



BUPATI BULELENG

Singaraja, 14 Nopember 2024

Kepada,

- Yth. 1. Para Pimpinan Organisasi
Perangkat Daerah Lingkup
Pemerintah Kabupaten
Buleleng
2. Sekretaris DPRD Kab.
Buleleng
3. Direktur Rumah Sakit
Umum Daerah Kabupaten
Buleleng
4. Para Kepala Bagian
Sekretariat Daerah
Kabupaten Buleleng
5. Para Camat Se-Kabupaten.
Buleleng
6. Perbekel dan Lurah Se-
Kabupaten Buleleng
7. Seluruh Pemilik Sertifikat
Elektronik Instansi di
Lingkup Pemkab. Buleleng
di –

Kabupaten Buleleng

SURAT EDARAN

Nomor : 100.3.4.2/3107/Kominfosanti/XI/2024

**TENTANG
PEDOMAN STANDAR KEAMANAN SIBER
DI LINGKUNGAN PEMERINTAH KABUPATEN BULELENG**

Berdasarkan ketentuan Pasal 17 ayat (1) Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, setiap instansi Pusat dan Pemerintah Daerah harus menerapkan keamanan Sistem Pemerintahan Berbasis Elektronik dan berdasarkan Peraturan Bupati Nomor 20 Tahun 2019 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi, untuk mewajibkan seluruh Perangkat Daerah dan jajaran pegawai baik PNS, PPPK maupun non PNS di Pemerintah Kabupaten Buleleng mengikuti pedoman standar keamanan siber sebagai berikut:

1. Setiap Perangkat Daerah dan jajaran pegawai baik PNS, PPPK maupun non PNS mengamankan secara fisik seluruh aset Teknologi Informasi Komunikasi yang menggunakan layanan organisasi;
2. Setiap Perangkat Daerah **diwajibkan** menggunakan Sertifikat Elektronik, dengan Tanda Tangan Elektronik dalam transaksi dokumen di aset layanan organisasi yang bertransaksi secara elektronik;
3. Setiap Perangkat Daerah, untuk keamanan dan tanggung jawab dari keamanan siber, setiap Aset Layanan Organisasi yaitu Aplikasi, Akun Media Sosial, *Website*, *Personal Computer* (PC), Laptop, dan *Email*, agar memiliki admin/operator dengan surat keputusan penunjukkan oleh Kepala masing-masing Perangkat Daerah/instansi;
4. Setiap pegawai yang mengalami kehilangan aset Teknologi Informasi Komunikasi seperti laptop, *smartphone* atau lainnya yang pernah digunakan untuk mengakses aset layanan organisasi wajib segera melakukan penggantian *password* pada aset layanan organisasi tersebut;
5. Setiap pegawai yang menggunakan aset layanan organisasi melengkapi keamanan perangkatnya dengan mengaktifkan penguncian otomatis maksimal 5 menit setelah tidak aktif;
6. Setiap pegawai yang memegang aset layanan organisasi wajib menjaga keamanan aset dan informasi di dalamnya dan peruntukannya hanya untuk kebutuhan organisasi;
7. Setiap pegawai yang menggunakan layanan jaringan internet organisasi atau mengakses aplikasi aset organisasi wajib memastikan perangkat yang digunakan dilengkapi dengan antivirus yang selalu diperbaharui dan aktif;
8. Setiap pegawai yang menggunakan layanan aset organisasi selalu melakukan **pembaruan** sistem operasi pada perangkat lunak, agar selalu *patch* keamanannya terbaru.
9. Setiap pegawai/operator/admin menjaga keamanan akunnya pada seluruh aset layanan organisasi termasuk akun Media Sosial, dan jaringan internet organisasi dengan cara:
 - 7.1 Menerapkan kata sandi di setiap aset layanan perangkat organisasi yang kuat dengan kriteria:
 - a. minimal terdiri dari 8 (delapan) karakter;
 - b. mengandung huruf kapital dan huruf kecil;
 - c. minimal mengandung 1 (satu) karakter numerik/angka; dan
 - d. minimal mengandung 1 (satu) simbol/karakter khusus
(contoh karakter khusus : @#%!.*).(contoh : Tag4r123*#!)
 - 7.2 Menjaga kata sandi dengan cara:
 - a. tidak membagikan kata sandi kepada siapapun dengan alasan apapun termasuk kepada pihak penyedia layanan;
 - b. mengganti kata sandi secara berkala minimal setiap 3 (tiga) bulan sekali;

- c. tidak menuliskan kata sandi dan/atau menyimpan kata sandi secara fisik maupun non fisik (*online*) kecuali diamankan secara memadai;
 - d. tidak menggunakan kata sandi yang sama pada aset layanan organisasi yang berbeda;
 - e. tidak mengaktifkan fitur *login* otomatis dan/atau fitur simpan kata sandi di *browser* pada komputer/laptop yang digunakan oleh beberapa pegawai;
 - f. pastikan selalu *logout* setelah selesai menggunakan aset layanan organisasi pada komputer/laptop yang digunakan oleh beberapa pegawai; dan
 - g. selalu mengaktifkan fitur *Multi-Factor Authentication* atau aplikasi *Authenticator* jika aplikasi mendukung.
10. Setiap pegawai **dilarang** mengakses situs/konten negatif yang tidak mendukung kinerja pada aset layanan organisasi (seperti; pornografi, judi online, game online dan lainnya);
11. Setiap pegawai/operator/admin yang ditugaskan mengelola aset layanan organisasi dan pengelolaan teknisnya berada di Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng (baik aplikasi, website, dan domain), jika terjadi insiden siber segera melaporkan kepada Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng.
12. Setiap pegawai **wajib** menjaga keamanan siber dari potensi *phishing* dan/atau *malware* dengan cara:
- a. **tidak asal mengklik link** atau tautan dari pesan masuk pada *electronic mail (e-mail)* dan/atau media sosial (*WhatsApp*) yang mencurigakan (seperti : file berbentuk .APK, dan tautan yang bersumber dari *e-mail bukan government (.go.id)* dan lainnya);
 - b. tidak mengunduh aplikasi ilegal/bajakan atau dari sumber yang tidak dikenal/dipercaya, berpotensi *malware*;
 - c. tidak mengklik dan/atau mengunduh *attachment* di *e-mail* dari sumber yang tidak dikenal dan/atau mencurigakan, **bukan** dari *e-mail government (.go.id)*;
 - d. tidak mengklik dan/atau mengunduh *file* melalui *link* yang disertakan pada *website* dan/atau media sosial yang mencurigakan;
 - e. hanya melakukan login pada situs yang menggunakan jalur komunikasi aman (*https*); dan
 - f. tidak mengaktifkan fitur *auto-run* pada *removable disk/flash drive/stik memory*.
13. Setiap pegawai **wajib** melakukan verifikasi 4B (baca, berpikir, baik, bermanfaat) pada setiap informasi sebelum melakukan sharing/berbagi;
14. Setiap pegawai mengetahui klasifikasi informasi terbuka dan dikecualikan/rahasia termasuk penanganannya sesuai Ketentuan Peraturan Perundang-undangan;

15. Setiap pegawai dilarang keras membocorkan data dan informasi sensitif milik organisasi;
16. Setiap pegawai mengikuti dan mengisi survei terkait kesadaran keamanan informasi;
17. Setiap pegawai ikut bertanggung jawab terhadap keamanan siber pada instansi/organisasinya dengan cara melaporkan segala bentuk insiden siber yang terjadi pada aset dan layanan organisasinya kepada Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng;
18. Pengaturan Ulang / *Reset* Kode Kredensial Aplikasi

Seluruh pegawai yang ditugaskan sebagai operator/admin sistem informasi dan aplikasi layanan aset organisasi (OPD/Kelurahan/Kantor Perbekel/Kantor BUMD) yang pengelolaan teknisnya dikelola oleh Dinas Komunikasi Informatika Persandian dan Statistik Kabupaten Buleleng, untuk **wajib** menjaga penuh kerahasiaan akses kredensialnya seperti : username dan password. Jika ingin melakukan pengaturan ulang atau *reset* kode kredensial tersebut, **wajib** melakukan permohonan melalui administrasi surat yang ditandatangani oleh Pimpinan OPD/Lurah/BUMD/Perbekel secara elektronik kepada Dinas Komunikasi Informatika Persandian dan Statistik Kabupaten Buleleng.

19. Pengaturan Ulang/*Reset* Sertifikat Elektronik

Seluruh pemilik Sertifikat Elektronik memiliki phassprase (Pimpinan OPD/Lurah/Perbekel/Direktur BUMD/Kepala Sekolah). Pemilik Sertifikat Elektronik **wajib menjaga** kerahasiaan phassprase tersebut dari bawahan maupun pemilik lain. Jika pemilik ingin melakukan Pengaturan Ulang/*Reset*, **wajib** mengajukan permohonan melalui administrasi surat yang ditandatangani oleh pemilik Sertifikat Elektronik dan atau Pimpinan Instansi tempat Pemilik Sertifikat Elektronik bertugas, kepada Dinas Komunikasi Informatika Persandian dan Statistik Kabupaten Buleleng.

20. Setiap pegawai yang menggunakan aset organisasi untuk menghindari *wifi* gratis/publik yang tidak dikenal penyedianya, apalagi mengakses informasi sensitif (membuka media sosial, aplikasi keuangan, dan lainnya).
21. Setiap pegawai yang menggunakan aset organisasi, pastikan hanya personil yang memang perlu dan berkepentingan untuk mengakses dalam suatu sistem informasi yang bersifat strategis.

Dengan terbitnya surat edaran ini, maka surat edaran dengan Nomor 000.1.10/693/Kominfosanti/III/2023 tidak berlaku lagi.

Demikian disampaikan, untuk mendapat perhatian dan dilaksanakan dengan penuh tanggung jawab.



Pj. Bupati Buleleng

Ketut Lihadnyana