PEMERINTAH PROVINSI KALIMANTAN UTARA
SEKRETARIAT DAERAH
Jalan Kolonel H.Soetadji Nomor 1 Tanjung Selor, Kode Pos 77212
Telp/Fax 0552-22454 Email : *kaltaraprov@gmail.com*
Website:*www.kaltaraprov.go.id*

Yth.

1. Asisten Sekretaris Daerah Provinsi Kalimantan Utara;
2. Staf Ahli Gubernur Kalimantan Utara;
3. Inspektur Daerah Provinsi Kalimantan Utara;
4. Sekretaris DPRD Provinsi Kalimantan Utara;
5. Kepala Badan/Biro/Dinas/Satuan di Lingkungan Pemerintah Provinsi Kalimantan Utara;
6. Direktur RSUD dr. H. Jusuf SK Provinsi Kalimantan Utara; dan
7. Pejabat Administrator, Pengawas, Fungsional, Pegawai ASN, dan PTT di Lingkungan Pemerintah Provinsi Kalimantan Utara

di Tempat

SURAT EDARAN
NOMOR 000.6/5377/DKISP/SETDA

TENTANG
PENINGKATAN KEWASPADAAN DAN BUDAYA KEAMANAN SIBER DI LINGKUNGAN PEMERINTAH PROVINSI KALIMANTAN UTARA

1. Latar Belakang

Kementerian Komunikasi dan Digital melalui Surat Nomor B-720/DJTPD.4/DT.01.10/11/2026 tanggal 9 November 2026 mengimbau seluruh instansi pemerintah meningkatkan kewaspadaan dan kesiapsiagaan keamanan siber. Imbauan tersebut menindaklanjuti *Security Advisory* Gov-CSIRT Indonesia, Badan Siber dan Sandi Negara (BSSN), tanggal 8 November 2026.

Pada tanggal 7 November 2026 beredar ancaman dari akun media sosial yang mengatasnamakan kelompok peretas untuk melumpuhkan situs pemerintah secara massal. Ancaman ini dikaitkan dengan penolakan terhadap penerapan pajak digital yang berlaku mulai 9 November 2026. Keaslian ancaman tersebut belum terverifikasi, namun berpotensi menimbulkan:

– gangguan layanan publik akibat serangan banjir lalu lintas (DDoS);
– perubahan tampilan situs (*defacement*);
– pencurian kata sandi melalui pesan atau surel palsu (*phishing*) bertema pajak digital; dan
– penyebaran hoaks yang meresahkan masyarakat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

Selain itu, terdapat sejumlah celah keamanan kritis pada perangkat lunak yang lazim digunakan situs pemerintah, yaitu PHP, kernel Linux, NGINX, dan Ghost CMS. Sebagian celah tersebut dilaporkan telah dimanfaatkan secara aktif oleh penyerang.

Keamanan siber tidak hanya bergantung pada perangkat teknologi. Banyak insiden berawal dari kebiasaan sehari-hari, seperti kata sandi yang lemah, tautan palsu yang diklik, atau informasi yang disebarkan tanpa verifikasi. Oleh karena itu, kewaspadaan seluruh pegawai sama pentingnya dengan pengamanan sistem.

2. Maksud dan Tujuan

Surat Edaran ini dimaksudkan sebagai imbauan dan bahan edukasi bagi Perangkat Daerah dan seluruh pegawai, dengan tujuan:

a. meningkatkan kewaspadaan terhadap ancaman siber yang sedang berkembang;
b. menumbuhkan kebiasaan kerja yang aman dalam menggunakan perangkat, akun, dan layanan digital kedinasan;
c. mempercepat pelaporan apabila ditemukan indikasi gangguan atau insiden siber; dan
d. menjaga keberlangsungan layanan publik dan kepercayaan masyarakat terhadap layanan digital Pemerintah Provinsi Kalimantan Utara.

3. Ruang Lingkup

Surat Edaran ini berlaku bagi seluruh Perangkat Daerah di lingkungan Pemerintah Provinsi Kalimantan Utara, termasuk UPTD, beserta seluruh pegawai PNS, PPPK, dan non-PNS yang menggunakan aset Teknologi Informasi dan Komunikasi (TIK) kedinasan.

4. Dasar

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024;
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
4. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber;
5. Peraturan Gubernur Kalimantan Utara Nomor 63 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi dan Pemerintah Kabupaten/Kota;
6. Peraturan Gubernur Kalimantan Utara Nomor 20 Tahun 2024 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;
7. Keputusan Gubernur Kalimantan Utara Nomor 100.3.3.1/603/2025 tentang Tim Tanggap Insiden Siber Provinsi Kalimantan Utara;

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

8. Surat Edaran Gubernur Kalimantan Utara Nomor 000.6/4385/DKISP.SET/IX/2026 tentang Pedoman Standar Keamanan SPBE di Lingkungan Pemerintah Provinsi Kalimantan Utara; dan
9. Surat Kementerian Komunikasi dan Digital Nomor B-720/DJTPD.4/DT.01.10/11/2026 tanggal 9 November 2026 perihal Imbauan Peningkatan Kewaspadaan dan Kesiapsiagaan Keamanan Siber kepada Pejabat Nama Domain Instansi Kementerian/Lembaga/Pemerintah Daerah.

5. Isi Edaran

Sehubungan dengan hal tersebut di atas, disampaikan imbauan sebagai berikut:

a. Kepada Kepala Perangkat Daerah dan Pengelola Sistem Elektronik

Kepala Perangkat Daerah diimbau memastikan pengelola situs web, aplikasi, dan sistem elektronik di unit kerjanya melaksanakan langkah-langkah berikut sesuai kewenangan masing-masing:

1) menyiagakan Agen Siber/Tim Tanggap Insiden Siber (TTIS) Perangkat Daerah serta menunjuk narahubung utama dan cadangan yang dapat dihubungi selama masa siaga;
2) mendata situs web, aplikasi, dan layanan yang dapat diakses dari internet, dengan mendahulukan layanan publik dan aplikasi yang paling penting;
3) mengaktifkan autentikasi dua langkah (*Multi-Factor Authentication*/MFA) pada akun administrator, serta mengganti kata sandi akun administrator, *hosting*, dan domain apabila kata sandi lemah atau diduga bocor;
4) menonaktifkan akun yang sudah tidak digunakan dan membatasi akses jarak jauh (SSH, RDP, panel administrator, dan VPN) hanya untuk pihak yang berwenang;
5) memeriksa dan memperbarui PHP, kernel Linux, *web server*, dan CMS yang digunakan, termasuk memastikan PHP telah diperbarui ke versi 8.5.12, 8.4.27, 8.3.36, atau 8.2.35. Apabila pembaruan belum dapat dilakukan, agar berkoordinasi dengan pengembang atau penyedia layanan untuk mitigasi sementara;
6) memeriksa tanda-tanda sistem telah disusupi, antara lain berkas atau halaman yang tidak dikenal, akun administrator baru tanpa izin, perubahan tampilan atau konfigurasi, dan aktivitas jaringan yang tidak wajar;
7) meningkatkan pemantauan catatan aktivitas (*log*) sistem dan memastikan salinan cadangan (*backup*) data dan aplikasi tersimpan terpisah serta dapat dipulihkan;
8) menonaktifkan subdomain, modul, layanan, dan *port* yang tidak digunakan; dan
9) berkoordinasi dengan Dinas Komunikasi, Informatika, Statistik dan Persandian (DKISP) Provinsi Kalimantan Utara untuk pemeriksaan kerentanan, perlindungan situs (WAF dan proteksi DDoS), serta pendampingan teknis.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

Sebelum memulihkan atau memasang ulang sistem yang terdampak, pengelola diimbau mengamankan bukti digital seperti *log*, berkas yang berubah, dan tangkapan layar, sepanjang tidak menghambat penanganan yang mendesak.

b. Kepada Seluruh Pegawai

Seluruh pegawai PNS, PPPK, dan non-PNS diimbau membiasakan langkah-langkah sederhana berikut dalam bekerja sehari-hari:

1) **Waspada pesan palsu bertema pajak.** Jangan membuka tautan atau lampiran mencurigakan yang mengatasnamakan Direktorat Jenderal Pajak atau membahas pajak digital. Pastikan kebenarannya melalui kanal resmi Direktorat Jenderal Pajak.
2) **Jaga kerahasiaan kata sandi dan kode OTP.** Jangan memberikan kata sandi maupun kode autentikasi kepada siapa pun, termasuk yang mengaku petugas, teknisi, atau atasan.
3) **Gunakan kata sandi yang kuat dan berbeda.** Kata sandi minimal 8 karakter, memadukan huruf besar, huruf kecil, angka, dan simbol, serta tidak dipakai ulang untuk akun lain.
4) **Aktifkan autentikasi dua langkah (MFA)** pada surel kedinasan, aplikasi kantor, dan akun media sosial instansi apabila fitur tersebut tersedia.
5) **Kunci perangkat saat ditinggalkan** dan pastikan sistem operasi, aplikasi, serta antivirus selalu diperbarui.
6) **Unduh aplikasi hanya dari sumber resmi** dan jangan menyimpan kata sandi kedinasan di peramban perangkat yang dipakai bersama.
7) **Saring sebelum berbagi.** Terapkan prinsip 4B (Baca, Berpikir, Baik, dan Bermanfaat) sebelum meneruskan informasi, terutama kabar tentang serangan siber atau situs pemerintah yang “diretas”.
8) **Lindungi data pribadi dan data kedinasan.** Jangan mengunggah atau membagikan dokumen yang memuat data pribadi masyarakat atau informasi yang dikecualikan melalui grup percakapan atau media sosial.
9) **Laporkan, jangan panik.** Apabila menerima pesan mencurigakan atau melihat situs instansi tidak dapat diakses atau berubah tampilan, segera laporkan sesuai angka 5 huruf c.

c. Pelaporan Indikasi Insiden Siber

Apabila ditemukan indikasi serangan, gangguan layanan, kebocoran data, atau pesan mencurigakan, Perangkat Daerah dan pegawai diimbau segera melapor kepada Tim Tanggap Insiden Siber Provinsi Kalimantan Utara (KaltaraProv-CSIRT) melalui:

1) Portal Layanan Persandian dan Keamanan Informasi: https://csirt.kaltaraprov.go.id;
2) Surel: diskominfo@kaltaraprov.go.id; atau
3) Narahubung: Sdr. Jeki Ansari, S.Kom. (0813-5004-2338).

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

Laporan cukup memuat waktu kejadian, alamat situs atau aplikasi yang terdampak, uraian singkat kejadian, dan tangkapan layar apabila ada. Pegawai tidak perlu mencoba menangani sendiri insiden yang terjadi; penanganan akan dikoordinasikan oleh KaltaraProv-CSIRT bersama Perangkat Daerah terkait.

6. Penutup

Kewaspadaan agar tetap dipertahankan sampai ada pemberitahuan lebih lanjut. Kepala Perangkat Daerah diharapkan meneruskan Surat Edaran ini kepada seluruh pegawai di lingkungan masing-masing dan menjadikannya bahan pembinaan budaya keamanan siber secara berkelanjutan.

Demikian Surat Edaran ini disampaikan untuk menjadi perhatian. Atas perhatian dan kerja sama Bapak/Ibu, diucapkan terima kasih.

Ditetapkan di Tanjung Selor
Pada, 16 November 2026

SEKRETARIS DAERAH
PROVINSI KALIMANTAN UTARA,

H. DENNY HARIANTO, S.E., M.M.
Pembina Utama Muda (IV/c)
NIP. 19780325 200212 1 009

Tembusan:
1. Gubernur Kalimantan Utara (sebagai laporan);
2. Wakil Gubernur Kalimantan Utara (sebagai laporan);
3. Direktur Jenderal Teknologi Pemerintah Digital, Kementerian Komunikasi dan Digital di Jakarta; dan
4. Direktur Keamanan Siber dan Sandi Pemerintah Daerah, Badan Siber dan Sandi Negara di Depok.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

LAMPIRAN
SURAT EDARAN SEKRETARIS DAERAH
PROVINSI KALIMANTAN UTARA
NOMOR : 000.6/5377/DKISP/SETDA
TANGGAL :16 November 2026

PANDUAN SINGKAT MENGENALI DAN MENGHADAPI ANCAMAN SIBER

Tabel berikut membantu pegawai mengenali situasi yang sering terjadi dan langkah yang perlu dilakukan.

No	Situasi	Tanda-tanda	Yang perlu dilakukan
1	Surel atau pesan palsu bertema pajak	Mengaku dari Direktorat Jenderal Pajak, meminta segera klik tautan, mengisi data, atau membayar; alamat pengirim atau tautan tidak resmi	Jangan klik atau membalas; periksa melalui kanal resmi Direktorat Jenderal Pajak; laporkan ke KaltaraProv-CSIRT
2	Permintaan kode OTP atau kata sandi	Mengaku atasan, rekan kerja, teknisi, atau petugas; mendesak dan meminta dirahasiakan	Jangan berikan; hubungi orang yang bersangkutan melalui nomor yang sudah dikenal; segera ganti kata sandi apabila telanjur diberikan
3	Lampiran berbahaya	Berkas berakhiran .apk, .exe, .scr, atau dokumen yang meminta mengaktifkan *macro*	Jangan dibuka atau dipasang; hapus pesan dan laporkan
4	Situs instansi berubah tampilan	Muncul gambar, tulisan, atau halaman asing di situs resmi	Jangan disebarkan; ambil tangkapan layar dan laporkan segera
5	Situs instansi tidak dapat diakses	Sangat lambat atau gagal dimuat dalam waktu lama	Laporkan waktu kejadian dan alamat situs kepada pengelola dan KaltaraProv-CSIRT
6	Kabar “situs pemerintah diretas”	Beredar di grup percakapan atau media sosial tanpa sumber resmi	Terapkan prinsip 4B; tunggu penjelasan resmi; jangan meneruskan
7	Perangkat terasa janggal	Muncul iklan atau aplikasi asing, akun keluar sendiri, perangkat sangat lambat	Putuskan dari jaringan, pindai dengan antivirus, ganti kata sandi dari perangkat lain, laporkan

SEKRETARIS DAERAH
PROVINSI KALIMANTAN UTARA

H. DENNY HARIANTO, S.E., M.M.
Pembina Utama Muda (IV/c)
NIP. 19780325 200212 1 009

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).