PEMERINTAH KABUPATEN WONOSOBO
SEKRETARIAT DAERAH
Jalan Soekarno-Hatta Nomor 2-4 Wonosobo Jawa Tengah
56311 Telepon (0286) 321345 / Faksimile (0286) 321345
Laman: ppidsetda.wonosobokab.go.id, Pos-el:setda@wonosobokab.go.id

Yth. 1. Staf Ahli Bupati Wonosobo
2. Asisten Sekretaris Daerah Kabupaten Wonosobo
3. Kepala Perangkat Daerah Kabupaten Wonosobo
4. Direktur RSUD Setjonegoro Kabupaten Wonosobo
5. Kepala Bagian di Lingkungan Sekretariat Daerah Kabupaten Wonosobo

SURAT EDARAN

NOMOR : 500.12.10/1182 /Diskominfo

TENTANG

STANDAR PENGAMANAN PERANGKAT *ENDPOINT*

PADA PENGGUNA PERANGKAT TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUNGAN PEMERINTAH KABUPATEN WONOSOBO

I. Latar Belakang

Seiring perkembangan teknologi digital yang sangat pesat, Perangkat *Endpoint* seperti komputer, laptop, telepon genggam, dan perangkat sejenis telah menjadi komponen utama dalam pemanfaatan teknologi informasi dan komunikasi. Perangkat tersebut digunakan secara luas untuk mengakses data sensitif serta sumber daya penting organisasi, sehingga berpotensi menghadapi berbagai ancaman keamanan siber, antara lain serangan *malware, phishing, ransomware*, akses tidak sah, dan bentuk ancaman lainnya. Kondisi ini menegaskan bahwa pelindungan terhadap data dan informasi merupakan kebutuhan mendesak yang harus memperoleh perhatian serius.

Untuk menjawab tantangan tersebut sekaligus menjamin keamanan data dan informasi di lingkungan Pemerintah Kabupaten Wonosobo, diperlukan penerapan standar pengamanan Perangkat *Endpoint* yang terukur dan konsisten. Standar ini diharapkan mampu meningkatkan tingkat keamanan setiap perangkat, sehingga risiko kebocoran data dapat diminimalkan. Lebih jauh, penerapan standar pengamanan dimaksudkan untuk memastikan terjaganya kerahasiaan, keutuhan, ketersediaan, keotentikan, serta keteraksesan aset informasi strategis yang dimiliki Pemerintah Kabupaten Wonosobo.

II. Maksud dan Tujuan

a. Maksud

Surat Edaran ini sebagai acuan dalam pengelolaan dan penggunaan Perangkat *Endpoint* di lingkungan Pemerintah Kabupaten Wonosobo untuk melindungi serta menjaga kerahasiaan, keutuhan, ketersediaan, keotentikan, dan keteraksesan aset informasi.

b. Tujuan:

1. Mengurangi dan mencegah risiko kebocoran data dan informasi akibat serangan siber pada Perangkat *Endpoint* pada Perangkat Daerah.
2. Meningkatkan keamanan data dan informasi pada pengguna perangkat *endpoint* secara konsisten.
3. Meningkatkan kesadaran dan pemahaman mengenai pentingnya menjaga keamanan aset informasi seluruh pengguna Perangkat *Endpoint* di lingkungan Pemerintah Kabupaten Wonosobo.

III. Ruang Lingkup

Surat Edaran ini mengatur penerapan standar pengamanan Perangkat *Endpoint* yang digunakan oleh pengguna dalam aktivitas kedinasan di lingkungan Pemerintah Kabupaten Wonosobo.

IV. Definisi

1. Teknologi Informasi yang selanjutnya disingkat TI adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
2. Pengguna adalah setiap orang di lingkungan Pemerintah Kabupaten Wonosobo yang menggunakan perangkat TI dan terhubung ke jaringan TI Pemerintah Kabupaten Wonosobo.
3. Perangkat *Endpoint* adalah alat telekomunikasi, perangkat TI, atau sistem informasi yang terhubung pada suatu jaringan yang bertindak sebagai titik akhir (*endpoint)* di sisi pengguna seperti komputer, laptop/*notebook,* dan gawai/*mobile device*.
4. Barang Milik Daerah yang selanjutnya disingkat BMD adalah semua barang yang dibeli atau diperoleh atas beban Anggaran Pendapatan dan Belanja Daerah (APBD) atau berasal dari perolehan lainnya yang sah.
5. Bawa Perangkat Sendiri/*Bring Your Own Device* yang selanjutnya disingkat BYOD adalah kebijakan yang memungkinkan pengguna menggunakan Perangkat *Endpoint* pribadi untuk mengakses langsung sumber daya, aplikasi serta data dan informasi milik organisasi.
6. *Firewall* adalah sebuah sistem keamanan jaringan yang berfungsi untuk melindungi perangkat dari ancaman jaringan eksternal serta memantau dan mengendalikan lalu lintas jaringan, baik yang masuk maupun yang keluar, berdasarkan aturan keamanan yang ditetapkan.
7. Enkripsi adalah proses mengubah data atau informasi ke dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang tanpa kunci deskripsi yang sesuai.
8. *Internet of Things* yang selanjutnya disingkat IoT adalah perangkat fisik yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lain sehingga dapat saling terhubung dan bertukar data melalui internet.
9. Autentikasi biometrik adalah metode verifikasi identitas pengguna berdasarkan karakteristik fisik yang unik, seperti sidik jari, pengenalan wajah, iris mata, atau suara.
10. Forensik Digital adalah proses mengidentifikasi, memperoleh, memproses, menganalisis, dan melaporkan data yang disimpan secara elektronik dengan

cara yang dapat diterima secara hukum.

11. Tim Keamanan TI internal atau agen siber adalah kelompok kerja atau perorangan yang bertugas merencanakan, mengoordinasikan, memantau, serta melaksanakan pengamanan terhadap sistem, jaringan, data dan informasi di setiap Perangkat Daerah Kabupaten Wonosobo.
12. Tim Tanggap Insiden Siber (TTIS) atau *Computer Security Incident Response Team* (CSIRT). adalah kelompok kerja yang bertugas merencanakan, mengoordinasikan, memantau dan melaksanakan pengamanan pada sistem, pusat data dan Jaringan Intra Pemerintah (JIP) Kabupaten Wonosobo serta pengelolaan insiden siber.

V. Dasar Hukum

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
4. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
5. 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.
6. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.
7. Peraturan Bupati Wonosobo Nomor 37 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik dalam Penyelenggaraan Pemerintah Daerah Kabupaten Wonosobo.
8. Peraturan Bupati Wonosobo Nomor 38 Tahun 2022 tentang Sistem Manajemen Keamanan Informasi.
9. Keputusan Bupati Wonosobo Nomor : 046/392/2022 tanggal 30 November 2022 tentang Pembentukan Tim Tanggap Insiden Keamanan Siber Kabupaten Wonosobo.

VI. Isi Edaran

Sebagai upaya pengamanan data dan informasi dalam kerangka keamanan siber Pemerintah Kabupaten Wonosobo, dimohon perhatian Saudara agar menyampaikan kepada seluruh pengguna Perangkat *Endpoint* untuk mematuhi pengamanan *endpoint* yang digunakan untuk aktivitas kerja Perangkat Daerah dengan ketentuan sebagai berikut:

1. Standar Pengamanan Perangkat *Endpoint* Pengguna
    a. Ketentuan Umum
        1) Setiap Perangkat *Endpoint* yang digunakan di lingkungan Pemerintah Kabupaten Wonosobo harus memenuhi standar keamanan yang ditetapkan dalam Surat Edaran ini.

2) Setiap Perangkat *Endpoint* yang telah usang, ketinggalan zaman (*obsolete*) dan tidak lagi mendapatkan pembaruan sistem agar dihentikan penggunaannya serta beralih kepada penggunaan Perangkat *Endpoint* terbaru dengan memperhatikan skala prioritas kebutuhan.

3) Setiap Perangkat *Endpoint* harus menggunakan sistem operasi dan perangkat lunak yang berlisensi resmi dengan pembaruan otomatis (*auto-update*) yang diaktifkan.

4) Pengguna dilarang memasang atau menggunakan perangkat lunak bajakan/ilegal di Perangkat *Endpoint*.

5) Setiap pengguna harus mengaktifkan pengamanan kata sandi dan/atau biometrik pada Perangkat *Endpoint*.

6) Kata sandi wajib diubah secara berkala paling lama setiap 90 (sembilan puluh) hari kalender dan dilarang menggunakan kata sandi yang pernah dipakai sebelumnya.

7) Kerahasiaan kata sandi wajib dijaga oleh setiap pengguna dan satu akun dilarang digunakan secara bersama oleh lebih dari satu orang.

8) Kata sandi dilarang disimpan di peramban web atau desktop. Sebagai gantinya, gunakan password manager yang terpercaya untuk menyimpan kata sandi.

9) Setiap Perangkat *Endpoint* pada Perangkat Daerah wajib dicatat atau didaftarkan untuk manajemen akses informasi secara terkendali oleh setiap Perangkat Daerah.

b. Pengamanan Perangkat *Endpoint* berupa *personal computer* (pc), laptop, dan gawai

1) Data dan informasi sensitif pada setiap Perangkat *Endpoint* wajib dilindungi.

2) Setiap Perangkat *Endpoint* harus memiliki sistem operasi yang berlisensi resmi dan masih mendapatkan dukungan pembaruan dari penyedia resminya, misalnya Windows, Linux, macOS, dan lainnya.

3) Setiap Perangkat *Endpoint* harus menggunakan perangkat lunak yang berlisensi resmi untuk pengolahan dokumen, pengolahan data, pengolahan audio visual, *programming*, komunikasi dan perangkat lunak untuk kolaborasi kerja.

4) Setiap Perangkat *Endpoint* harus dilindungi oleh perangkat lunak keamanan, seperti *endpoint protection*, antivirus, *anti-malware*, dan sejenisnya.

5) Koneksi *bluetooth* dan *wi-fi* pada setiap Perangkat *Endpoint* wajib dinonaktifkan apabila tidak digunakan.

6) Port USB pada setiap Perangkat *Endpoint* wajib dinonaktifkan apabila tidak digunakan.

7) Pengguna hanya diperbolehkan memasang media penyimpanan portabel (*removable media*), seperti *flashdisk* dan perangkat penyimpanan eksternal, yang berasal dari sumber yang terpercaya pada Perangkat *Endpoint.*

8) Fitur pengunci layer otomatis (*auto screen lock*) pada setiap Perangkat *Endpoint* wajib diaktifkan dengan batas waktu paling lama 10 (sepuluh) menit setelah perangkat tidak digunakan.

9) *Firewall* pada setiap Perangkat *Endpoint* wajib diaktifkan dan dikonfigurasi dengan benar.

10) Hak akses pada Perangkat *Endpoint* hanya diberikan sesuai kebutuhan pelaksanaan tugas.

11) Serah terima atau pemindahtanganan Perangkat *Endpoint* berupa PC, laptop dan gawai kepada pengguna lain harus dilakukan pembersihan data sensitif terlebih dahulu agar sesuai dengan kewenangan akses data yang dimiliki pengguna *endpoint* baru.

12) Penghapusan data di setiap Perangkat *Endpoint* yang merupakan aset BMD agar dilakukan *back up* data terlebih dahulu melalui media penyimpanan terpisah serta dilakukan pembersihan data dan informasi secara total yang tersimpan dalam Perangkat *Endpoint* yang akan dilakukan penghapusan.

c. Pengamanan Perangkat IoT

Setiap perangkat *Internet of Things* (IoT) seperti CCTV, perangkat sensor, papan informasi digital dan jenis IoT lainnya, wajib :

1) Menggunakan *firmware* dan perangkat lunak terbaru (*up to date*);

2) Membatasi akses hanya kepada pengguna yang berwenang;

3) Mengganti kata sandi bawaan (*default password*) dengan kata sandi yang kuat;

4) Menggunakan mekanisme enkripsi pada komunikasi data;

5) Ditempatkan pada jaringan yang tersegmentasi dari jaringan utama; dan

6) Dilakukan pemantauan dan pencatatan aktivitas (*logging)* secara berkala.

2. Ketentuan Keamanan Tambahan pada *Perangkat Endpoint pribadi* /BYOD yang Digunakan untuk Aktivitas Kerja Kedinasan, sebagai berikut:

a. Setiap pengguna yang menggunakan Perangkat *Endpoint* pribadi/ BYOD untuk mengakses jaringan internal, data, informasi, atau sistem informasi Pemerintah Kabupaten Wonosobo, wajib mematuhi standar keamanan yang ditetapkan.

b. *Perangkat Endpoint pribadi*/BYOD yang digunakan untuk kepentingan kedinasan dapat dilakukan pemantauan keamanan secara terbatas oleh Tim Keamanan TI internal Perangkat Daerah, sepanjang berkaitan dengan upaya pelindungan jaringan, data, informasi, dan sistem informasi Pemerintah Kabupaten Wonosobo.

c. Dalam hal *Perangkat Endpoint pribadi*/BYOD terindikasi atau terlibat dalam insiden siber, Tim Keamanan TI internal atau agen siber Perangkat Daerah dapat melakukan pemeriksaan teknis dan/atau forensik digital sesuai kebutuhan penanganan insiden serta melaporkan kepada TTIS Kabupaten Wonosobo dengan tetap memperhatikan ketentuan peraturan perundang- undangan.

d. Akses Perangkat *Endpoint* pribadi terhadap jaringan internal, data,

informasi, atau sistem informasi Pemerintah Kabupaten Wonosobo dapat dibatasi, diblokir, atau diputus sementara apabila ditemukan pelanggaran terhadap standar keamanan yang telah ditetapkan.

e. Pengguna bertanggung jawab menjaga keamanan Perangkat *Endpoint* pribadi yang digunakan untuk kepentingan kedinasan, termasuk penggunaan kata sandi yang kuat, pembaruan sistem operasi dan aplikasi, serta pemasangan perangkat lunak keamanan yang memadai.

f. Perangkat Daerah, Unit Pelaksana Teknis Daerah/UPTD atau unit kerja lainnya melakukan pendataan pengguna *endpoint* yang berupa komputer milik pribadi pengguna/BYOD untuk aktivitas kerja kedinasan dan melakukan pemantauan dan pengawasan terhadap hak akses pengguna.

g. Jika pengguna Perangkat *Endpoint* pribadi /BYOD mengalami mutasi tempat kerja atau pemberhentian status pegawai agar data aktivitas kerja kedinasan termasuk data sensitif Perangkat Daerah yang tersimpan pada Perangkat *Endpoint* pribadi/BYOD, wajib diserahkan kepada Kepala Perangkat Daerah, Kepala UPTD atau Kepala Bagian disertai Berita Acara Serah Terima Data.

3. Tata Kelola dan Kepatuhan

   a. Setiap pengguna bertanggung jawab atas keamanan *Endpoint* yang digunakannya, termasuk menjaga kerahasiaan akses dan penggunaan sesuai dengan ketentuan yang berlaku.

   b. Perangkat *Endpoint* yang merupakan aset BMD dilarang digunakan untuk aktivitas yang tidak terkait dengan kepentingan kedinasan.

   c. TTIS Kabupaten Wonosobo berwenang melakukan pemantauan terhadap keamanan Perangkat *Endpoint* dalam rangka melindungi jaringan, data, dan sistem informasi Pemerintah Kabupaten Wonosobo.

   d. TTIS Kabupaten Wonosobo berwenang melakukan pemeriksaan teknis dan/atau forensik digital terhadap Perangkat *Endpoint* yang terindikasi atau terlibat dalam insiden siber sesuai dengan prosedur yang berlaku.

   e. Setiap Perangkat Daerah wajib menyediakan dukungan teknis terkait pengamanan Perangkat *Endpoint* bagi pengguna.

   f. TTIS Kabupaten Wonosobo bertugas menyusun, mengelola, dan melakukan evaluasi terhadap kebijakan keamanan informasi.

   g. TTIS Kabupaten Wonosobo bertugas melaksanakan sosialisasi, edukasi, dan peningkatan literasi keamanan informasi kepada pengguna secara berkala.

4. Tindakan dalam Keadaan Darurat Keamanan Siber, sebagai berikut :

   a. Setiap pengguna wajib segera melaporkan kepada Tim Tanggap Insiden Siber (TTIS)/*Computer Security Incident Response Team* (CSIRT) Kabupaten Wonosobo apabila terdapat aktivitas mencurigakan, dugaan ancaman siber, insiden siber, atau kehilangan Perangkat *Endpoint*.

   b. Aktivitas mencurigakan sebagaimana dimaksud pada huruf a meliputi, tetapi tidak terbatas pada:

      1) Akses tidak sah ke sistem atau akun;

2) Perangkat terinfeksi *malware* atau menunjukkan perilaku tidak normal;

3) Kebocoran atau dugaan kebocoran data;

4) Kehilangan atau pencurian Perangkat *Endpoint*; dan/atau

5) Gangguan layanan sistem informasi.

c. Setiap insiden siber yang yang terjadi pada Perangkat Daerah yang berdampak kepada terganggunya sistem dan layanan elektronik Perangkat Daerah wajib dilaporkan kepada TTIS Kabupaten Wonosobo melalui kanal aduan siber https://csirt.wonosobokab.go.id atau secara langsung kepada TTIS Kabupaten Wonosobo.

d. Pelaporan sebagaimana dimaksud pada huruf b dilakukan paling lambat 1 x 24 (satu kali dua puluh empat) jam sejak kejadian.

e. Dalam kondisi darurat, pengguna *endpoint* wajib:

1) Segera memutuskan koneksi perangkat dari jaringan;

2) Tidak melakukan perubahan atau penghapusan data yang berpotensi menjadi barang bukti; dan

3) Mengikuti arahan dari TTIS/CSIRT Kabupaten Wonosobo.

f. TTIS/CSIRT Kabupaten Wonosobo bertugas melakukan penanganan insiden, analisis, mitigasi, dan pemulihan layanan sesuai dengan prosedur yang berlaku.

5. Penutup

Surat Edaran ini agar dilaksanakan sebagaimana mestinya oleh seluruh pegawai pengguna *Perangkat Endpoint* di lingkungan Pemerintah Kabupaten Wonosobo.

Berkaitan dengan hal tersebut, maka dimohon:

1. Kepala Perangkat Daerah agar menindaklanjuti dan/atau meneruskan kepada Kepala Unit Pelaksana Teknis Daerah (UPTD) di bawah koordinasinya;
2. Kepala Dinas Kesehatan agar menindaklanjuti dan/atau meneruskan Surat Edaran ini kepada Kepala UPTD Laboratorium Kesehatan Daerah dan Kepala Puskesmas se-Kabupaten Wonosobo;
3. Camat agar menindaklanjuti dan/atau meneruskan Surat Edaran ini kepada Lurah di wilayah masing-masing.

Ditetapkan di Wonosobo pada
tanggal 2 Juni 2026
SEKRETARIS DAERAH
KABUPATEN WONOSOBO

ONE ANDANG WARDOYO