PEMERINTAH KOTA PEKALONGAN
DINAS KOMUNIKASI DAN INFORMATIKA

KEBIJAKAN DAN PROSEDUR MANAJEMEN INSIDEN

Nomor Dokumen	SMKI/500.12.10/25/2025
Versi	2.0
Tanggal Berlaku Efektif	21 Oktober 2025
Klasifikasi	Internal
Pemilik Dokumen	Tim SMKI

Halaman Pengesahan

Disetujui Oleh:	**ARIF KARYADI S.Sos.** Kepala Dinas Komunikasi dan Informatika
Diketahui Oleh:	**TOTOK TRI HARIANTO, A.P.** Sekretaris Dinas Komunikasi dan Informatika
Diperiksa Oleh:	**Dr. KUSUMA ADI ACHMAD, S.E., S.Kom, M.T.** Kepala Bidang Aplikasi dan Persandian selaku CISO
Disusun Oleh:	**MEIDY PRASETYO UTOMO, S.Kom** Kepala Seksi Persandian dan Keamanan Informasi selaku Tim SMKI

Riwayat Perubahan Dokumen

Versi	Tanggal Revisi	Uraian Perubahan	Penyusun
1.0		Terbitan Awal	Tim SMKI
2.0	21 Oktober 2025	Perubahan prosedur	Tim SMKI

1. Sasaran

Prosedur manajemen insiden bertujuan untuk memastikan pendekatan konsisten dan efektif untuk manajemen insiden keamanan informasi, termasuk komunikasi tentang kejadian dan kelemahan keamanan.

2. Ruang Lingkup

Prosedur ini berlaku dalam ruang lingkup manajemen insiden keamanan informasi dalam proses bisnis di Dinas Komunikasi dan Informatika Kota Pekalongan.

3. Peran dan Tanggung Jawab

3.1. Koordinator Manajemen Insiden bertanggung jawab untuk mengkoordinasikan proses dan aktivitas yang dijabarkan dalam prosedur ini termasuk pemeliharaan dari catatan (records) hasil proses aktivitas tersebut.

3.2. Tim SMKI bertanggung jawab untuk pelaksanaan dari keseluruhan proses dan aktivitas yang dijabarkan dalam prosedur ini.

3.3. Manajemen Puncak bertanggung jawab penuh atas terlaksananya dari keseluruhan proses dan aktivitas yang dijabarkan dalam prosedur ini.

3.4. Pengendali Dokumen bertanggung jawab untuk proses proses peninjauan dan pemeliharaan dari prosedur ini.

4. Referensi

4.1. SNI ISO/IEC 27001:2022 Lampiran A 5.24 - Perencanaan dan Persiapan Manajemen Insiden Keamanan Informasi

4.2. SNI ISO/IEC 27001:2022 Lampiran A 5.25 - Penilaian dan Keputusan tentang peristiwa Keamanan Informasi

4.3. SNI ISO/IEC 27001:2022 Lampiran A 5.26 - Respon terhadap Insiden Keamanan Informasi

4.4. SNI ISO/IEC 27001:2022 Lampiran A 5.27 - Pembelajaran dari Insiden Keamanan Informasi

4.5. SNI ISO/IEC 27001:2022 Lampiran A 5.28 - Pengumpulan Bukti

4.6. SNI ISO/IEC 27001:2022 Lampiran A 6.8 Pelaporan peristiwa keamanan informasi

5. Dokumen Terkait

5.1. Form Pelaporan Insiden

5.2. Rekapitulasi Laporan Insiden

6. Kebijakan Umum

Prosedur manajemen insiden harus dilaksanakan dalam proses bisnis di Dinas Komunikasi dan Informatika Kota Pekalongan.

6.1. Peristiwa keamanan informasi adalah sebuah peristiwa yang mengindikasikan adanya kemungkinan pelanggaran keamanan informasi.

6.2. Ancaman adalah potensi penyebab insiden yang tidak diinginkan, yang dapat mengakibatkan bahaya pada sistem atau organisasi.

6.3. Kerentanan (*vulnerability*) adalah sebuah kelemahan pada aset atau kontrol yang dapat dieksploitasi oleh satu atau lebih ancaman.

6.4. Insiden keamanan informasi adalah satu atau beberapa peristiwa keamanan informasi terkait dan teridentifikasi yang dapat menimbulkan gangguan terhadap operasional dan membahayakan keamanan informasi.

6.5. Insiden keamanan informasi dibagi menjadi 2, yaitu insiden IT dan insiden Non-IT.

a. Insiden IT adalah semua insiden yang terkait dengan sistem informasi atau aplikasi yang dapat mengganggu proses bisnis. Contoh: insiden IT adalah kerusakan pada perangkat sistem informasi, jaringan tidak dapat diakses, error pada aplikasi serta kegagalan proses *backup* dan *restore*, hilangnya notebook/PC. Kemudian Insiden Kecerdasan IT adalah hilangnya/bocornya informasi perusahaan, *phishing, etc*.

b. Insiden non-IT adalah semua insiden yang tidak terkait dengan sistem informasi atau aplikasi namun berpotensi untuk menimbulkan gangguan terhadap keamanan informasi. Contoh insiden non-IT adalah kerusakan genset, akses kontrol pintu tidak berfungsi, pintu akses ke wilayah terbatas dalam keadaan terbuka saat tidak ada personel.

6.6. Kategori insiden:

a. *Low impact incident*: adalah insiden yang mempengaruhi user secara individu saja, contohnya user tidak dapat login/ data seorang user hilang. Kategori insiden ini harus diselesaikan dalam waktu maksimal 3 (hari) hari.

b. *Medium impact incident*: mempengaruhi beberapa user tetapi tidak mempengaruhi secara keseluruhan, contoh email tidak dapat diakses, beberapa data hilang, beberapa fitur tidak dapat diakses. Kategori insiden ini harus diselesaikan dalam waktu maksimal 2 (dua) hari.

c. *High impact incident*: mempengaruhi seluruh sistem, contoh gangguan server, gangguan network ke server, domain, dan lainnya. Kategori insiden ini harus diselesaikan dalam waktu maksimal 1 (satu) hari.

6.7. Tim IT yang bertanggung jawab atas manajemen insiden harus memiliki kesadaran dan pengetahuan yang cukup untuk mengidentifikasi kejadian, kelemahan dan insiden keamanan informasi.

6.8. Setiap kejadian, kerentanan dan insiden keamanan informasi harus terdokumentasi dan ditangani dengan memadai.

6.9. Pelaporan Insiden

6.9.1. Setiap kejadian, kerentanan dan insiden keamanan informasi harus dilaporkan secepat mungkin kepada koordinator manajemen insiden.

6.9.2. Koordinator manajemen insiden yang menerima pelaporan kejadian, kelemahan dan insiden keamanan informasi harus membuat catatan tertulis terkait laporan yang diterima.

6.10. Penanganan Insiden

6.10.1. Setiap kejadian, kerentanan dan insiden keamanan informasi harus dianalisis dan dievaluasi.

6.10.2. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalkan dampak dari insiden.

6.10.3. Setiap laporan akan menjadi bukti rekaman pelaporan internal yang harus dijaga dan dilindungi

6.11. Pembelajaran dari Insiden

6.11.1. Setiap proses penanganan setiap kejadian, kelemahan dan insiden keamanan informasi harus dianalisis untuk mencari penyebab utamanya. Proses ini mencakup pengumpulan dan analisis terhadap fakta terkait kejadian, kelemahan dan insiden keamanan informasi.

6.11.2. Proses analisis dan setiap tindakan korektif maupun peningkatan yang diambil harus didokumentasikan dengan baik.

7. Prosedur

No	Aktivitas	Dokumen	Bagian terkait	Koordinator Manajemen Insiden
1	Pelaporan insiden	Form Pelaporan Insiden	Mulai	
2	Pencatatan dan verifikasi awal terkait insiden yang dilaporkan	1. Form pelaporan insiden 2.Form rekap insiden		
3	Perencanaan tindak lanjut insiden	1. Form pelaporan insiden 2.Form rekap insiden		
4	Tindak lanjut insiden	1. Form pelaporan insiden 2.Form rekap insiden		
5	Menganalisis *root cause* dan menentukan tindakan korektif	Form rekap insiden		
6	Penanganan insiden dan pencatatan *lesson learned*	Form rekap insiden		Selesai