PEMERINTAH KABUPATEN BULELENG
DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK
Jl. Pahlawan No. 1 Telp. 21146 – Fax.(0362) 21146
S I N G A R A J A
Website : ***http: www.bulelengkab.go.id***Email :***kominfosanti@bulelengkab.go.id***

Singaraja, 3 April 2023

Kepada :
Yth : Pimpinan OPD dan BUMD Lingkup
Pemerintahan Kabupaten Buleleng
di-
Singaraja

SURAT PENGANTAR

Nomor : 045.2/0265/santi.kominfosanti/IV/2023

No	Uraian	Banyaknya	Ket
1.	Disampaikan Surat Edaran tentang Pedoman Standar Keamanan Siber di Lingkungan Pemerintah Kabupaten Buleleng. Nomor : 000.1.10/693/Kominfosanti/III/2023	1 (satu) buah	Dikirim dengan Hormat untuk diterima, dapat dijadikan pedoman untuk menjaga ruang siber bersama. Terima Kasih

Ditandatangani secara elektronik oleh
Kepala Dinas Komunikasi,
Informatika, Persandian dan Statistik
Kabupaten Buleleng
Ketut Suwarmawan, SSTP., MM
Pembina Tk.I (IV/b)
NIP. 198107112001121002

Dokumen di tandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE, BSSN

BUPATI BULELENG

Singaraja, 20 Maret 2023

Kepada,

Yth. 1. Para Pimpinan Perangkat Daerah Lingkup Pemerintah Kabupaten Buleleng
2. Direktur Rumah Sakit Umum Daerah Kabupaten Buleleng
3. Para Kepala Bagian Sekretariat Daerah Kabupaten Buleleng
4. Para Camat Se-Kabupaten. Buleleng

di –

Kabupaten Buleleng

SURAT EDARAN
Nomor : 000.1.10/693/Kominfosanti/III/2023

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 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 *Webmail*, untuk memiliki admin/operator dengan surat keputusan penunjukkan oleh Kepala masing-masing Perangkat Daerah;

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 organisasi wajib memastikan perangkat yang digunakan dilengkapi dengan antivirus yang selalu diperbaharui dan aktif;

8. Setiap pegawai/operator/admin menjaga keamanan akunnya pada seluruh aset layanan organisasi 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.

9. Setiap pegawai dilarang mengakses situs/konten negatif dan/atau yang tidak mendukung kinerja organisasi;
10. Setiap pegawai wajib menjaga keamanan siber dari potensi *phishing* dan/atau *malware* dengan cara:
    a. tidak asal mengklik *link* dari *website*, *email* dan/atau media sosial yang mencurigakan;
    b. tidak mengunduh aplikasi ilegal/bajakan atau dari sumber yang tidak dikenal/dipercaya;
    c. tidak mengklik dan/atau mengunduh *attachment* di *email* dari sumber yang tidak dikenal dan/atau mencurigakan;
    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*.
11. Setiap pegawai wajib melakukan verifikasi 4B (baca, berpikir, baik, bermanfaat) pada setiap informasi sebelum melakukan sharing;
12. Setiap pegawai mengetahui klasifikasi informasi terbuka dan dikecualikan/rahasia termasuk penanganannya sesuai Ketentuan Peraturan Perundang-undangan;
13. Setiap pegawai dilarang keras membocorkan data dan informasi sensitif milik organisasi;
14. Setiap pegawai mengikuti survei terkait kesadaran keamanan informasi;
15. Setiap Perangkat Daerah yang ingin mengembangkan/membangun aplikasi dengan menggunakan jasa pihak ketiga diwajibkan memohon rekomendasi kepada Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng; dan
16. Setiap pegawai ikut bertanggung jawab terhadap keamanan siber pada instansi/organisasinya dengan cara melaporkan segala bentuk insiden siber kepada Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng.

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

Pjp Bupati Buleleng

Ketut Lihadnyana