Si Anggota: - Tri Haryanta
10	Koordinator Keamanan Sumber Daya Manusia	Kepala Sub Bagian Umum dan Kepegawaian	Edi Sutanto, S.T Anggota: - Tri Budiyanto

Klaten, 13 Agustus 2026
Kepala Dinas Komunikasi dan Informatika Kabupaten Klaten



Aris Pramana, S.E., M.M
Pembina Tingkat I (IV-b)
NIP 197507182005011006

LAMPIRAN
KEPUTUSAN KEPALA DINAS
KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLATEN
NOMOR : 000.6/43/2026
TANGGAL : 13 Agustus 2026

SUSUNAN TIM *DATA PROTECTION OFFICER* BERBASIS ISO
27001:2022

No	Posisi Tim DPO	Nama
1.	<i>Data Protection Officer</i>	Heri Wismo Handono, S.E., M.M.
2.	Anggota	Firmansyah Abdul Rafi
3.	Anggota	Yasin Manganugrahana K S. Kom
4.	Anggota	Herlan Sumarwanto S.T

Klaten, 13 Agustus 2026
Kepala Dinas Komunikasi dan
Informatika Kabupaten Klaten



Aris Pramana, S.E., M.M
Pembina Tingkat I (IV-b)
NIP 197507182005011006