PEMERINTAH KABUPATEN KUTAI TIMUR

Dinas Komunikasi, Informatika, Statistik dan Persandian

Tim Tanggap Insiden Siber — KUTIM-CSIRT

PANDUAN TEKNIS

Pengamanan Website Perangkat Daerah

Acuan praktis bagi pengelola situs web di lingkungan Pemerintah Kabupaten Kutai Timur untuk mencegah, mendeteksi, dan menanggapi gangguan keamanan siber.

Nomor Dokumen	**KUTIM-CSIRT/PANDUAN/001/2026**
Versi	**1.0**
Klasifikasi	**TERBUKA — untuk umum**
Tanggal Terbit	**Mei 2026**
Disusun oleh	**Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT)**

KUTIM-CSIRT

csirt.kutaitimurkab.go.id · csirt@kutaitimurkab.go.id

Kata Pengantar

Penyelenggaraan pemerintahan berbasis elektronik menempatkan situs web Perangkat Daerah sebagai wajah resmi pelayanan publik sekaligus pintu masuk informasi bagi masyarakat. Seiring meningkatnya pemanfaatannya, situs web pemerintah juga menjadi sasaran gangguan keamanan siber — mulai dari perusakan tampilan, penyisipan konten yang tidak sah, hingga penanaman program berbahaya yang membahayakan data dan kepercayaan publik.

Pengalaman penanganan insiden di lingkungan Pemerintah Kabupaten Kutai Timur menunjukkan bahwa sebagian besar gangguan dapat dicegah melalui langkah pengamanan dasar yang diterapkan secara konsisten. Atas dasar itu, Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT) menyusun panduan ini sebagai acuan praktis bagi pengelola situs web di seluruh Perangkat Daerah.

Panduan ini sengaja disajikan ringkas dan langsung dapat diterapkan. Pengelola tidak perlu memiliki latar belakang keamanan siber yang mendalam untuk menjalankan langkah-langkah di dalamnya. Kami berharap dokumen ini menjadi rujukan bersama dalam membangun budaya keamanan informasi yang lebih baik di lingkungan Pemerintah Kabupaten Kutai Timur.

Kepada semua pihak yang telah memberikan masukan dalam penyusunan panduan ini, kami sampaikan penghargaan dan terima kasih. Saran perbaikan untuk edisi berikutnya dapat disampaikan melalui kanal resmi KUTIM-CSIRT.

Sangatta, Mei 2026

Tim Tanggap Insiden Siber
Kabupaten Kutai Timur

KUTIM-CSIRT

Daftar Isi

BAB 1

Pendahuluan

1.1 Latar Belakang

Situs web Perangkat Daerah merupakan sarana resmi penyampaian informasi dan pelayanan publik. Karena dapat diakses secara terbuka dari mana saja, situs web juga merupakan aset yang paling sering menjadi sasaran gangguan keamanan siber. Gangguan pada satu situs tidak hanya mengganggu layanan, tetapi juga dapat menurunkan kepercayaan masyarakat terhadap pemerintah daerah secara keseluruhan.

Penanganan insiden yang dilakukan KUTIM-CSIRT bersama Dinas Komunikasi, Informatika, Statistik dan Persandian menunjukkan pola yang berulang: situs yang terganggu umumnya menjalankan perangkat lunak yang tidak diperbarui, menggunakan akun dengan kata sandi lemah, atau tidak memiliki pemantauan sama sekali. Hampir seluruh kasus tersebut dapat dicegah dengan langkah pengamanan dasar yang diterapkan secara disiplin dan berkelanjutan.

1.2 Maksud dan Tujuan

Panduan ini disusun dengan maksud menyediakan acuan tunggal yang ringkas bagi pengelola situs web Perangkat Daerah dalam menjaga keamanan aset yang menjadi tanggung jawabnya. Tujuannya adalah:

- menyamakan pemahaman tentang ancaman yang umum dihadapi situs web pemerintah;
- menyediakan langkah pengamanan baku yang dapat segera diterapkan;
- menyediakan daftar periksa untuk menilai kesiapan keamanan secara mandiri;
- menjelaskan langkah yang harus diambil dan cara pelaporan apabila terjadi insiden.

1.3 Ruang Lingkup

Panduan ini mencakup pengamanan situs web Perangkat Daerah pada tingkat aplikasi dan konfigurasi dasar layanan, termasuk pengelolaan akun, pemutakhiran, pencadangan, serta penanganan awal insiden. Panduan ini tidak membahas pengamanan tingkat lanjut seperti pengerasan infrastruktur pusat data atau pengujian penetrasi, yang penanganannya dikoordinasikan langsung dengan KUTIM-CSIRT.

1.4 Sasaran Pengguna

Dokumen ini ditujukan bagi pengelola dan administrator situs web di lingkungan Perangkat Daerah Pemerintah Kabupaten Kutai Timur, baik pegawai yang ditugaskan secara khusus maupun penyedia jasa pengembang yang bekerja sama dengan Perangkat Daerah. Pimpinan Perangkat Daerah juga dapat menggunakan panduan ini untuk memastikan langkah pengamanan telah berjalan.

1.5 Dasar Acuan

- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
- Peraturan Badan Siber dan Sandi Negara mengenai penyelenggaraan keamanan siber dan pembentukan Tim Tanggap Insiden Siber pada instansi pemerintah;
- Keputusan Bupati Kutai Timur Nomor 555/K.557/2024 tentang Pembentukan Tim Tanggap Insiden Siber Kabupaten Kutai Timur.

BAB 2

Ancaman Umum terhadap Website Perangkat Daerah

Pengelola perlu mengenali bentuk gangguan yang paling sering terjadi agar dapat menempatkan langkah pengamanan secara tepat. Penjelasan berikut bersifat umum dan edukatif; rincian teknis yang dapat disalahgunakan sengaja tidak dicantumkan.

No	Bentuk Gangguan	Uraian Singkat dan Dampak
1	**Perusakan tampilan** (*defacement*)	Penggantian tampilan halaman situs oleh pihak tidak berwenang. Berdampak langsung pada citra instansi dan menandakan adanya akses tidak sah yang lebih dalam.
2	**Penyisipan konten judi daring** dan SEO parasit	Penyisipan halaman atau tautan promosi judi daring ke dalam situs resmi. Sering tidak terlihat pada tampilan utama, namun terindeks oleh mesin pencari sehingga merusak reputasi domain pemerintah.
3	**Webshell dan pintu belakang** (*backdoor*)	Penanaman program tersembunyi yang memberi penyerang akses berulang ke server. Memungkinkan gangguan terjadi kembali meskipun tampilan situs telah diperbaiki.
4	**Kebocoran data**	Pengambilan data dari situs atau basis datanya oleh pihak tidak berwenang, termasuk data pribadi masyarakat. Berisiko hukum dan merugikan pemilik data.
5	**Penyalahgunaan akun lemah**	Pengambilalihan akun pengelola karena kata sandi yang mudah ditebak, digunakan ulang, atau tidak pernah diganti. Merupakan jalan masuk paling umum bagi seluruh gangguan di atas.

> **CATATAN**
>
> Sebagian besar gangguan tidak berdiri sendiri. Akun lemah yang disalahgunakan dapat berujung pada penanaman *backdoor*, yang kemudian dipakai untuk penyisipan konten judi daring atau perusakan tampilan. Karena itu, langkah pengamanan pada Bab 3 perlu diterapkan secara menyeluruh, bukan sebagian.

BAB 3

Langkah Pengamanan

Bab ini memuat delapan langkah pengamanan dasar. Seluruh langkah sebaiknya diterapkan; bila sumber daya terbatas, dahulukan pemutakhiran perangkat lunak, penguatan akun, dan pencadangan.

3.1 Pemutakhiran dan Manajemen Tambalan

Perangkat lunak yang sudah usang adalah celah masuk yang paling sering dimanfaatkan. Pengelola perlu memastikan seluruh komponen situs selalu mutakhir.

- Perbarui sistem pengelolaan konten (CMS), tema, pustaka, dan pengaya secara berkala dan segera setelah pembaruan keamanan dirilis.
- Hapus tema, pengaya, atau modul yang tidak digunakan — komponen yang tidak aktif tetap dapat menjadi celah.
- Pastikan versi bahasa pemrograman dan layanan pendukung di server masih didukung resmi oleh pengembangnya.
- Catat seluruh komponen yang digunakan beserta versinya agar pembaruan mudah dipantau.

3.2 Autentikasi dan Pengelolaan Akun

Akun pengelola adalah kunci utama situs. Pengamanannya harus menjadi prioritas.

- Gunakan kata sandi yang panjang dan unik untuk setiap akun; hindari penggunaan ulang kata sandi pada layanan lain.
- Aktifkan autentikasi dua faktor apabila tersedia.
- Ganti seluruh kata sandi bawaan dari pengembang atau penyedia jasa sebelum situs dipublikasikan.
- Nonaktifkan akun yang tidak lagi digunakan, termasuk akun mantan pegawai atau penyedia jasa yang masa kerjanya berakhir.

3.3 Hak Akses dan Pemisahan Peran

Setiap pengguna sebaiknya hanya memiliki hak akses seminimal yang diperlukan untuk tugasnya.

- Berikan peran administrator hanya kepada pihak yang benar-benar membutuhkannya.
- Gunakan akun terpisah untuk tugas yang berbeda; hindari satu akun bersama yang dipakai banyak orang.
- Tinjau daftar pengguna dan hak aksesnya secara berkala, sekurang-kurangnya setiap tiga bulan.

3.4 Konfigurasi Server dan Aplikasi

- Nonaktifkan tampilan pesan kesalahan rinci kepada pengunjung; pesan tersebut dapat mengungkap informasi internal.
- Batasi akses ke halaman administrasi, sedapat mungkin hanya dari jaringan internal yang terpercaya.
- Tutup layanan dan porta jaringan yang tidak digunakan.
- Pastikan berkas konfigurasi yang memuat kata sandi tidak dapat diakses publik.

3.5 Pengamanan Pengunggahan Berkas

Fitur pengunggahan berkas yang tidak dibatasi merupakan jalan umum penanaman program berbahaya.

- Batasi jenis berkas yang boleh diunggah hanya pada yang benar-benar diperlukan, misalnya gambar atau dokumen.
- Simpan berkas unggahan pada lokasi yang tidak dapat dijalankan sebagai program oleh server.

- Ganti nama berkas unggahan secara otomatis dan batasi ukurannya.

3.6 Penerapan HTTPS dan Header Keamanan

- Pastikan situs diakses melalui HTTPS dan sertifikatnya selalu berlaku; perpanjang sebelum masa berlakunya habis.
- Arahkan seluruh akses HTTP polos ke HTTPS.
- Terapkan header keamanan dasar untuk mengurangi risiko penyalahgunaan tampilan dan konten situs.

3.7 Pencadangan Data

Pencadangan adalah jaring pengaman terakhir yang memungkinkan pemulihan cepat setelah insiden.

- Lakukan pencadangan berkas situs dan basis data secara berkala dan terjadwal.
- Simpan salinan cadangan pada lokasi terpisah dari server situs.
- Uji pemulihan dari cadangan secara berkala untuk memastikan cadangan benar-benar dapat digunakan.

3.8 Pemantauan dan Pencatatan Log

- Aktifkan pencatatan log akses dan aktivitas administrasi, serta simpan dalam jangka waktu yang memadai.
- Periksa situs secara berkala untuk memastikan tidak ada halaman atau konten yang tidak dikenali.
- Tindak lanjuti dengan segera setiap kejanggalan, seperti munculnya akun baru yang tidak dibuat oleh pengelola.

BAB 4

Daftar Periksa Pengamanan

Daftar periksa berikut digunakan untuk menilai kesiapan keamanan situs web secara mandiri. Pengelola memberi tanda pada kolom status untuk setiap butir yang telah dipenuhi, dan menjadikan butir yang belum terpenuhi sebagai prioritas perbaikan.

No	Butir Pengamanan	Sudah
A. PEMUTAKHIRAN		
1	CMS, tema, pengaya, dan pustaka berada pada versi terbaru.	☐
2	Komponen yang tidak digunakan telah dihapus.	☐
3	Versi bahasa pemrograman dan layanan server masih didukung resmi.	☐
B. AKUN DAN HAK AKSES		
4	Setiap akun memakai kata sandi panjang dan unik.	☐
5	Autentikasi dua faktor diaktifkan bila tersedia.	☐
6	Kata sandi bawaan telah diganti.	☐
7	Akun yang tidak aktif telah dinonaktifkan.	☐
8	Hak akses ditinjau berkala, minimal tiga bulan sekali.	☐
C. KONFIGURASI		
9	Pesan kesalahan rinci tidak ditampilkan kepada pengunjung.	☐
10	Akses ke halaman administrasi dibatasi.	☐
11	Pengunggahan berkas dibatasi jenis, lokasi, dan ukurannya.	☐
12	Situs diakses melalui HTTPS dengan sertifikat yang berlaku.	☐
D. PEMULIHAN DAN PEMANTAUAN		
13	Pencadangan berkas dan basis data berjalan terjadwal.	☐
14	Salinan cadangan disimpan terpisah dari server situs.	☐
15	Pemulihan dari cadangan pernah diuji.	☐
16	Pencatatan log aktif dan situs diperiksa berkala.	☐

BAB 5

Tanggap Insiden

Sebaik apa pun pengamanan diterapkan, insiden tetap mungkin terjadi. Yang menentukan besarnya dampak adalah kecepatan dan ketepatan penanganan awal.

5.1 Mengenali Tanda-tanda Insiden

Pengelola perlu waspada terhadap tanda-tanda berikut:

- tampilan halaman berubah tanpa dilakukan oleh pengelola;
- muncul halaman, tautan, atau berkas yang tidak dikenali;
- situs dialihkan ke alamat lain, atau hasil pencarian memuat konten yang tidak pantas;
- muncul akun pengelola baru yang tidak pernah dibuat;
- situs menjadi sangat lambat atau tidak dapat diakses tanpa sebab yang jelas.

5.2 Langkah Awal Penanganan

1. Tetap tenang dan jangan menghapus apa pun — jejak insiden diperlukan untuk penelusuran.
2. Catat waktu dan gejala yang ditemukan, serta ambil tangkapan layar sebagai bukti.
3. Ganti kata sandi akun pengelola dari perangkat lain yang terpercaya.
4. Bila memungkinkan, batasi akses publik ke situs untuk sementara guna mencegah dampak meluas.
5. Segera laporkan kepada KUTIM-CSIRT dan jangan menangani sendiri bila ragu.

> **PENTING**
>
> Memperbaiki tampilan situs tanpa menghilangkan penyebabnya akan membuat gangguan berulang. Penelusuran dan pembersihan menyeluruh sebaiknya dilakukan bersama KUTIM-CSIRT.

5.3 Pelaporan kepada KUTIM-CSIRT

KUTIM-CSIRT menerima pelaporan insiden dari seluruh Perangkat Daerah dan masyarakat. Saat melapor, sertakan informasi sejelas mungkin: nama dan alamat situs yang terdampak, waktu dan gejala yang ditemukan, serta bukti pendukung. Pelaporan dapat dilakukan melalui kanal berikut.

Kanal Pelaporan Insiden — KUTIM-CSIRT

Formulir daring	**csirt.kutaitimurkab.go.id/lapor**
Surel	**csirt@kutaitimurkab.go.id**
Telepon	**(0549) 2021207 — pada jam kerja**
Lacak laporan	**csirt.kutaitimurkab.go.id/lacak-tiket**

PENUTUP

Penutup

Keamanan situs web bukanlah pekerjaan sekali selesai, melainkan kebiasaan yang dijaga terus-menerus. Langkah-langkah dalam panduan ini sederhana, namun memberikan perlindungan yang nyata apabila diterapkan secara konsisten oleh setiap Perangkat Daerah.

KUTIM-CSIRT terbuka untuk membantu Perangkat Daerah dalam menerapkan panduan ini, baik melalui pendampingan, peninjauan kesiapan keamanan, maupun penanganan insiden. Panduan ini akan ditinjau secara berkala dan diperbarui sesuai perkembangan ancaman serta masukan dari para pengguna.

PERNYATAAN DOKUMEN

Dokumen ini diterbitkan oleh Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT) di bawah Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Kutai Timur. Dokumen berklasifikasi TERBUKA dan boleh disebarluaskan di lingkungan pemerintah maupun masyarakat untuk tujuan peningkatan keamanan siber.

— SELESAI —