Pemerintah
Kabupaten
Purbalingga

JAGA DATA, JAGA NEGERI

PANDUAN KEAMANAN INFORMASI UNTUK ASN DIGITAL

Dinas Komunikasi dan Informatika
September 2025

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, buku digital "Jaga Data, Jaga Negeri – Panduan Keamanan Informasi untuk ASN Digital" ini dapat disusun sebagai pedoman bagi Aparatur Sipil Negara di Kabupaten Purbalingga dalam menjaga keamanan informasi di era digital.

Panduan ini memuat langkah-langkah praktis perlindungan data, keamanan perangkat, pengelolaan kata sandi, hingga penanganan insiden siber, yang diharapkan mampu membentuk budaya kerja aman secara digital serta melindungi layanan publik dari ancaman keamanan informasi.

Semoga buku ini bermanfaat dalam memperkuat kesadaran dan kemampuan ASN untuk menjaga data demi terwujudnya pemerintahan yang bersih, efektif, dan terpercaya.

Purbalingga, 1 September 2025
Kepala Dinas Komunikasi dan Informatika
Kabupaten Purbalingga

PEMERINTAH KABUPATEN PURBALINGGA

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

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

Kenapa Keamanan Informasi itu Penting?

Keamanan informasi adalah upaya sistematis untuk melindungi informasi dari ancaman yang dapat merusak kerahasiaan, integritas, dan ketersediaannya. Perlindungan ini mencakup proses, kebijakan, dan teknologi untuk mencegah akses tidak sah, penyalahgunaan, modifikasi, atau penghancuran data, baik yang tersimpan maupun yang sedang diproses atau ditransmisikan.

Prinsip Keamanan Informasi

01 Kerahasiaan (Confidentiality) – Informasi hanya dapat diakses oleh pihak yang berwenang.

02 Integritas (Integrity) – Informasi harus akurat, utuh, dan tidak dimodifikasi secara tidak sah.

03 Ketersediaan (Availability) – Informasi dan sistem harus dapat diakses ketika dibutuhkan.

04 Aspek tambahan: otentikasi, non-repudiation, dan kontrol akses.

Dampak Kebocoran Data di Dunia Nyata

Kebocoran data dapat menimbulkan kerugian besar baik bagi individu, organisasi, maupun negara. Dampaknya tidak hanya berupa kerugian finansial, tetapi juga kerusakan reputasi, gangguan operasional, dan ancaman keamanan nasional.

1. **Kerugian finansial** – Penipuan, pencurian dana, atau kompensasi korban.
2. **Kehilangan kepercayaan publik** – Reputasi organisasi hancur.
3. **Eksposur informasi sensitif** – Data pribadi, rahasia bisnis, atau informasi strategis bocor.
4. **Gangguan operasional** – Layanan terganggu, proses bisnis terhenti.
5. **Ancaman keamanan nasional** – Data infrastruktur kritis atau strategi negara jatuh ke tangan pihak asing.

Contoh Kasus Siber di Indonesia dan Dunia

Kasus serangan siber terjadi di berbagai sektor dan negara. Beberapa insiden besar menunjukkan betapa pentingnya keamanan informasi dan kesiapan menghadapi ancaman digital.

Kasus di Indonesia

1. Pusat Data Nasional Lumpuh (Juni 2024): Ransomware menimpa 82 kementerian/lembaga; tebusan USD 8 juta diminta pelaku.
2. Bank Syariah Indonesia (2023): Serangan LockBit merusak server dan mencuri 1,5 TB data nasabah selama 5 hari.
3. Hacker Bjorka (2022): Mencuri data personal masif dari BI, PLN, Pertamina, dan lainnya.
4. BPJS Kesehatan (2021): Data 279 juta peserta bocor dan dijual di dark web.
5. BRI Life (2021): Data 2 juta nasabah, termasuk dokumen KTP dan rekening, bocor.
6. e-HAC & POLRI & Kejaksaan (2021): Bocoran data dari aplikasi kesehatan, POLRI, dan Kejagung; termasuk data pribadi jutaan warga.
7. Tokopedia (2020): Data 91 juta pengguna bocor, dijual di darknet

Kasus di Luar negeri

1. MOVEit Breach (2023): Kerentanan pada software transfer file yang dieksploitasi oleh grup CL0P, memengaruhi lebih dari 2.700 organisasi dan ~93 juta individu.
2. DaVita Breach (2025): Penyedia layanan dialisis asal AS terkena Interlock ransomware; 900.000 individu terdampak melalui pencurian data medis dan identitas.
3. MagentaTV Leak (2025): Basis data Elasticsearch tak terenkripsi menyebabkan kebocoran 324 juta catatan pengguna Deutsche Telekom.
4. Password Mega-Leak (2025): Terungkap 16 miliar kredensial login dari platform seperti Apple, Google, Facebook; mencerminkan ancaman besar terhadap keamanan digital global. ShinyHunters vs Google (2025): Google jadi korban serangan saat menyelidiki grup ShinyHunters. Data dari database Salesforce perusahaan bocor.
5. Israel–Iran Cyber Clash (2025): Serangan siber sebagai bentuk perpindahan konflik fisik. Melibatkan ribuan serangan lintas negara, membidik infrastruktur dan lembaga keuangan

Tiga Pilar Keamanan Informasi (CIA Triad)

Confidentiality (Kerahasiaan)

- **Makna**: Menjamin bahwa informasi hanya diketahui oleh pihak yang memiliki hak akses.
- **Fokus:** Melindungi data dari pihak tidak berwenang.
- **Cara menjaga:** Enkripsi, autentikasi, kontrol akses, dan kebijakan kerahasiaan.

Integrity (Integritas)

- **Makna:** Menjaga keakuratan, kelengkapan, dan konsistensi informasi dari perubahan yang tidak sah.
- **Fokus:** Memastikan data tetap benar dan utuh selama penyimpanan atau pengiriman.
- **Cara menjaga**: Kontrol versi, hash/checksum, tanda tangan digital, audit trai

---

Availability (Ketersediaan)

- **Makna**: Memastikan informasi dan sistem selalu tersedia bagi pihak yang berwenang saat dibutuhkan.
- **Fokus**: Meminimalkan downtime dan mencegah gangguan akses.
- **Cara menjaga:** Backup, redundansi server, pemeliharaan rutin, mitigasi DDoS.

Contoh Pilar Keamanan Informasi dilingkungan kerja

Confidentiality (Kerahasiaan)

- Menetapkan password pada dokumen internal.
- Menggunakan akses terbatas pada sistem (misalnya, hanya HR yang dapat melihat data gaji).
- Menyimpan dokumen fisik di lemari terkunci.
- Mengaktifkan enkripsi pada email berisi data sensitif.

Integrity (Integritas)

- Menggunakan versi kontrol dokumen untuk menghindari data lama tertimpa.
- Memberikan otorisasi edit hanya kepada pegawai tertentu.
- Menyimpan log perubahan (audit trail) pada aplikasi.
- Melakukan checksum atau verifikasi data setelah transfer file.

Availability (Ketersediaan)

- Menggunakan UPS (Uninterruptible Power Supply) agar server tetap hidup saat listrik padam.
- Menyediakan backup data secara rutin.
- Menggunakan server cadangan atau cloud service untuk layanan penting.
- Melakukan pemeliharaan sistem berkala agar tidak sering down.

Ancaman dan Serangan Siber yang Sering Terjadi

Phishing, Smishing, dan Vishing

- Phishing – Upaya menipu korban melalui email palsu atau situs tiruan untuk mencuri data seperti username, password, atau informasi kartu kredit.
  Contoh: Email yang menyerupai bank, meminta login ulang karena "akun diblokir".

- Smishing – Phishing melalui SMS atau pesan instan.
  Contoh: SMS mengatasnamakan kurir paket dengan tautan palsu.

- Vishing – Phishing lewat panggilan telepon (voice phishing).
  Contoh: Penipu berpura-pura sebagai petugas bank yang meminta OTP.

Malware, Ransomware, Spyware

- Malware – Perangkat lunak berbahaya yang merusak sistem, mencuri, atau memanipulasi data.
  Contoh: Trojan yang menyamar sebagai aplikasi resmi.

- Ransomware – Malware yang mengenkripsi data dan meminta tebusan untuk membukanya kembali.
  Contoh: Serangan ransomware PDN 2024 yang melumpuhkan layanan pemerintah.
- Spyware – Malware yang diam-diam memantau aktivitas pengguna dan mencuri informasi.
  Contoh: Keylogger yang merekam setiap ketikan pengguna.

Ancaman dan Serangan Siber yang Sering Terjadi

Social Engineering dan Rekayasa Psikologis

- Definisi: Teknik manipulasi manusia agar mau memberikan informasi sensitif atau melakukan tindakan tertentu tanpa sadar.

Contoh:

- Pelaku mengaku sebagai atasan yang meminta transfer dana mendesak.
- Menggunakan rasa takut (“akun Anda akan diblokir dalam 24 jam”) untuk memaksa korban bertindak cepat.

Insider Threat (Ancaman dari Orang Dalam)

- Definisi: Ancaman yang datang dari pegawai, kontraktor, atau pihak internal yang memiliki akses ke sistem atau data.

Tipe:

- Malicious insider – Sengaja membocorkan atau merusak data.
- Negligent insider – Lalai, misalnya mengklik tautan berbahaya atau membagikan password.

Contoh:

- Pegawai yang menjual data pelanggan kepada pihak luar.
- Staf yang menyimpan data rahasia di flashdisk pribadi tanpa enkripsi, lalu hilang.

Keamanan Perangkat & Jaringan

Keamanan perangkat dan jaringan adalah pondasi penting dalam melindungi informasi di era kerja digital. Laptop, smartphone, dan koneksi internet yang kita gunakan setiap hari bukan hanya alat bantu kerja, tetapi juga menjadi target empuk bagi pelaku kejahatan siber. Risiko bisa datang dari perangkat yang tidak terkunci, software yang tidak diperbarui, atau koneksi Wi-Fi publik yang tidak aman. Mengetahui potensi ancaman ini adalah langkah awal untuk melindungi diri dan organisasi dari serangan yang merugikan.

Tanpa perlindungan yang memadai, data sensitif dapat dengan mudah diakses, disadap, atau dicuri. Serangan siber bisa dilakukan dari jarak jauh melalui malware, phishing, atau pencurian fisik perangkat. Untuk itu, setiap pengguna perlu membiasakan diri menerapkan langkah-langkah pengamanan seperti penggunaan password yang kuat, pembaruan sistem secara berkala, instalasi patch keamanan, pemanfaatan VPN, dan enkripsi data. Langkah-langkah ini sederhana, namun sangat efektif untuk menutup celah serangan.

Mari disiplin menjaga keamanan perangkat dan jaringan sebagai bagian dari budaya kerja. Dengan kebiasaan yang baik, kita tidak hanya melindungi data pribadi, tetapi juga menjaga kelancaran operasional dan reputasi organisasi. Ingat, keamanan informasi bukan hanya tugas tim IT, tetapi tanggung jawab kita semua. Setiap tindakan kecil yang kita lakukan hari ini akan berkontribusi pada pertahanan besar organisasi di masa depan.

TIPS Keamanan Perangkat & Jaringan

Tips Keamanan Laptop & Smartphone
Tujuan: Melindungi perangkat kerja dari pencurian fisik, peretas

Langkah:

- Gunakan password kuat atau biometrik (sidik jari, face unlock).
- Aktifkan kunci layar otomatis jika perangkat tidak digunakan.
- Simpan perangkat di tempat aman saat tidak dipakai.
- Hindari menginstal aplikasi dari sumber tidak resmi.
- Aktifkan temukan perangkat saya untuk pelacakan jika hilang.

Update Software & Patch Keamanan
Tujuan: Menutup celah keamanan yang bisa dieksploitasi oleh peretas

Langkah:

- Selalu perbarui sistem operasi dan aplikasi ke versi terbaru.
- Aktifkan pembaruan otomatis jika memungkinkan.
- Gunakan perangkat lunak resmi dan berlisensi.
- Hapus aplikasi yang tidak digunakan untuk mengurangi potensi kerentanan.

Penggunaan Wi-Fi Publik dengan Aman
Risiko: Wi-Fi publik (kafe, bandara, hotel) sering menjadi target penyadapan atau serangan man-in-the-middle.

Langkah:

- Hindari mengakses layanan keuangan atau data sensitif di Wi-Fi publik tanpa perlindungan tambahan.
- Gunakan VPN untuk mengenkripsi lalu lintas data.
- Matikan fitur koneksi otomatis ke Wi-Fi.
- Gunakan hotspot pribadi saat melakukan pekerjaan penting.

VPN & Enkripsi Data
VPN (Virtual Private Network)

- Mengenkripsi koneksi internet, menyembunyikan IP, dan melindungi data saat menggunakan jaringan publik.
- Cocok digunakan saat bekerja dari luar kantor.

Enkripsi Data

- Pastikan file penting dienkripsi, baik saat disimpan (at rest) maupun saat dikirim (in transit).
- Gunakan format enkripsi bawaan sistem (BitLocker di Windows, FileVault di Mac, atau fitur enkripsi di Android/iOS).

Keamanan Password & Otentikasi

Password merupakan garis pertahanan pertama untuk melindungi akses ke berbagai sistem dan data penting. Namun, banyak pengguna masih menggunakan password yang mudah ditebak atau sama untuk banyak akun, sehingga berisiko tinggi diretas. Oleh karena itu, penting untuk membuat password yang kuat—menggabungkan huruf besar dan kecil, angka, serta simbol—dan memastikan panjangnya cukup agar sulit dipecahkan oleh alat peretas otomatis.

Selain itu, penggunaan password manager sangat membantu dalam mengelola berbagai password yang berbeda tanpa harus mengingat semuanya secara manual. Password manager menyimpan password secara aman dan terenkripsi, sehingga memudahkan pengguna untuk menggunakan password unik di setiap layanan tanpa risiko lupa.

Untuk meningkatkan keamanan lebih jauh, penerapan Multi-Factor Authentication (MFA) sangat dianjurkan. MFA menambahkan lapisan verifikasi tambahan di luar password, misalnya kode OTP dari aplikasi autentikator atau biometrik seperti sidik jari. Dengan MFA, meskipun password bocor, pelaku tidak bisa masuk tanpa melewati proses verifikasi tambahan. Oleh sebab itu, disiplin menggunakan password kuat, password manager, dan MFA adalah langkah penting dalam menjaga keamanan akun dan data pribadi kita.

Tips Keamanan Password & Otentikasi

Cara Membuat Password Kuat

Fungsi : Mencegah pihak tidak berwenang menebak atau membobol akun.

Langkah:

- Minimal 12 karakter (semakin panjang, semakin sulit dibobol).
- Kombinasi huruf besar, huruf kecil, angka, dan simbol.
- Hindari kata-kata umum, tanggal lahir, atau pola mudah ditebak.
- Gunakan frasa acak yang mudah diingat tapi sulit ditebak.
- Contoh: L@mpuHijau_2025!

Password Manager

Fungsi : Menyimpan dan mengelola semua password dalam bentuk terenkripsi, sehingga pengguna hanya perlu mengingat satu master password.

Manfaat:

- Mengurangi risiko lupa password.
- Memungkinkan penggunaan password unik di setiap akun.
- Sinkronisasi di berbagai perangkat secara aman.
- Contoh layanan: Bitwarden, LastPass, 1Password, KeePass.

Multi-Factor Authentication (MFA)

Definisi: Metode otentikasi yang menggunakan lebih dari satu lapisan verifikasi.

Jenis faktor keamanan:

1. Sesuatu yang Anda tahu – password atau PIN.
2. Sesuatu yang Anda punya – token fisik, kode OTP dari aplikasi/authenticator.
3. Sesuatu yang melekat pada Anda – biometrik seperti sidik jari atau pengenalan wajah.
4. Manfaat:

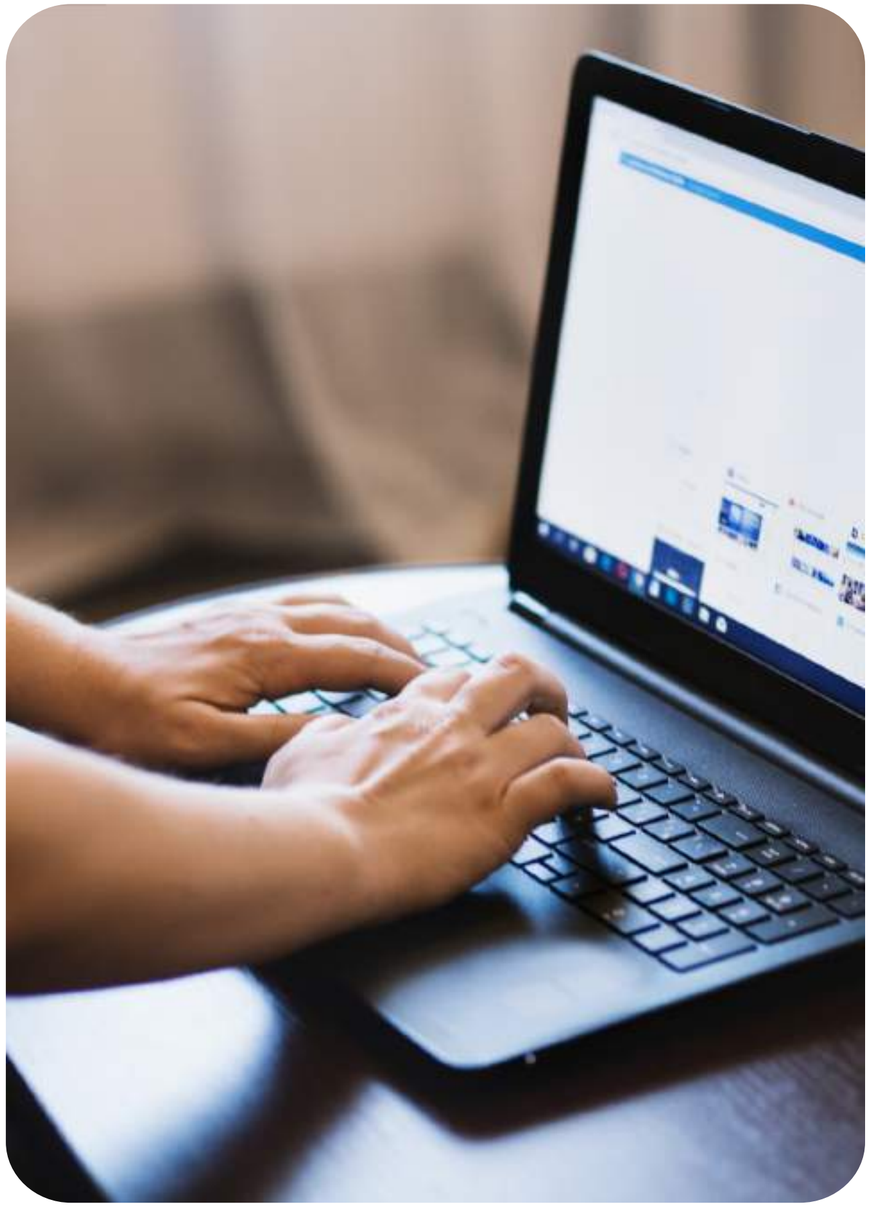
- Jika password bocor, akun tetap aman karena pelaku memerlukan faktor tambahan.
- Contoh penerapan: Login email kantor dengan password + OTP dari aplikasi Google Authenticator.

Perlindungan Data Pribadi

Data pribadi yang harus dilindungi

Regulasi & UU Perlindungan Data Pribadi di Indonesia

Praktik pengamanan data di instansi

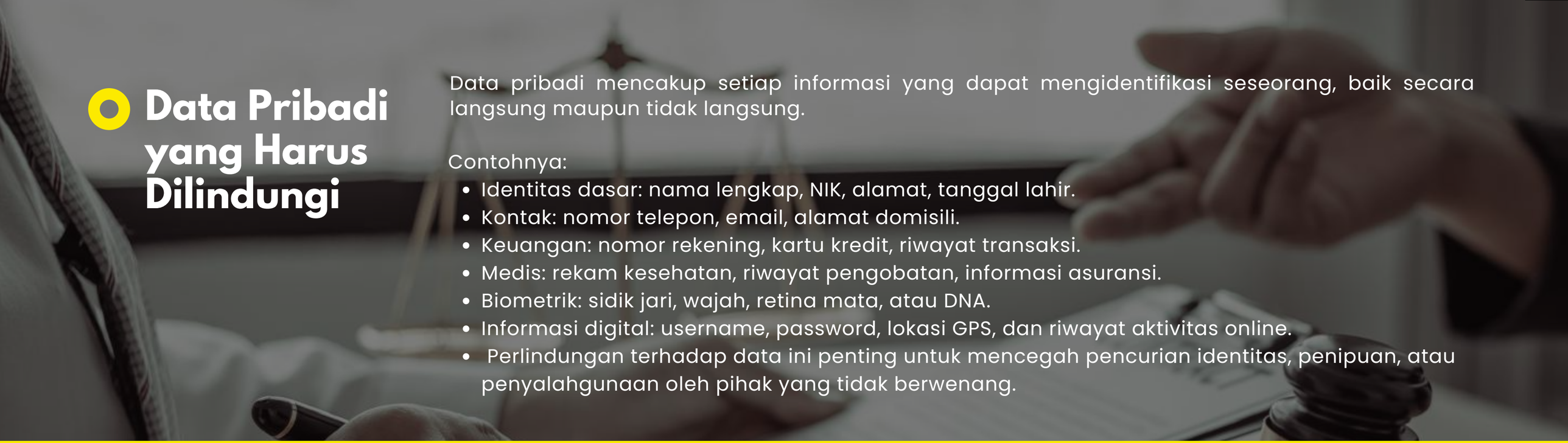


Perlindungan Data Pribadi

Data pribadi adalah informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun tidak langsung, seperti nama, alamat, nomor identitas, nomor telepon, alamat email, rekam medis, hingga informasi biometrik. Data-data ini memiliki nilai tinggi dan sering menjadi target pihak tidak bertanggung jawab untuk tujuan penipuan, pencurian identitas, atau penyalahgunaan lainnya.

Di Indonesia, perlindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur hak subjek data, kewajiban pengendali data, serta sanksi administratif dan pidana bagi pelanggar. UU ini menekankan bahwa setiap pengelolaan data pribadi harus dilakukan secara sah, transparan, aman, dan sesuai dengan tujuan pengumpulannya.

Di lingkungan instansi pemerintah maupun organisasi, praktik perlindungan data pribadi mencakup pengendalian akses terhadap data, penggunaan enkripsi saat penyimpanan dan pengiriman, penerapan kebijakan kerahasiaan bagi pegawai, serta audit berkala untuk memastikan kepatuhan. Pegawai wajib memahami jenis data pribadi yang dikelola, prosedur penanganannya, dan tanggung jawab hukum jika terjadi kebocoran. Dengan disiplin dan kesadaran semua pihak, perlindungan data pribadi dapat terjaga sehingga kepercayaan publik tetap terpelihara.



Data Pribadi yang Harus Dilindungi

Data pribadi mencakup setiap informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun tidak langsung.

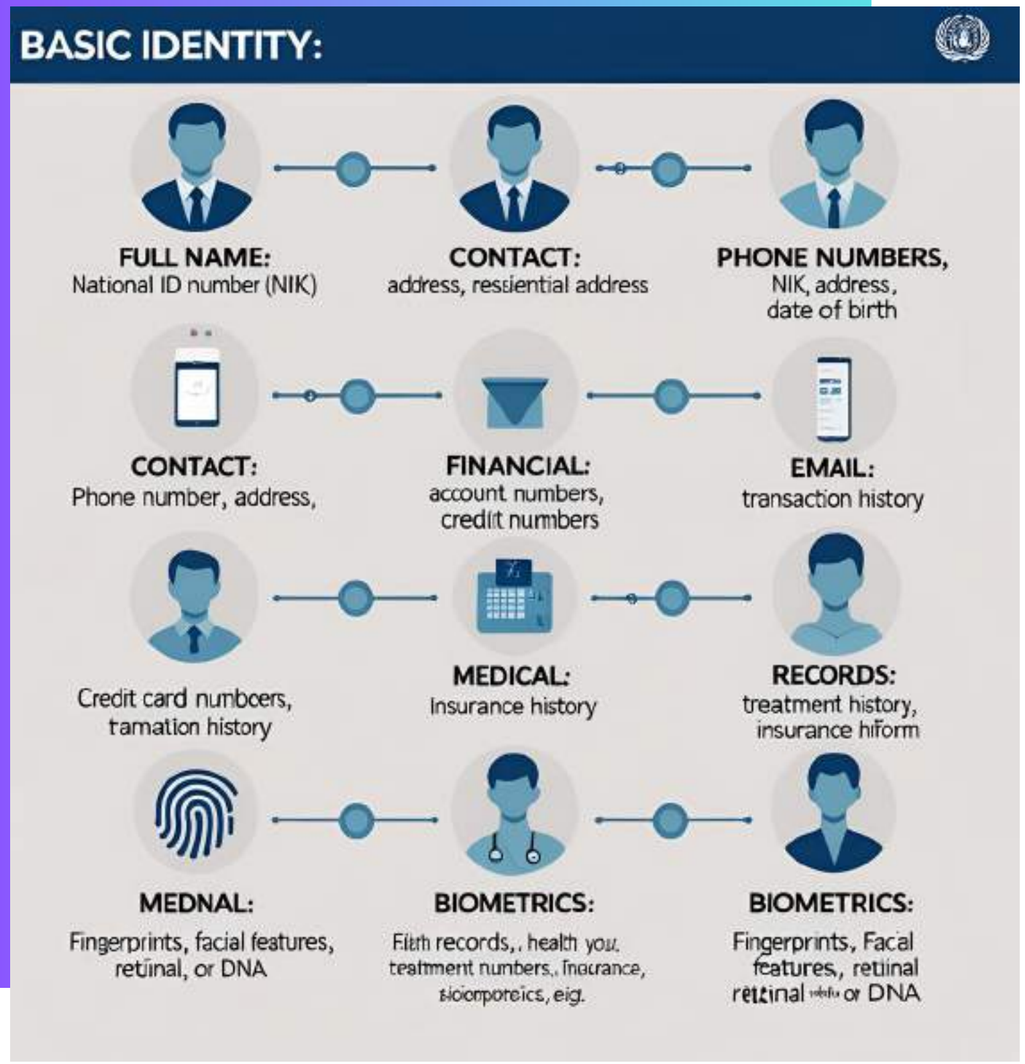
Contohnya:

- Identitas dasar: nama lengkap, NIK, alamat, tanggal lahir.
- Kontak: nomor telepon, email, alamat domisili.
- Keuangan: nomor rekening, kartu kredit, riwayat transaksi.
- Medis: rekam kesehatan, riwayat pengobatan, informasi asuransi.
- Biometrik: sidik jari, wajah, retina mata, atau DNA.
- Informasi digital: username, password, lokasi GPS, dan riwayat aktivitas online.
- Perlindungan terhadap data ini penting untuk mencegah pencurian identitas, penipuan, atau penyalahgunaan oleh pihak yang tidak berwenang.

Regulasi & UU Perlindungan Data Pribadi di Indonesia

Di Indonesia, perlindungan data pribadi diatur dalam:

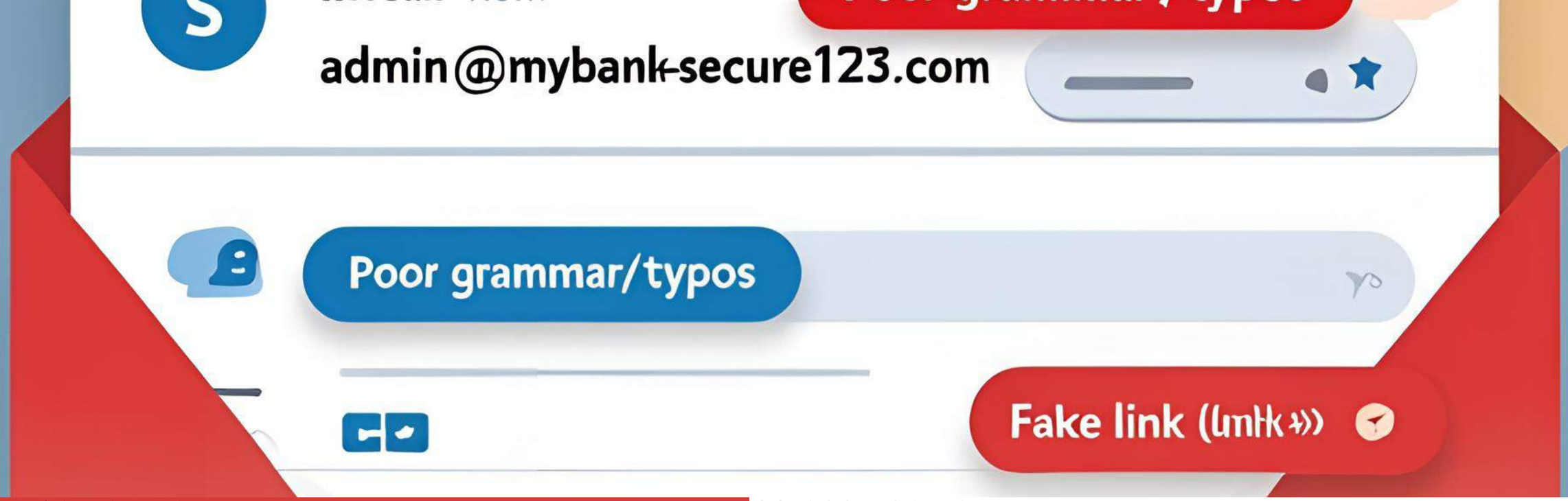
- UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP): Mengatur hak subjek data, kewajiban pengendali data, serta sanksi atas pelanggaran.
- UU ITE dan peraturan turunannya: Melindungi data dalam transaksi elektronik.
- Peraturan sektoral seperti Peraturan BSSN, Permendagri, dan kebijakan internal instansi.
- UU PDP menekankan prinsip pemrosesan data yang sah, transparan, terbatas pada tujuan tertentu, serta menjamin keamanan data dari kebocoran.



Praktik Pengamanan Data di Instansi

Untuk melindungi data pribadi, instansi perlu menerapkan langkah-langkah berikut:

1. Mengklasifikasikan data berdasarkan tingkat kerahasiaan.
2. Menerapkan kontrol akses agar hanya pihak berwenang yang dapat melihat atau mengubah data.
3. Menggunakan enkripsi untuk penyimpanan dan pengiriman data.
4. Melakukan pencadangan data secara berkala.
5. Melatih pegawai terkait kebijakan privasi dan keamanan data.
6. Menerapkan prosedur penghapusan data yang aman ketika tidak lagi digunakan.
7. Melakukan audit dan pengujian keamanan secara rutin.



Ciri-Ciri Email Phishing

Label teks menunjuk ke elemen mencurigakan:

- **Alamat pengirim aneh (contoh: admin@bankku-secure123.com)**
- **Tata bahasa buruk / typo**
- **Tautan palsu (ditunjukkan link yang beda dari teks)**
- **Lampiran mencurigakan**

Cara Aman Berbagi Informasi di Media Sosial

Yang Dilakukan	Boleh	Tidak Boleh
		
Contoh	**Contoh**	**Contoh**
Membagikan Informasi Umum Saja, Menggunakan Filter atau jaringan yang aman.	Upload kartu ID, Kartu Vaksin, Tiket Penerbangan, Perjalanan Dengan Detail tanpa informasi sensitif.	Upload kartu ID, Kartu Vaksin, Tiket Penerbangan, Perjalanan Dengan Detail
Mengguakan Foto yang aman tanpa penambahan geotag atau GPS.	Menyebarkan Foto Pribadi namun tidak pada lokasi yang jelas.	Menampilkan semua informasi berupa lokasi, tiket perjalanan,, penginapan dan tujuan selanjutnnya, atau kartu kredit/ debid.
Penggunaan Bahasa saat posting atau status.	Gunakan bahasa yang sopan dan profesional.	Menggunakan bahasa yang tidak etis atau menjelakan sesuatu hal yang bersifat sensitif
Penggunaan Akun Media Sosial.	Menggunakan Akun Berbeda pada pekerjaan atau pribadi.	Menggunakan satu akun sama sehingga Membagikan rahasia pekerjaan atau dokumen kantor

Mengatur Privasi Akun

1. Pengaturan Izin Aplikasi (App Permissions)

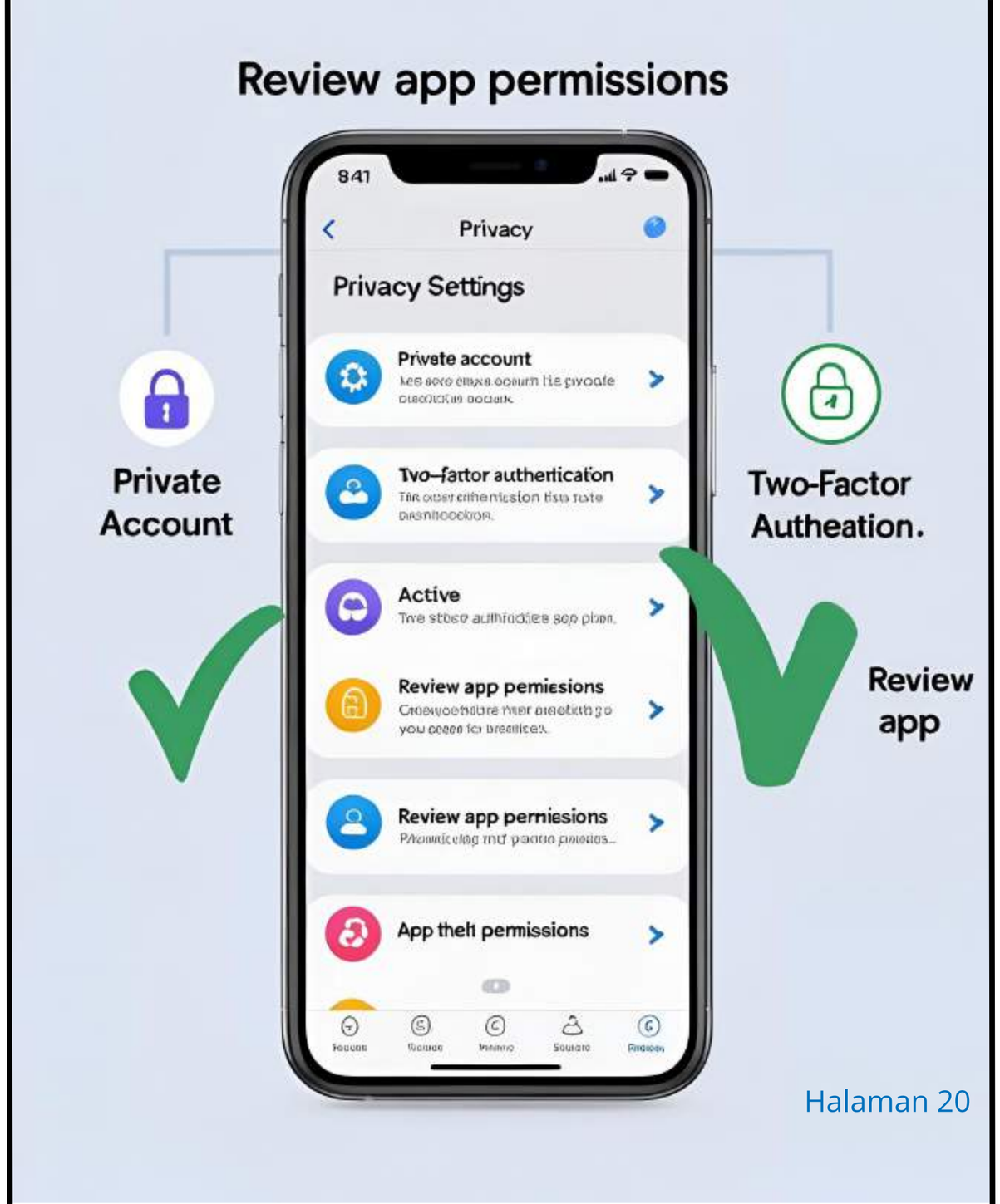
- Batasi akses aplikasi hanya pada data dan fitur yang memang diperlukan (kamera, mikrofon, lokasi, kontak).
- Nonaktifkan izin untuk aplikasi yang jarang digunakan atau mencurigakan.

2. **Penguncian Layar & Otentikasi**

- Gunakan PIN, password, pola, atau biometrik (sidik jari/wajah) untuk mencegah akses ilegal.
- Aktifkan auto-lock dalam waktu singkat (misalnya 30 detik – 1 menit).

3**. Kontrol Lokasi & Pelacakan**

- Matikan GPS jika tidak digunakan.
- Atur agar aplikasi hanya boleh mengakses lokasi saat digunakan (bukan selalu).



Keamanan Jaringan

1. **Gunakan Wi-Fi yang Aman (Trusted Network)**
   → Sambungkan hanya ke Wi-Fi yang Anda kenal, seperti rumah atau kantor.
   → Pastikan Wi-Fi dilindungi dengan password kuat (WPA2/WPA3).
   → Ubah password Wi-Fi secara berkala untuk mencegah akses tidak sah.

2 . Aktifkan VPN Saat Mengakses Jaringan Publik
→ Instal aplikasi VPN terpercaya di smartphone.
→ Aktifkan VPN sebelum menggunakan Wi-Fi publik di kafe, bandara, atau hotel.
→ Pilih server VPN yang cepat dan sesuai lokasi untuk kinerja optimal .

3. Matikan Auto-Connect ke Wi-Fi
→ Buka pengaturan Wi-Fi di smartphone.
→ Nonaktifkan fitur auto-connect atau connect automatically
→ Hapus jaringan Wi-Fi yang sudah tidak digunakan dari daftar tersimpan.

Pembaruan Sistem & Aplikasi

Pembaruan sistem operasi (OS) dan aplikasi bukan sekadar menambah fitur baru, tetapi juga menutup celah keamanan yang dapat dimanfaatkan peretas. Versi lama seringkali memiliki bug atau kelemahan yang sudah diketahui publik, sehingga memperbarui OS dan aplikasi adalah langkah preventif yang penting. Selain itu, mengunduh aplikasi dari sumber tidak resmi berisiko membawa malware yang dapat mencuri data atau merusak perangkat.

Backup & Enkripsi Data

Kehilangan perangkat tidak selalu berarti kehilangan data, asalkan backup dilakukan secara rutin. Backup membantu memulihkan data saat terjadi kerusakan, pencurian, atau serangan siber. Sementara itu, enkripsi penyimpanan memastikan bahwa data tetap terlindungi meskipun perangkat jatuh ke tangan orang yang tidak berwenang.

Penanganan Insiden Keamanan Informasi

Insiden keamanan informasi dapat terjadi kapan saja dan dalam berbagai bentuk, seperti defacement situs web (misalnya diganti dengan konten judi online seperti slot gacor atau cytotect), kebocoran data pribadi, hingga eksploitasi kelemahan sistem. Tanda-tanda umum serangan meliputi perubahan tampilan situs tanpa izin, file atau data hilang atau rusak, adanya aktivitas login mencurigakan, dan peningkatan lalu lintas jaringan yang tidak wajar.

Saat mendeteksi tanda-tanda ini, langkah pertama yang harus dilakukan adalah mengamankan sistem untuk mencegah kerusakan lebih lanjut, seperti memutus koneksi internet sementara, menonaktifkan akun yang terdampak, dan membuat salinan log sistem untuk analisis. Selanjutnya, insiden harus segera dilaporkan kepada tim terkait agar dapat ditangani dengan cepat dan efektif.

Penerapan:

1. **Identifikasi tanda serangan** — periksa perubahan tidak wajar pada sistem atau data.
2. **Isolasi sistem terdampak** — matikan koneksi internet atau jaringan lokal untuk membatasi penyebaran.
3. **Amankan bukti digital** — simpan log dan bukti aktivitas untuk investigasi.
4. Laporkan insiden ke CSIRT Pemerintah Kabupaten Purbalingga melalui:
   - Email: csirt@purbalinggakab.go.id
   - Formulir Laporan Keamanan Informasi (https://s.id/Insdensiberpbg)
5. Ikuti instruksi tim CSIRT untuk pemulihan sistem dan pencegahan serangan berulang.

Budaya Kerja Aman Secara Digital

Budaya kerja aman secara digital adalah kebiasaan positif yang diterapkan setiap hari oleh seluruh pegawai untuk menjaga keamanan informasi, mencegah kebocoran data, dan memastikan keberlangsungan layanan sistem elektronik. Budaya ini mencakup kepatuhan pada kebijakan keamanan, kewaspadaan terhadap ancaman siber, serta kesadaran bahwa setiap individu memiliki peran penting dalam melindungi data dan sistem. Penerapan budaya kerja aman bukan hanya tanggung jawab tim IT, tetapi menjadi tanggung jawab bersama di seluruh instansi.

---

1. Gunakan kata sandi yang kuat dan unik untuk setiap akun kerja.
2. Selalu kunci perangkat kerja (PC, laptop, smartphone) saat tidak digunakan.
3. Hindari membuka tautan atau lampiran mencurigakan pada email maupun pesan instan.
4. Laporkan segera insiden atau aktivitas mencurigakan ke CSIRT atau tim keamanan informasi.
5. Ikuti pelatihan keamanan informasi secara berkala untuk meningkatkan kesadaran dan keterampilan.
6. Pisahkan penggunaan perangkat dan akun pribadi dengan pekerjaan untuk menghindari kebocoran data.
7. Patuh pada SOP dan kebijakan keamanan informasi yang berlaku di instansi.

Ingatlah, Bahwa Kechilafan Satu Orang Sahaja Tjukup Sudah MenJebabkan Keruntuhan Negara

dr. Roebiono Kertopati

Bapak Persandian indonesia