KEMENTERIAN PERTAHANAN RI
SEKRETARIAT JENDERAL

SURAT EDARAN
NOMOR: SE/ 35 /II/2026

TENTANG

KEWASPADAAN KEAMANAN SIBER

1. Dasar:

   a. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

   b. Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

   c. Peraturan Menteri Pertahanan Nomor 30 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Pertahanan.

   d. Keputusan Menteri Pertahanan Nomor: KEP/1826/XI/2025 tanggal 21 November 2025 tentang Tim Tanggap Insiden Siber di Lingkungan Kementerian Pertahanan.

   e. Surat Kepala Badan Siber dan Sandi Negara Nomor: T.4551/BSSN/D2/OS.01.04/12/2025 tanggal 29 Desember 2025 tentang Penyampaian Notifikasi Analisis Dugaan Kampanye Serangan Siber UNC1549 Menargetkan Sektor Pertahanan dan *Aerospace*.

2. Sehubungan dasar di atas, agar Kasatker/Kasubsatker di lingkungan Kementerian Pertahanan RI meningkatkan pengamanan data dan informasi dengan arahan sebagai berikut:

   a. Melaksanakan Pengelolaan Keamanan Komputer di antaranya:

      1) Wajib menggunakan Sistem Operasi yang asli.
      2) Menghapus aplikasi yang tidak berhubungan dengan pekerjaan.
      3) Memasang dan melakukan pembaruan *antivirus*.
      4) Hanya mengunduh dan memasang aplikasi dari sumber terpercaya.
      5) Pembaruan kata sandi secara berkala dan penyimpanan yang aman.

   b. Melaksanakan Pengelolaan Keamanan Server dan Sistem Elektronik di antaranya:

      1) Menunjuk *System Administrator* (*Sys Admin*) pengelola server dan sistem elektronik pada Satker masing-masing. *Sys Admin* merupakan organik Satker dan memahami kesadaran keamanan siber.
      2) Mendata server dan sistem elektronik yang digunakan masing-masing Satker dan melaporkan kepada Ka BIK Intelhan Kemhan untuk dilakukan pengujian keamanan sistem/*Information Technology Security Assessment* (ITSA). Pengujian keamanan sistem dilakukan secara berkala minimal 1 (satu) tahun sekali oleh Pussiber Inteltekhan BIK Intelhan Kemhan.

3) Dalam...

3) Dalam hal pembangunan, pengembangan, dan pemeliharaan server maupun sistem elektronik yang melibatkan pihak ketiga, wajib terlebih dahulu memperoleh izin dari Kapusdatin Kemhan serta persetujuan dari Sekjen Kemhan, dan pelaksanaannya tetap berada dalam pengawasan *Sys Admin* satker masing-masing
4) Setiap perubahan konfigurasi server dan sistem elektronik wajib dilaksanakan pengujian ulang keamanan sistem.
5) Menghapus akun-akun yang sudah tidak dipergunakan baik server dan komputer pengguna.
6) Melaksanakan penggantian kata sandi secara berkala (minimal 3 bulan sekali) dengan memperhatikan kaidah *secure password* yaitu:
   a) minimal 10 karakter
   b) kombinasi huruf besar dan kecil
   c) kombinasi angka
   d) mempergunakan simbol
   e) tidak menggunakan kata sandi yang mudah ditebak seperti tanggal lahir/identitas/informasi terkait pengguna.
7) Melaksanakan *update/patching operating system server* maupun PC pengguna.

c. Untuk yang sudah memiliki aplikasi internal Kemhan agar:
   1) Melakukan pencadangan data secara berkala dan menempatkan lokasi *file backup* berbeda dengan lokasi data asli atau sistem pencadangan terpusat di 1 (satu) komputer/server yang aman.
   2) Selain menggunakan *antivirus* yang sudah ada (Windows Defender), pengguna disarankan untuk menerapkan proteksi tambahan dengan menggunakan *antivirus* yang memiliki reputasi baik seperti Bitdefender, Kaspersky, Avast dan sebagainya.
   3) Apabila terdapat pembaruan fitur baru atau terindikasi adanya anomali pada aplikasi internal Kemhan agar mengajukan permintaan ITSA kepada Pussiber Inteltekhan BIK Intelhan Kemhan. Pengajuan ITSA dapat dilakukan melalui tautan s.id/itsa-kemhan.

d. Untuk pembangunan/pengembangan aplikasi internal/eksternal Kemhan yang baru agar:
   1) Menyiapkan sistem *Backup Data* di luar server utama (*Server Backup*).
   2) Menerapkan fitur *Multi-factor Authentication* (MFA)/*One Time Password* (OTP) sebagai fitur tambahan selain nama pengguna dan kata sandi dalam mengakses aplikasi.
   3) Membatasi waktu *session* aplikasi terbatas maksimal 1 (satu) hari.
   4) Mengimplementasikan parameter *cookie (secure* dan *HttpOnly)*.
   5) Menggunakan enkripsi pada basis data yang mengandung data kredensial terutama kata sandi dengan kombinasi algoritma enkripsi minimal SHA256 (*password plaintext+salt*).
   6) Wajib mengajukan permintaan ITSA kepada Pussiber Inteltekhan BIK Intelhan Kemhan sebelum aplikasi diluncurkan di internet. Pengajuan ITSA dapat dilakukan melalui tautan s.id/itsa-kemhan.

e. Melakukan pengelolaan keamanan personel di ranah siber dengan mensosialisasikan dan meningkatkan perilaku kesadaran keamanan siber kepada seluruh personel di masing-masing Satker.

f. Pussiber...

f. Pussiber Inteltekhan BIK Intelhan Kemhan agar melaksanakan ITSA di seluruh sistem elektronik yang dimiliki dan dioperasikan oleh Satker/Subsatker Kemhan.

g. Menekanan kepada seluruh pegawai Kemhan untuk mengantisipasi serangan *phising*, dengan cara sebagai berikut:

1) Memeriksa keaslian pengirim, tautan, dan lampiran *email* sebelum dibuka, terutama jika bersifat mendesak atau tidak biasa.
2) Tidak membagikan kata sandi, OTP, atau informasi sensitif kepada siapa pun, termasuk pihak yang mengaku sebagai tim IT.
3) Segera melaporkan *email* atau aktivitas mencurigakan kepada unit atau tim keamanan teknologi informasi.

3. Demikian untuk menjadikan perhatian.

Dikeluarkan di Jakarta
pada tanggal 23 Februari 2026

Sekretaris Jenderal,

KEMENTERIAN PERTAHANAN SEKRETARIS JENDERAL

Tri Budi Utomo
Letnan Jenderal TNI

Kepada Yth:

- Kasatker dan Kasubsatker
  di lingkungan Kemhan.

Tembusan:

1. Menhan RI
2. Wamenhan RI
3. Ka TTIS Kemhan.