



BUKU PANDUAN KEAMANAN INFORMASI

Dinas Komunikasi dan Informatika
Agustus – 2025



KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa, karena dengan rahmat dan karunia-Nya, Buku Panduan Keamanan Informasi Pemerintah Kabupaten Purbalingga Tahun 2025 ini dapat disusun dan diselesaikan dengan baik.

Panduan ini merupakan bentuk komitmen Pemerintah Kabupaten Purbalingga dalam memperkuat keamanan informasi di era digital dan mendukung implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE). Penyusunan panduan ini juga didasarkan pada hasil Survei Keamanan Informasi ASN Tahun 2025 yang mengungkap berbagai tantangan dalam pengelolaan informasi, perangkat kerja, serta budaya kerja ASN yang aman.

Harapannya, buku panduan ini dapat digunakan sebagai acuan praktis oleh seluruh perangkat daerah, terutama dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi pemerintah. Diharapkan pula, penerapan panduan ini dapat meningkatkan kesadaran serta budaya keamanan informasi yang lebih baik dan berkelanjutan.

Akhir kata, kami menyampaikan terima kasih kepada seluruh pihak yang telah terlibat dalam penyusunan buku ini. Semoga buku ini memberikan manfaat dan dapat diterapkan secara konsisten di lingkungan Pemerintah Kabupaten Purbalingga.

Purbalingga, 8 Agustus 2025



Dokumen ini ditandatangani secara elektronik oleh :
Plt. Kepala Dinas Komunikasi dan Informatika

SADONO, S.Sos., M.Si
Pembina Utama Muda(IV/c)



Mengapa Keamanan Informasi Penting?

Keamanan Informasi adalah fondasi utama keberhasilan Sistem Pemerintahan Berbasis Elektronik (SPBE). Tanpa keamanan, integritas, kerahasiaan, dan ketersediaan data menjadi rentan.

Fakta dari Survei Penilaian Perilaku Keamanan Informasi ASN Pemerintah Kabupaten Purbalingga 2025 (1.172 ASN)

- ➡ 62% ASN masih menyimpan data dinas di perangkat pribadi
- 🔑 47% belum menggunakan autentikasi ganda
- 📁 35% pernah mengirim dokumen sensitif tanpa enkripsi
- 🔍 54% belum memahami SOP pengelolaan data SPBE

Risiko Jika Diabaikan:

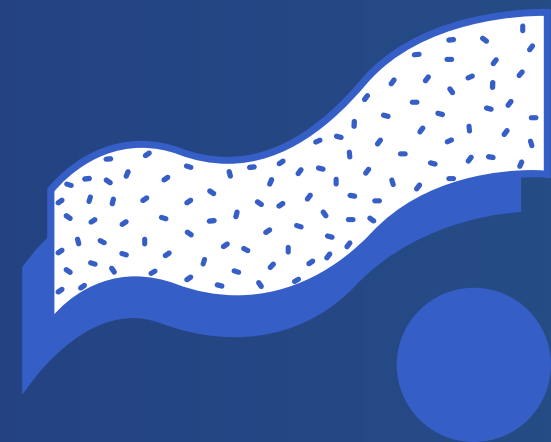
- 🚨 Kebocoran Data Publik
- 🚨 Manipulasi Informasi
- 🚨 Gangguan Layanan SPBE
- 🚨 Turunnya Kepercayaan Masyarakat

Kesimpulan:

- 💡 SPBE tanpa keamanan adalah ancaman tersembunyi.
- 🔒 Semua ASN wajib paham dan patuh terhadap prinsip keamanan informasi.

Dasar Hukum dan Kebijakan Keamanan Informasi

Landasan ASN dalam menjaga informasi publik



Regulasi Nasional

UU No. 27/2022 - Perlindungan Data Pribadi (hak, kewajiban, sanksi)

PP No. 71/2019 - Penyelenggaraan Sistem Elektronik (keamanan, audit, pemulihan)

Perpres No. 95/2018 - SPBE (tata kelola & keamanan digital pemerintah)

Landasan ASN dalam menjaga informasi publik

Perubahan atas Peraturan Bupati Purbalingga Nomor 90 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Bupati Nomor 31 Tahun 2023 tentang Sistem manajemen Keamanan Informasi di lingkungan Pemerintah Kabupaten Purbalingga

Wajib dipatuhi oleh seluruh ASN sebagai penjaga data publik



Perilaku Aman ASN dalam SPBE

Langkah sederhana, dampak besar untuk keamanan informasi publik

- ✓ Gunakan perangkat resmi/dinas saja
- ✓ Hindari Wi-Fi publik tanpa VPN
- ✓ Selalu logout setelah akses sistem
- ✓ Gunakan password berbeda untuk setiap akun

Kebocoran informasi sering terjadi karena kelalaian kecil.



Standar Operasional Prosedur (SOP)

Keamanan Informasi

Panduan Wajib Bagi ASN pengguna SPBE

SOP PELAPORAN INSIDEN KEAMANAN

- Identifikasi insiden (contoh: phishing, kebocoran data, akun dibajak);
- Laporkan segera ke Admin OPD/TIM Keamanan Informasi;
- Dokumentasikan kronologi, bukti, dan dampak;
- Tindak lanjuti bersama tim sesuai kategori insiden.

SOP PENGGUNAAN AKUN & BACKUP DATA

- Gunakan akun resmi (email, akses sistem dinas);
- Jaga kerahasiaan username & password;
- Backup rutin ke media resmi (server/cloud internal);
- Pantau akses dan ubah password secara berkala.

SOP PENGIRIMAN INFORMASI/ DOKUMEN DIGITAL

- Gunakan media resmi (Email dinas);
- Lindungi dokumen (beri password sebelum dikirim);
- Cek penerima (Pastikan alamat tujuan benar & berwenang);
- Simpan bukti kirim (Arsipkan log/email sebagai dokumentasi).



Perlindungan Data Pribadi dalam SPBE

Data pribadi adalah hak warga negara. ASN wajib menjaganya.

Prinsip Utama Perlindungan Data:

Data Minimization

Ambil dan simpan hanya data yang diperlukan untuk keperluan layanan publik.

Jangan mengumpulkan informasi berlebihan seperti NIK, nomor rekening, atau data keluarga jika tidak relevan.

Enkripsi Data

Semua data pribadi wajib disimpan dan dikirim dalam bentuk terenkripsi.

Gunakan aplikasi atau format yang aman: PDF dengan password, ZIP terenkripsi, atau sistem SPBE resmi.

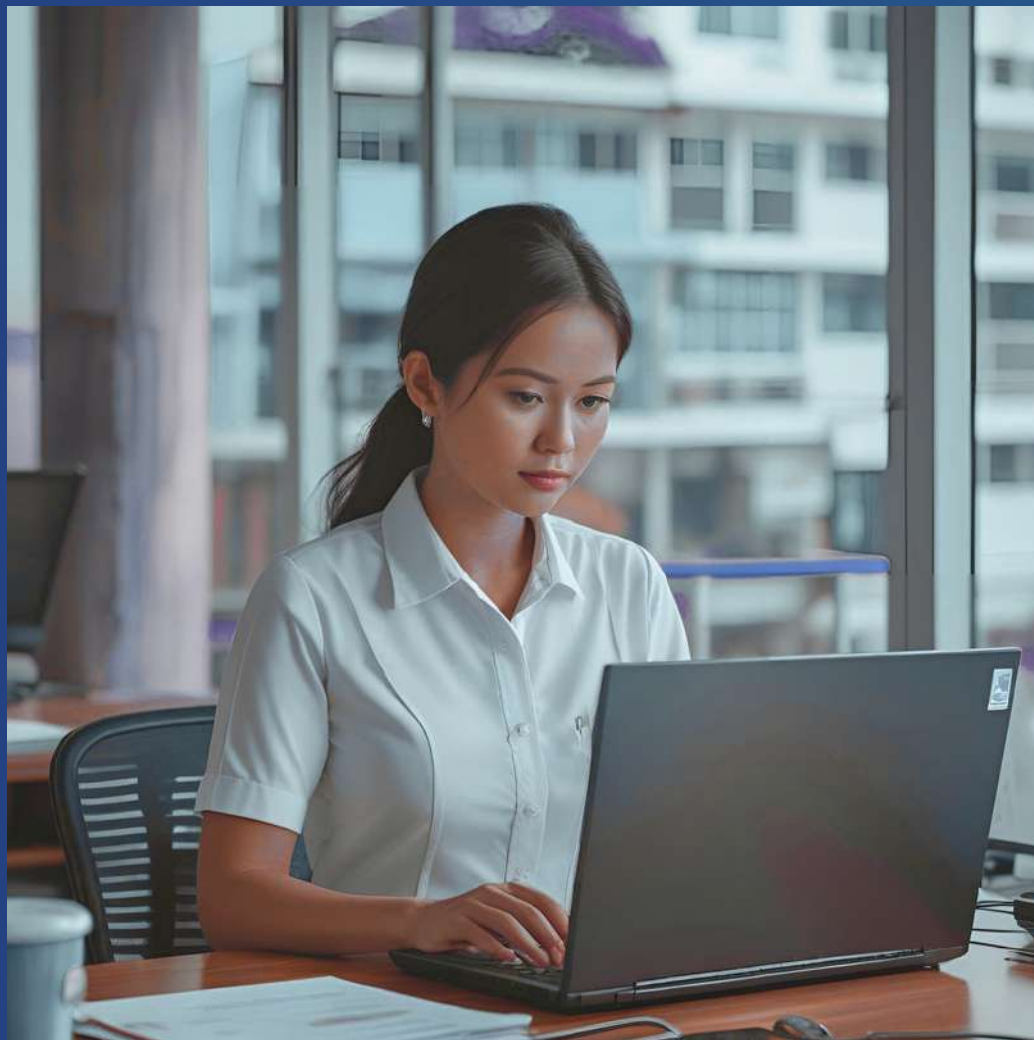
Tim Pengawas Data di OPD

Tiap OPD wajib memiliki penanggung jawab perlindungan data pribadi (bisa melekat pada Tim Keamanan Informasi/SMKI).

Bertugas mencegah kebocoran, menyusun SOP, dan menindak insiden keamanan data.

📌 Data pribadi = nama, NIK, alamat, biometrik, dsb. Harus dijaga dengan serius.

Perlindungan Data Itu Wajib, Bukan Pilihan



Setiap hari ASN mengakses dan mengelola data milik warga:

Nama, NIK, alamat, nomor HP, data medis, bahkan rekening bank.

Jika informasi ini jatuh ke tangan yang salah, bisa digunakan untuk:

- Penipuan identitas (identity theft)
- Peretasan akun pribadi
- Pemerasan, pencemaran nama baik, hingga penyalahgunaan layanan publik

Oleh karena itu, ASN wajib menjaga data pribadi seperti menjaga data diri sendiri.

- Jangan menyimpan data warga di HP pribadi.
- Jangan unggah dokumen data pribadi ke media sosial.
- Jangan kirim data ke pihak luar tanpa izin atau prosedur resmi.

Ingat Ini:

"Melanggar privasi warga = melanggar hukum."

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur sanksi tegas bagi individu atau instansi yang lalai atau menyalahgunakan data pribadi.

Panduan Sistem Elektronik yang Aman

Menjaga integritas, kerahasiaan, dan ketersediaan sistem SPBE

- 📊 Menjamin semua aktivitas tercatat dan bisa ditelusuri
- 🛡 Meningkatkan kepercayaan pengguna terhadap sistem digital pemerintah

1. Logging Aktivitas

- Sistem mencatat semua login, perubahan data, dan akses pengguna
- Log disimpan otomatis dan tidak boleh dihapus oleh pengguna biasa
- Admin wajib mengecek log secara berkala untuk mendeteksi aktivitas mencurigakan

3. Autentikasi Ganda (2FA)

- Aktifkan 2FA pada semua akun penting (admin/operator)
- Gunakan kombinasi password + OTP via email/sms/aplikasi Password harus unik – minimal 8 karakter, berisi huruf besar & kecil, angka, dan simbol khusus (@#\$%&*!). Mencegah akses ilegal meskipun password diketahui pihak lain.
- Ganti password secara berkala dan hindari penggunaan password yang sama di banyak akun

2. Backup Otomatis

- Sistem melakukan backup otomatis harian/mingguan ke server cadangan
- Backup disimpan di lokasi aman dan terenkripsi
- Lakukan uji pemulihan (restore test) secara berkala untuk memastikan data bisa dipulihkan

4. Akses Admin Tidak Dipakai Bersama

- Setiap admin wajib memiliki akun pribadi, tidak boleh berbagi akun
- Beri akses sesuai tugas, gunakan prinsip least privilege
- Nonaktifkan akun admin yang tidak aktif atau pindah tugas

Penerapan Keamanan Informasi di Lingkungan Kerja

Terapkan akses terbatas pada dokumen dan sistem sesuai tugas ASN

Jaga kerahasiaan informasi sensitif di ruang kerja terbuka

Hindari menyimpan data penting di flashdisk pribadi atau layanan cloud tanpa izin

Gunakan Tanda Peringatan di area terbatas (seperti ruang server atau ruang data)

Pastikan pengelolaan perangkat (laptop, printer, scanner) hanya oleh pegawai yang ditugaskan

Waspadaai rekayasa sosial (social engineering) yang memanfaatkan interaksi antarpegawai

Penerapan Keamanan Informasi di Lingkungan Kerja

Laptop & Komputer

1. Gunakan antivirus dan firewall aktif;
2. Aktifkan kunci layar otomatis (auto-lock 3–5 menit);
3. Hindari menyimpan data sensitif di desktop/lokal tanpa enkripsi;
4. Jangan pinjamkan perangkat kepada pihak tidak berwenang.

Laptop & Komputer

1. Aktifkan kunci layar (PIN, fingerprint, pattern);
2. Hindari instalasi aplikasi tidak resmi;
3. Pisahkan akun pribadi dan akun dinas.

Hard Disk & Flashdisk

1. Gunakan media penyimpanan terenkripsi;
2. Jangan digunakan bersama antar pegawai;
3. Lakukan scan virus sebelum & sesudah penggunaan;

Jaringan & Kelistrikan

1. Pastikan perangkat dihubungkan ke jaringan internal aman
2. Hindari meninggalkan kabel daya menyambung tanpa pengawasan
3. Letakkan kabel rapi untuk menghindari kerusakan atau kebakaran

Budaya Keamanan ASN

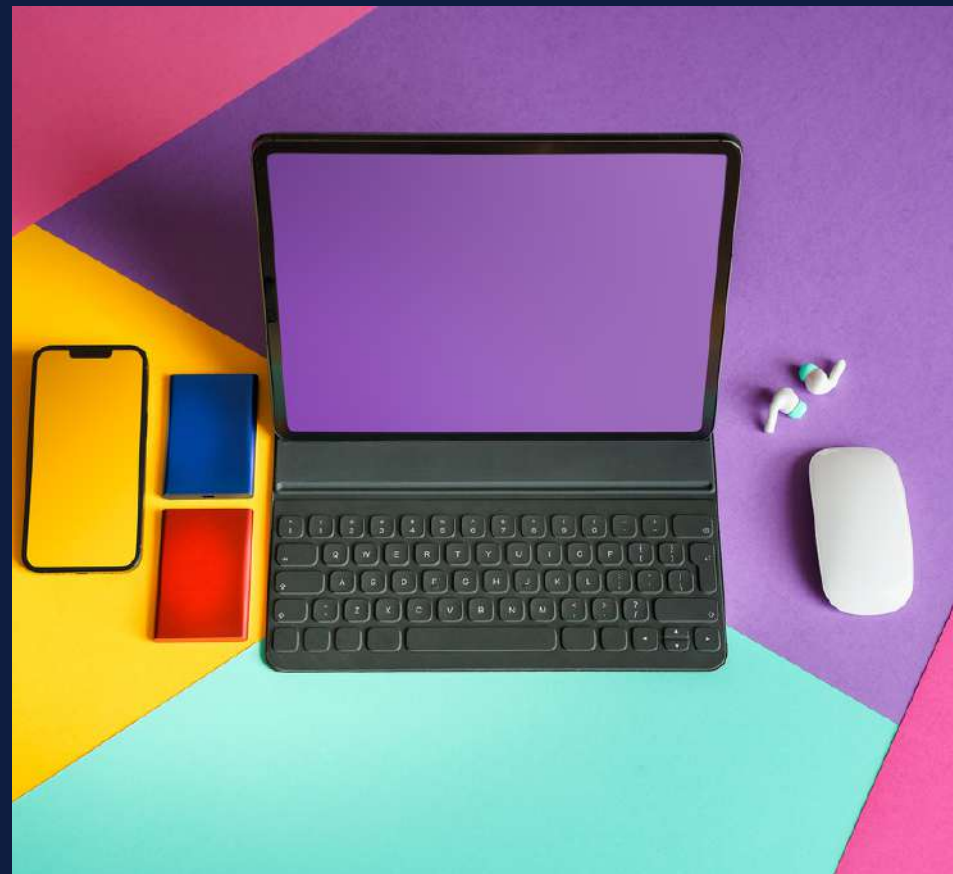
Kebiasaan Sehari-hari



Rapikan Ruang Kerja

- Jangan tinggalkan dokumen penting di meja;
- Simpan berkas fisik di laci terkunci;
- Tutup laptop saat tidak digunakan.

Lingkungan kerja yang rapi = informasi lebih aman



Hapus Data Sebelum Serah Terima Perangkat

- Reset HP/laptop dinas sebelum dipindahtangankan;
- Hapus akun, file, cache, dan histori browser;
- Pastikan tidak ada data pribadi/OPD tertinggal.

Serah terima perangkat = bukan serah terima data!

Budaya Keamanan ASN

Kolaborasi & Konsistensi

Kampanye Digital Keamanan Informasi (Tahunan)

- Kampanye bisa dimulai oleh siapa saja: perorangan, unit kerja, atau lintas OPD;
- Bentuknya bisa sederhana namun berdampak: poster digital, video pendek, kuis, simulasi insiden, hingga diskusi santai;
- Libatkan seluruh ASN, termasuk non-teknis, agar paham risiko dan cara pencegahannya.

✦ Keamanan informasi bukan tugas satu unit saja. Mari kita bentuk budaya peduli bersama, mulai dari lingkungan kerja terkecil.

Ciptakan Budaya Aman Digital di Lingkungan Perangkat Daerah

- Jadikan keamanan informasi bagian dari budaya kerja;
- Dorong rekan kerja untuk saling mengingatkan;
- Masukkan topik keamanan ke dalam forum OPD dan apel pagi.

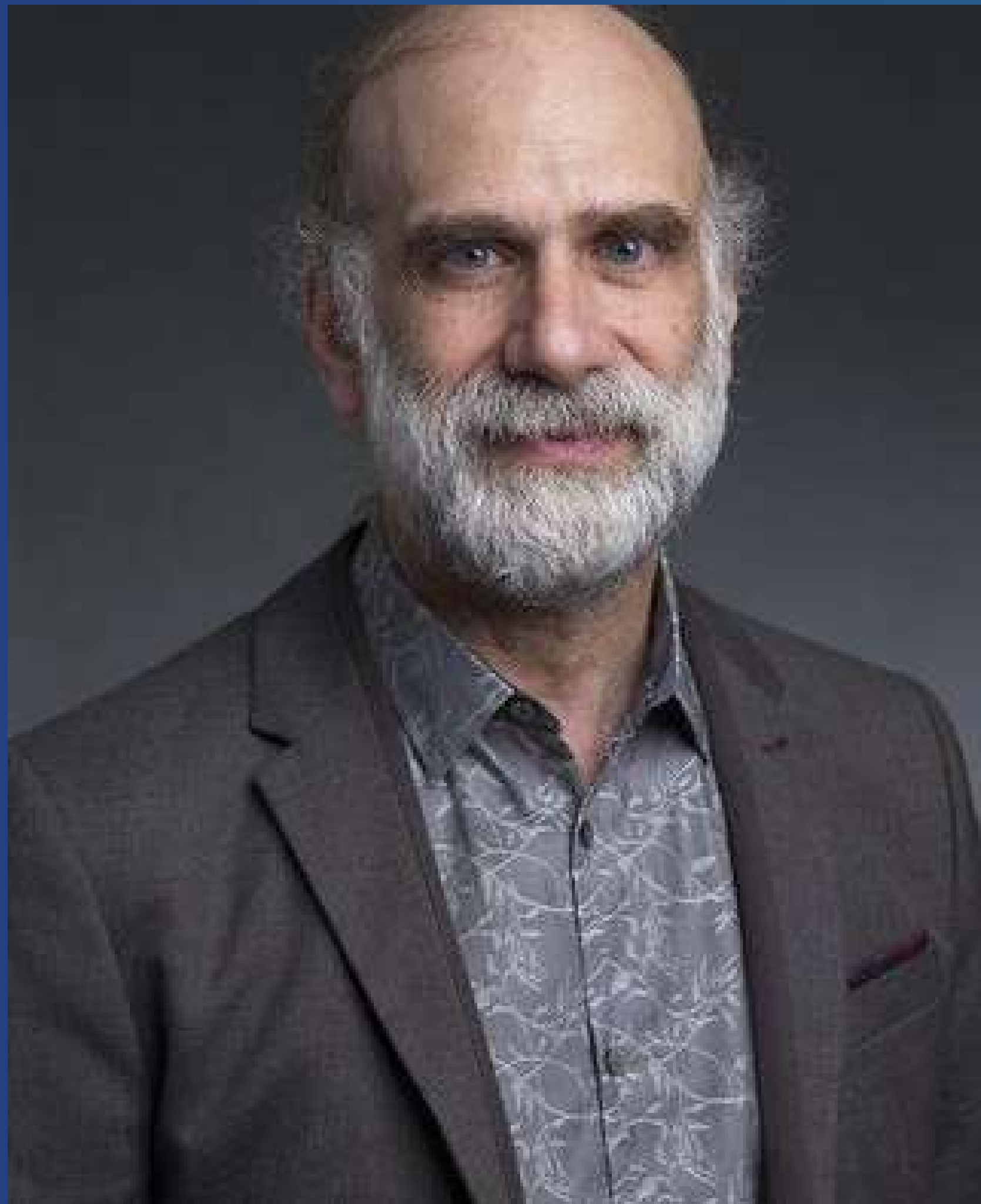
✦ Budaya terbentuk dari kebiasaan, bukan hanya aturan

Kolaborasi dan Konsistensi Keamanan Informasi

Keamanan informasi merupakan tanggung jawab bersama yang membutuhkan kolaborasi lintas perangkat daerah serta konsistensi dalam penerapan kebijakan. Koordinasi antar-OPD, peran aktif Tim Koordinasi SPBE, serta kedisiplinan dalam menjalankan Standar Operasional Prosedur (SOP) menjadi fondasi penting untuk menjaga sistem, data, dan informasi pemerintah secara aman dan berkelanjutan.

Panduan ini menjadi awal dari komitmen bersama dalam membangun budaya keamanan informasi di lingkungan Pemerintah Kabupaten Purbalingga. Setiap ASN diharapkan terus meningkatkan kesadaran, keterampilan, dan sikap tanggap terhadap risiko digital, serta secara aktif mengikuti pelatihan dan melaporkan insiden siber. Dengan kerja sama dan kesungguhan seluruh pihak, keamanan informasi akan menjadi pilar penting dalam mendukung tata kelola pemerintahan yang andal dan terpercaya.





Keamanan bukanlah produk, tetapi sebuah proses.

Bruce Schneier, pakar keamanan siber
dunia