PEMERINTAH DAERAH PROVINSI JAWA BARAT
SEKRETARIAT DAERAH
Jalan Diponegoro Nomor 22 Telepon : (022) 4232448 - 4233347 - 4230963
Faksimile: (022) 4203450 Website: www.jabarprov.go.id e-mail: info@jabarprov.go.id
Bandung 40115

Bandung, 13 Maret 2026

Kepada

Yth. Kepala Perangkat Daerah/Biro
di lingkungan Pemerintah
Daerah Provinsi Jawa Barat
di

T E M P A T

SURAT EDARAN
NOMOR: 45/KOM.03.05/DISKOMINFO

TENTANG
PENINGKATAN KEAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH DAERAH PROVINSI JAWA BARAT

Dalam rangka meningkatkan keamanan informasi di Lingkungan Pemerintah Daerah Provinsi Jawa Barat serta menindaklanjuti peningkatan intensitas insiden siber yang berpotensi mengganggu stabilitas operasional aspek ketersediaan, integritas, serta kerahasiaan data dan informasi pada Sistem Pemerintahan Berbasis Elektronik (SPBE), disampaikan langkah-langkah preventif dan mitigatif bagi setiap pegawai maupun pengelola sistem elektronik sebagai berikut:

A. Bagi seluruh pegawai di lingkungan Pemerintah Daerah Provinsi Jawa Barat

1. Menerapkan kebijakan syarat penggunaan kata sandi yang kuat dengan menggunakan minimal 12 karakter yang mengandung:
   a. 1 (satu) huruf kapital;
   b. 1 (satu) huruf nonkapital;
   c. 1 (satu) angka;
   d. 1 (satu) karakter spesial.
2. Menghindari penggunaan *password* yang mudah ditebak, seperti tanggal lahir, nama keluarga, atau informasi pribadi lainnya;
3. Memastikan penggunaan *password* yang berbeda untuk setiap akun;
4. *Username* dan *password* tidak disimpan secara otomatis pada *browser;*
5. Melakukan verifikasi dan memeriksa dengan cermat situs *(website)* yang akan dikunjungi;

6. Hindari mengklik tautan atau membuka lampiran *(file attachment)* yang berasal dari sumber yang tidak dikenal;
7. Tidak membagikan informasi *password/passphrase*/PIN/kode OTP/CVV kepada pihak manapun;
8. Tidak mengunggah atau menyebarkan data dan informasi sensitif di media sosial;
9. Meningkatkan kewaspadaan terhadap serangan *phishing* atau penipuan daring, seperti menerima panggilan, pesan WhatsApp dari nomor tidak dikenal, atau tautan mencurigakan melalui email dan media sosial;
10. Hindari menggunakan VPN gratis dan jaringan WiFi publik ketika mengakses layanan perbankan, transaksi keuangan, maupun aktivitas yang berkaitan dengan data dan informasi sensitif;
11. Mengunduh dan menginstal aplikasi hanya dari sumber resmi seperti Google Play Store atau Apple App Store;
12. Hanya memberikan izin akses aplikasi *(permissions)* sesuai kebutuhan;
13. Mengaktifkan dan memperbarui antivirus/*antimalware* secara berkala;
14. Melakukan pembaruan perangkat lunak pada *smartphone*/tablet/PC/Laptop secara berkala;
15. Tidak melakukan *login* akun penting dari perangkat milik orang lain;
16. Mengaktifkan fitur penguncian otomatis pada *smartphone*/*tablet*/PC/Laptop dengan *password* yang kuat;
17. Menghapus seluruh data pribadi dari perangkat *smartphone/tablet/*PC/*Laptop* sebelum dijual atau dipindahtangankan;
18. Menghindari penggunaan perangkat lunak bajakan yang berpotensi mengandung *malware* atau *virus*;
19. Melakukan pencadangan (*backup*) data secara berkala serta memastikan data cadangan disimpan secara aman dan dienkripsi;
20. Segera melaporkan setiap dugaan insiden siber kepada Agen Penanganan Insiden Siber Perangkat Daerah/Tim Pengelola Teknologi Informasi Perangkat Daerah atau pihak yang berwenang di lingkungan Pemerintah Daerah Provinsi Jawa Barat.

B. Bagi pengelola Sistem Elektronik di seluruh Perangkat Daerah

1. Memastikan perangkat lunak antivirus*/antimalware* pada perangkat yang digunakan oleh Administrator selalu aktif dan diperbarui secara berkala;
2. Melakukan pemutakhiran *(update/patching)* pada sistem operasi, perangkat lunak utilitas, serta perangkat lunak pendukung seperti API, *library,* dan komponen *middleware* yang digunakan secara berkala;

3. Memastikan akses *remote*/VPN ke *server* dengan menerapkan mekanisme kontrol akses yang kuat yang disediakan oleh Dinas Komunikasi dan Informatika;
4. Memastikan bahwa pihak ketiga hanya diberikan hak akses sesuai dengan kebutuhan tugasnya *(principle of least privilege);*
5. Mengimplementasikan Layanan Kriptografi Sandidata untuk pengamanan basis data yang mengandung data sensitif;
6. Melakukan pencadangan (*backup*) data penting secara berkala, disimpan terpisah dari sistem utama, dan memastikan data cadangan terenkripsi.

Demikian agar dipedomani serta diinformasikan kepada seluruh Pegawai untuk dilaksanakan sebagaimana mestinya.

SEKRETARIS DAERAH PROVINSI JAWA BARAT,

Ditandatangani secara elektronik oleh:
SEKRETARIS DAERAH PROVINSI JAWA BARAT,

Dr. Drs. HERMAN SURYATMAN, M.Si.
Pembina Utama

Tembusan:
1. Yth. Gubernur Jawa Barat;
2. Yth. Wakil Gubernur Jawa Barat.