Awareness Keamanan Informasi dan Privasi Data ISO/IEC 27001:2022 – ISO/IEC 27701

PT Perkebunan Nusantara I

AGUS HERMANTO, S.Kom, M.MT, ITIL, COBIT, SFC

Pre Test

https://bit.ly/pretesHO2025

Link Materi Awareness 2025

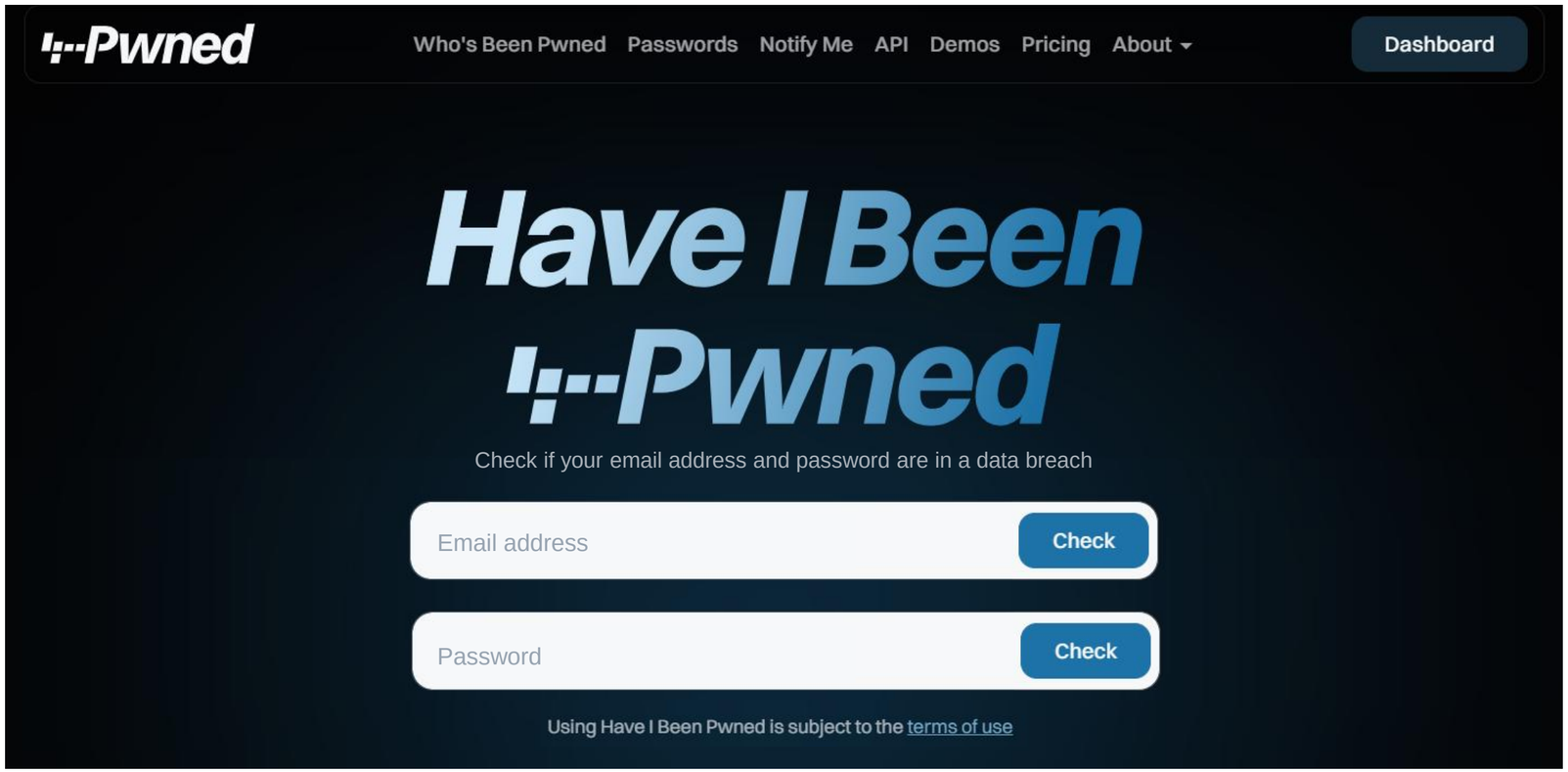
https://drive.ptpn1-ho.my.id/

Seberapa aman password-mu?

Jumlah Karakter	Huruf kecil semua	Ada satu huruf besar	Satu huruf besar + angka	Satu huruf besar + angka + simbol
5	Langsung	Langsung	Langsung	Langsung
6	Langsung	Langsung	Langsung	Langsung
7	Langsung	Langsung	1 menit	6 menit
8	Langsung	22 menit	1 jam	8 jam
9	2 menit	19 jam	3 hari	3 minggu
10	1 jam	1 bulan	7 bulan	5 tahun
11	1 hari	5 tahun	41 tahun	400 tahun
12	3 minggu	300 tahun	2000 tahun	34000 tahun

Ket: waktu yang dibutuhkan untuk meretas passwordmu

Taukah kamu?



Website *Have I Been Pwned* memungkinkan kamu memeriksa apakah alamat email dan passwordmu telah terekspos dalam pelanggaran data

Mari Simulasikan!
Seberapa aman email dan password-mu

https://haveibeenpwned.com/

DigiLife

The **digital landscape presents considerable perils**, yet it is a territory we can successfully secure, provided we implement the **appropriate defensive measures**.

Meskipun dunia digital memiliki kerentanan yang melekat, keamanannya dapat dijaga melalui **penerapan protokol** yang diperlukan secara tepat.

Agus Hermanto

Keamanan Siber + Privasi = ✓ Terpadu & Kuat


SALINAN

PRESIDEN
REPUBLIK INDONESIA

JNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 27 TAHUN 2022

TENTANG

PELINDUNGAN DATA PRIBADI

Relasional Standar Internasional dan UU PDP

Standar / Regulasi	Tujuan utama	Ruang Lingkup	Deskripsi Relasional
ISO 27001	Menetapkan Sistem Manajemen Keamanan Informasi (ISMS) untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi	Semua jenis informasi (tidak khusus data pribadi)	Merupakan fondasi keamanan yang harus dimiliki sebelum memperluas ke privasi (ISO 27701)
ISO 27701	Ekstensi ke ISMS untuk menambahkan kontrol dan persyaratan pengelolaan data pribadi (Privacy Information Management System / PIMS)	Pemrosesan PII (Personally Identifiable Information) oleh pengendali (controller) dan pemroses (processor)	Memanfaatkan kontrol ISO 27001 + tambahan kontrol privasi; mendukung kepatuhan regulasi (termasuk UU PDP)
UU No. 27 Tahun 2022 (UU PDP)	Memberikan dasar hukum perlindungan data pribadi di Indonesia, mengatur hak-hak subjek data, kewajiban pengendali dan pemroses, sanksi, lembaga pengawas, dsb.	Pemrosesan data pribadi dalam lingkup wilayah hukum Indonesia (meskipun pemrosesan lintas batas bisa diatur)	Menjadi kerangka regulatori yang harus dipenuhi; ISO 27701 dapat menjadi alat untuk membantu membuktikan kepatuhan dan kontrol operasional terhadap ketentuan UU PDP

Relasional Standar Internasional dan UU PDP

Prinsip	ISO 27001	ISO 27701	Relevansi dalam UU PDP
Prinsip keamanan informasi (CIA)	Fundamental (kerahasiaan, integritas, ketersediaan)	Masih berlaku sebagai dasar keamanan untuk PII	Pengendali dan pemroses wajib menjaga keamanan data pribadi dalam pemrosesan (Pasal UU PDP)
Akuntabilitas / pertanggungjawaban	Organisasi harus menunjukkan bahwa kontrol diterapkan dan dipantau	ISO 27701 mewajibkan dokumentasi, audit trail, bukti kepatuhan kontrol privasi	UU PDP menetapkan kewajiban pengendali/pemroses untuk dapat membuktikan bahwa mereka memproses data sesuai ketentuan (aspek pertanggungjawaban)
Prinsip minimalisasi dan kebutuhan	Dalam analisis risiko dan penerapan kontrol (hanya kontrol yang relevan)	ISO 27701 mengharuskan bahwa pemrosesan PII harus dibatasi sejauh yang diperlukan	UU PDP mengatur bahwa data pribadi hanya boleh diproses jika diperlukan dan proporsional (asas kebutuhan)
Security by design / default	ISO 27001 mendukung penerapan kontrol dari awal desain sistemnya	ISO 27701 menambahkan aspek privasi dari desain (privacy by design / default)	UU PDP memuat ketentuan bahwa pemrosesan harus mempertimbangkan keamanan dan privasi dalam desain sistem (secara teknis dan organisasi)

Aspek / Domain	Persyaratan ISO 27001 / kontrol relevan	Tambahan ISO 27701 (privasi)	Ketentuan UU PDP
Kebijakan keamanan & privasi	Kebijakan keamanan informasi umum	Kebijakan privasi / pengolahan data pribadi, standarisasi persetujuan & transparansi	Organisasi wajib menetapkan kebijakan internal pengelolaan data pribadi
Penilaian risiko	Identifikasi risiko keamanan umum	Penilaian risiko privasi (privacy risk assessment)	Pengendali/pemroses wajib mengidentifikasi dan mengelola risiko privasi
Kontrak dengan pemroses pihak ketiga	Pengendalian vendor & pihak ketiga (keamanan)	Kontrak pemroses harus mencakup kewajiban privasi, pembatasan, proteksi data	UU PDP mengamanatkan bahwa pengendali bertanggung jawab atas pemroses dan harus menjamin kepatuhan
Hak subjek data	— (tidak di ISO 27001)	Mekanisme untuk akses, koreksi, penghapusan, keberatan, dsb	UU PDP memberikan hak-hak ini dan mewajibkan pengendali memenuhi hak tersebut
Pelaporan pelanggaran	Prosedur insiden keamanan	Penanganan pelanggaran data pribadi, notifikasi subjek data / otoritas	UU PDP menentukan kewajiban pelaporan dalam jangka waktu tertentu dan sanksi jika tidak dilaksanakan
Retensi & penghapusan data	Kebijakan retensi umum	Kebijakan retensi khusus untuk PII, penghapusan, anonimisasi	UU PDP menyatakan data pribadi tidak boleh disimpan lebih lama dari yang diperlukan dan harus dihapus / anonimkan
Transfer data lintas negara	— atau kebijakan keamanan jaringan	Kontrol transfer data antar yurisdiksi, mekanisme perlindungan tambahan	UU PDP menetapkan ketentuan transfer data ke luar negeri hanya jika perlindungan data setara atau mekanisme legal lainnya

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Kebijakan – Kepemimpinan - Manajemen

ISO 27001 (area)	ISO 27701	UU PDP (relevansi)	Implementasi	Bukti / Artefak	Penanggung jawab
Kepemimpinan & konteks organisasi, kebijakan ISMS	Kebijakan PIMS (privacy policy internal), penetapan roles: PII controller/processor, DPO jika diperlukan	Kewajiban pengendali/pemroses, akuntabilitas; definisi pengendali/pemroses; kebijakan internal.	Tetapkan kebijakan ISMS + PIMS yang mencakup pemrosesan data karyawan, supplier, pelanggan, citra satelit, telemetri. Tentukan pengendali data (mis. BUMN unit bisnis) dan pemroses (mis. vendor cloud).	Dokumen Kebijakan ISMS, Kebijakan PIMS, SK penunjukan DPO/penanggung jawab data, peta peran organisasi.	Direktur IT / Direktur Kepatuhan / DPO
Manajemen risiko keamanan informasi	Privacy risk assessment (PIA/DPIA) untuk pemrosesan berisiko tinggi (biometrik, lokasi, pengawasan)	UU PDP mewajibkan identifikasi dan mitigasi risiko; DPIA bila diperlukan	Lakukan DPIA pada: sistem absensi biometrik pekerja, sistem tracing pembeli/mitra, integrasi IoT/SCADA kebun, transfer data lintas negara (vendor cloud).	Laporan DPIA/PIA, Matriks risiko, rencana mitigasi.	Risk Manager / DPO / Security Officer

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Pustaka dan Pengendalian Data

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Manajemen aset & klasifikasi informasi	Klasifikasi khusus PII (sensitive PII: biometrik, health, gaji), siklus hidup PII	Prinsip minimalisasi, pembatasan penyimpanan	Inventaris sumber data: HRIS (karyawan), CRM (pembeli), CCTV, data panen, kontrak mitra; tandai mana PII & sensitive.	Data inventory register, data flow diagram, klasifikasi PII list.	Data Owner (HR, Ops, Sales) & DPO
Kebijakan retensi & disposal	Retensi PII berdasarkan tujuan & dasar hukum; prosedur anonimisasi/pseduonimisasi	UU PDP: data tidak disimpan lebih lama dari yang diperlukan; hak penghapusan	Retensi dokumen karyawan, customer, CCTV (mis. 90 hari), kebijakan anonymization untuk dataset riset	Retention schedule, SOP deletion, bukti penghapusan/anonimisasi	Records Manager / Legal / DPO

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Legalitas & Hak Subjek Data

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Kontrak & manajemen vendor	Persyaratan kontrak PII (sub-processor), ketentuan pemrosesan, purpose limitation	UU PDP: dasar hukum pemrosesan (persetujuan, kontrak, kewajiban hukum, kepentingan publik, dll)	Perbarui SLA/contract dengan vendor cloud, payroll, biometrik agar mencantumkan kewajiban PDP (treatment, breach notification, audit rights).	Template kontrak pemroses PII, daftar vendor & assessment.	Procurement / Legal / DPO
Akses subjek data & mekanisme memenuhi permintaan	Mekanisme untuk memenuhi rights: akses, koreksi, penghapusan (right to be forgotten), portabilitas	UU PDP mengatur hak subjek data (akses, koreksi, penghapusan, keberatan)	Portal/Prosedur layanan pelanggan & HR untuk menerima & memproses permintaan hak subjek data; SLA jawaban.	SOP pemenuhan hak subjek, log permintaan & penyelesaian.	Customer Service, HR, DPO

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Kontrol akses & identitas

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Kontrol akses & manajemen identitas	Pembatasan akses PII berdasarkan role, least privilege, logging akses PII spesifik	UU PDP: kewajiban perlindungan teknis & organisasi	Implementasi RBAC pada HRIS/ERP; gateway untuk akses data lapangan; log akses ke data karyawan dan pelanggan; MFA untuk admin.	Access control matrix, user access reviews, access logs for PII.	IT Security / HR / DPO
Penggunaan data biometrik & sensor	Persyaratan eksplisit untuk pemrosesan sensitive PII; consent dan mitigasi	UU PDP biasanya memerlukan dasar hukum tambahan & perlindungan untuk data sensitif	Prosedur pengumpulan biometrik pekerja: persetujuan tertulis, minimisasi, enkripsi template biometrik, fallback manual	Consent forms, encryption configuration, usage SOP	HR / Ops / DPO

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Teknologi Luar Ruang / Manufaktur (OT/SCADA, IoT) & fisik

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Keamanan jaringan & endpoint (IT/OT segregation)	Fokus pada proteksi PII di sistem OT/IoT, enkripsi data in motion & at rest	UU PDP: langkah teknis untuk melindungi data pribadi	Segmentasi jaringan antara SCADA/IoT dan corporate IT; enkripsi telemetry yang berisi lokasi pekerja; hardening perangkat lapangan	Network diagrams, firewall rules, encryption configs, vulnerability scan reports	IT / OT Manager / Security
Keamanan fisik (peringatan akses area)	Kontrol akses fisik ke lokasi penyimpanan PII fisik (arsip, server)	UU PDP: perlindungan data pribadi termasuk non-electronic records	Kontrol akses gudang dokumen, server room; kebijakan pengunjung di kebun; CCTV retention sesuai kebijakan	Visitor logs, CCTV policy, physical access logs	Facilities / Security

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Logging, monitoring, insiden & breach notification

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Logging & monitoring	Log khusus PII access & processing; audit trail untuk pemenuhan hak & audit	UU PDP: pelaporan pelanggaran data kepada otoritas/subjek data dalam waktu tertentu	Sistem SIEM yang memantau akses PII; prosedur notifikasi pelanggaran; playbook incident response khusus data pribadi	Incidents register, SOC logs, breach notification templates, forensic reports	CSIRT / Security / DPO
Business continuity & backup	Proteksi backup PII, recovery plan yang mempertimbangkan privacy	UU PDP: kewajiban menjaga ketersediaan & integritas data	Backup terenkripsi untuk HR/payroll/transactional data; uji DR untuk pemulihan PII	Backup logs, restore test reports, BCP/DR plan	IT Ops / BC Manager / DPO

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Human Resources & Awareness

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung Jawab
Screening & training staff	Training spesifik privasi; kewajiban kerahasiaan untuk pegawai yang memproses PII	UU PDP: kewajiban organisasi untuk menerapkan langkah organisasi (termasuk SDM)	Program training berkala untuk HR, admin, petugas lapangan; klausul NDA/kerahasiaan ; onboarding privacy checklist	Rekam pelatihan, signed NDAs, policy acknowledgements	HR / DPO

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Transfer & Cross-border Data

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Transfer data & keterlibatan pihak ketiga	Kontrol transfer PII, due diligence pada transfer lintas yurisdiksi	UU PDP: aturan transfer lintas negara (kesetaraan perlindungan, mekanisme legal)	Evaluasi vendor cloud non-domestik; perjanjian SCC/garansi teknis; enkripsi end-to-end	Data transfer register, DPIA transfer, contracts with clauses on cross-border transfer	Legal / Procurement / DPO

Implementasi Terpadu ISO 27001-ISO 27701 dan UU PDP

Domain Audit, Compliance & Continuous Improvement

ISO 27001	ISO 27701	UU PDP	Implementasi	Bukti	Penanggung jawab
Internal audit & management review	Audit khusus PIMS; evidence koleksi pemenuhan hak subjek & kegiatan pemrosesan	UU PDP: pemenuhan kewajiban & sanksi — organisasi harus dapat menunjukkan kepatuhan	Jadwalkan audit internal PIMS + eksternal; gap analysis terhadap UU PDP; perbaikan berkelanjutan	Laporan audit, MRM minutes, compliance gap analysis	Internal Audit / Management / DPO

Penguatan Keamanan Dan Privasi

FROM THIS

CIA TRIAD

TO THIS

PARKERIAN HEXAD

CIA Triad tidak cukup memadai untuk mencakup semua aspek keamanan siber modern. Tiga elemen tambahan (Kepemilikan/Kontrol, Keaslian, dan Kegunaan) memperluas cakupan keamanan dari sekadar melindungi data menjadi memastikan bahwa data tersebut tetap dapat dipercaya, berguna, dan berada di bawah kendali yang tepat.

Confidentiality (Kerahasiaan)

Kerahasiaan merupakan elemen terpenting dari CIA TRIAD dan Parkerian Hexad

Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Tujuannya mencegah kebocoran data kepada pihak yang tidak berhak.

Resiko Ancaman Pada Aspek Confidentiality (Kerahasiaan)

Phising
(Pencurian Kredensial)

Eavesdroppong
(Penyadapan data)

Data Breach
(Kebocoran Data)

Cara menjaga Confidentiality:

- **Enkripsi:** Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi (contoh: AES, RSA).
- **Kontrol akses:** Mengatur siapa yang boleh melihat atau memodifikasi data (contoh: Role-Based Access Control).
- **Autentikasi kuat:** Menggunakan MFA (*multi-factor authentication*) atau biometrik.
- **Pengelolaan hak akses:** Menghapus akses bagi pegawai yang sudah keluar atau pindah posisi.

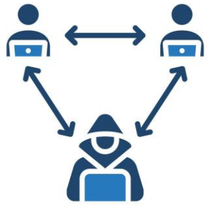
Integrity (Integritas)

Integritas adalah komponen asli dari triad CIA. Integritas didefinisikan sebagai kemampuan untuk mencegah data diubah dengan cara yang tidak sah atau tidak diinginkan, dengan menjaga data tetap akurat, lengkap, baik secara sengaja maupun tidak sengaja.

Resiko Ancaman Pada Aspek Integrity (Integritas)

Data Tampering
(Modifikasi data ilegal)

Hardware Failure
(Kerusakan Perangkat)



Man-in-the-Middle
(Pengubahan Pesan Saat Transferl)

Cara menjaga Integrity:

- **Hashing:** Menghasilkan nilai unik dari data (contoh: SHA-256) untuk memverifikasi keaslian.
- **Digital signature:** Menjamin bahwa pengirim adalah asli dan data tidak dimodifikasi.
- **Checksum / CRC:** Memeriksa integritas file saat transfer atau penyimpanan.
- **Version control:** Menyimpan riwayat perubahan sehingga bisa kembali ke versi sebelumnya.

Availability (Ketersediaan)

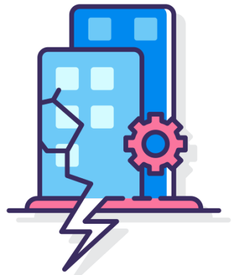
Availability adalah komponen terakhir dari model CIA asli.

Availability didefinisikan sebagai kemampuan untuk menyediakan sumber daya (data / informasi / layanan) saat dibutuhkan.

Resiko Ancaman Pada Aspek Availability (Ketersediaan)

Denial of services
(Modifikasi data ilegal)

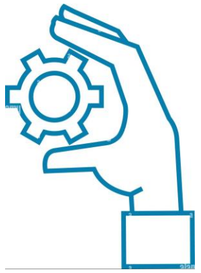
Siftware Failure
(Kegagalab Apps)



Disaster
(Bencana)

Cara menjaga Availability:

- **Backup dan pemulihan bencana (Disaster Recovery):** Menyimpan salinan data di lokasi terpisah.
- **Redundansi sistem:** Memiliki perangkat keras dan jaringan cadangan.
- **Load balancing:** Membagi beban lalu lintas ke beberapa server.
- **Patching dan pemeliharaan rutin:** Mencegah kegagalan karena bug atau kerentanan.

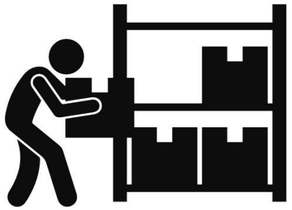


Possession or Control (Kepemilikan atau Kendali)

Komponen Posseion Or Control merupakan salah satu tambahan Parker pada model CIA..

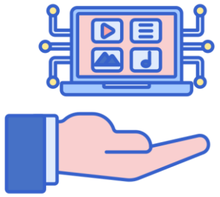
Komponen ini bertujuan memastikan bahwa pihak yang berhak (berwenang) tetap memiliki kendali fisik atau logis atas informasi.

Resiko Ancaman Pada Aspek Availability (Ketersediaan)



Theft or Exfiltration of Data:

(Pencurian atau Penghancuran Data)



Seizure of Assets (Physical or Digital)

(Pengambilan paksa akses fisik atau logis terhadap data)

Extortion Attacks

(Penguncian data untuk tebusan)

Cara menjaga Possesion or Control:

- Robust Access Control Mechanisms
- Physical Security Controls.
- Data Encryption (At Rest and In Transit).
- Network Security Measures
- Endpoint Security:
- Data Backup and Recovery
- Incident Response Plan

Authenticity (Keaslian)

Authenticity adalah salah satu tambahan Parker pada model CIA.

Menjamin bahwa informasi, komunikasi, atau dokumen memang berasal dari sumber yang sah dan dapat dipercaya..

Resiko Ancaman Pada Aspek Authenticity (Keaslian)

Impersonation/Spoofing

(Peniruan/Pemalsuan)

Source Forgery

(Tidak terverifikasi/Pemalsuan Sumber)

Compromised Signature

(Peniruan Tanda Tangan Digital)

Cara menjaga Authenticity:

- Strong Authentication Mechanisms
- Digital Signatures and Certificates (Public Key Infrastructure - PKI)
- Hashing and Checksums
- Secure Communication Protocols
- Logging and Auditing

Utility (Kegunaan)

Memastikan informasi tetap berguna dan dapat dimanfaatkan sesuai tujuan.

Data mungkin ada dan utuh, tetapi tidak berguna jika dalam format yang tidak dapat dibaca atau digunakan.

Resiko Ancaman Pada Aspek Utility (Kegunaan)

Format Incompatibility / Data Encoding Issues

(Format Tidak Layak)

Data Obsolescence / Irrelevance:

(Data Usang / Tidak Relevan)

Information Overload / Poor Presentation

(Peniruan Tanda Digital)

Lack of Interoperability / Integration Issues:

(Tidak terverifikasi/Pemalsuan Sumber)

Performance Degradation/impacting usability)

(Peniruan Tanda Digital)

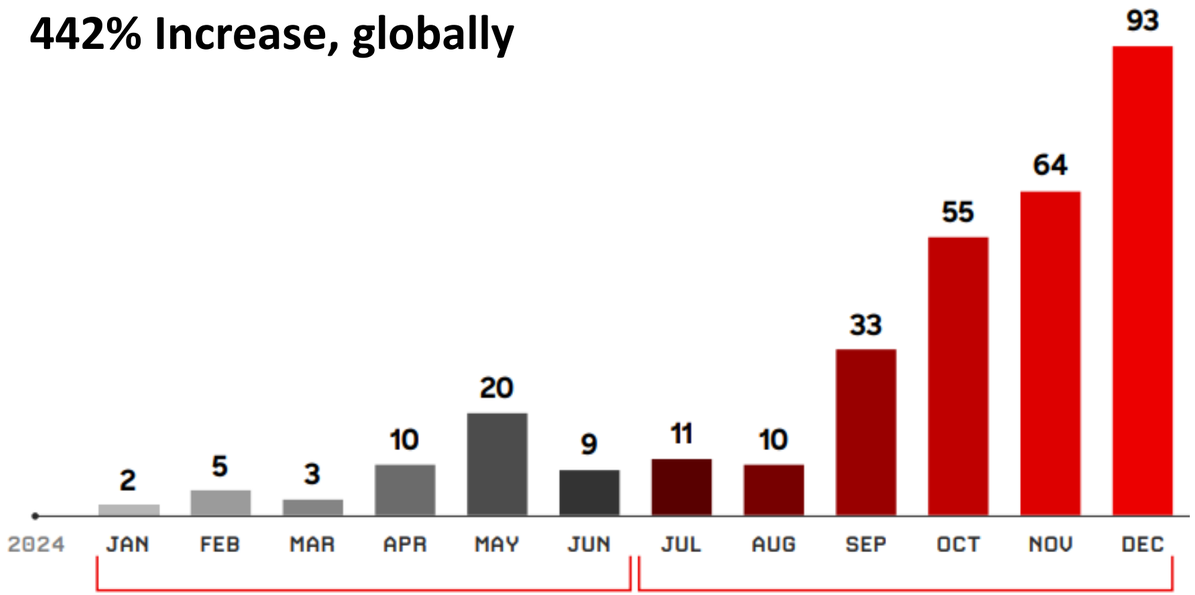
Cara menjaga Authenticity:

- Strong Authentication Mechanisms
- Digital Signatures and Certificates (Public Key Infrastructure - PKI)
- Hashing and Checksums
- Secure Communication Protocols
- Logging and Auditing

Cyber Security Threat Report 2024

2024 Vishing Detections

442% Increase, globally



What's next??

2025

2024

- **Aktivitas Ransomware** 514.508
- **Aktivitas Phising** 26.771.610
- **Defament Judol** 4.071

Best Practise Perlindungan Data

Jenis Data Pribadi yang Perlu Dilindungi

Data Karyawan: NIK, nomor rekening gaji, riwayat kesehatan (BPJS), data keluarga.
Data Petani Plasma: identitas, rekening bank, luas lahan, hasil panen.
Data Pelanggan & Vendor: kontrak, nomor telepon, alamat email, data transaksi.

Prinsip ISO 27701 koleksi, simpan dan gunakan data pribadi sesuai tujuan yang sah dan legal

Peran	Tanggung Jawab
Karyawan biasa	Menjaga kerahasiaan data (tidak membagikan tanpa izin), mengikuti SOP pengelolaan data.
Manajer / Supervisor	Memastikan data pribadi yang diproses di unitnya sesuai aturan (misal payroll, data petani).
Admin IT	Menjaga sistem aplikasi HR, ERP, dan produksi agar aman (akses terbatas, enkripsi).
Top Management	Menetapkan kebijakan privasi, mengawasi kepatuhan UU PDP dan ISO 27701.

Budaya Menjaga Data

Kerahasiaan Data

1. Jangan simpan NIK atau data gaji di flashdisk/WhatsApp tanpa enkripsi.
2. Gunakan sistem resmi perusahaan untuk mengirimkan data.

Prinsip Minimasi Data

Hanya minta data yang benar-benar dibutuhkan (misalnya, untuk subsidi pupuk cukup NIK & luas lahan, tidak perlu data keluarga).

Hak Pemilik Data

Staf terkait harus paham bahwa petani/karyawan punya **hak akses, hak perbaikan, dan hak hapus data** sesuai UU PDP.

Keamanan Digital

1. Gunakan password yang kuat & MFA untuk akses aplikasi perkebunan (ERP, payroll, e-office).
2. Jangan berbagi akun antar pekerja.

Insiden Kebocoran Data

Segera lapor ke atasan/Tim TI bila ada email/phishing mencurigakan, atau jika laptop/HP kerja hilang.

Budaya Menjaga Data

Kerahasiaan Data

1. Jangan simpan NIK atau data gaji di flashdisk/WhatsApp tanpa enkripsi.
2. Gunakan sistem resmi perusahaan untuk mengirimkan data.

Prinsip Minimasi Data

Hanya minta data yang benar-benar dibutuhkan (misalnya, untuk subsidi pupuk cukup NIK & luas lahan, tidak perlu data keluarga).

Hak Pemilik Data

Staf terkait harus paham bahwa petani/karyawan punya **hak akses, hak perbaikan, dan hak hapus data** sesuai UU PDP.

Keamanan Digital

1. Gunakan password yang kuat & MFA untuk akses aplikasi perkebunan (ERP, payroll, e-office).
2. Jangan berbagi akun antar pekerja.

Fakta yang sering terjadi

- **Payroll**: Data gaji staf disimpan di ERP dalam bentuk plaintext, seharusnya terenkripsi & hak akses hanya HR.
- **Data Petani Tebu**: Kontrak lahan & rekening bank disimpan di database, maka wajib dipastikan hanya unit tebu yang bisa akses.
- **Kesehatan Pekerja**: Hasil medical check-up, termasuk data yang tidak boleh dipublikasikan, hanya untuk dokter & HR.

GENERATIVE ARTIFICIAL INTELLIGENCE

Social Engineering

- FAMOUS CHOLLIMA employed fictitious LinkedIn profiles with genAI-created text and fake profile images
- Deepfake video and voice clones enabled business email compromise (BEC) schemes
- Studies validated effectiveness of genAI in phishing
- China-aligned, LLM-powered *Green Cicada* network posted coordinated inauthentic behavior on social media
- Russia-aligned operators used LLMs to spread disinformation on social media
- GenAI was used during Indian election season to create videos and images

Malicious Computer Network Operations

- Spam email campaign distributing *Snake Keylogger* likely used LLM-generated content
- Big game hunting (BGH) ransomware operators *APT INC* deployed likely LLM-authored data destruction script
- Likely LLM-generated decoy sites used in NITRO SPIDER campaigns
- Actors on criminal forms discussed using LLMs for coding and shell commands
- LLM was likely used to develop an alleged exploit for CVE-2024-3400
- Cloud-conscious operators attempted to gain access to enterprise LLMs

kevin mitnick

The most significant cyber threat that we face is not the one coming from criminal hackers, but from inside our organizations.

Ancaman dunia siber paling signifikan yang kita hadapi bukanlah ancaman yang datang dari hacker kriminal, tetapi dari dalam organisasi kita.

Integrasi dengan COBIT 2019

Area	ISO 27001 (Annex A)	ISO 27701	COBIT 2019 Objective
Governance & Risk	A.5 Information Security Policies	5.2 Privacy policy	EDM01 Ensure Governance Framework, EDM03 Ensure Risk Optimization
	A.6 Organization of Information Security	6.2 Roles & responsibilities for privacy	APO01 Manage the IT Management Framework, APO14 Manage Data
	A.18 Compliance with laws & regulations	8.2 Legal basis for processing PII	EDM02 Ensure Benefits Delivery, APO12 Manage Risk
Asset & Data Management	A.8 Asset Management	7.2 PII inventory & data mapping	APO03 Manage Enterprise Architecture, APO14 Manage Data
	A.9 Access Control	7.4 Access to PII	DSS05 Manage Security Services, DSS06 Manage Business Services
	A.10 Cryptography	7.5 Encryption of PII	DSS05 Manage Security Services
Human Resource Security	A.7 Human Resources Security	6.4 Privacy roles, awareness & training	APO07 Manage Human Resources, DSS04 Manage Continuity

Integrasi dengan COBIT 2019

Area	ISO 27001 (Annex A)	ISO 27701 (Kontrol tambahan PII)	COBIT 2019 Objective
Operations Security	A.12 Operations Security	7.6 Logging & monitoring PII	DSS01 Manage Operations, DSS05 Manage Security Services
	A.13 Communications Security	7.7 Data transfer controls	DSS01 Manage Operations, DSS05 Manage Security Services
Supplier Relationship	A.15 Supplier Relationships	8.3 Processor & third-party management	APO10 Manage Suppliers
Incident & Continuity	A.16 Information Security Incident Management	7.9 Breach notification (PII)	DSS02 Manage Service Requests & Incidents, DSS04 Manage Continuity
Monitoring & Improvement	A.17 Information Security Continuity	7.10 Privacy impact assessments (PIA)	MEA01 Monitor, Evaluate & Assess Performance, MEA02 Monitor, Evaluate & Assess Internal Control
	A.18 Information Security Compliance	7.11 Audit & assurance of PII controls	MEA03 Monitor, Evaluate & Assess Compliance

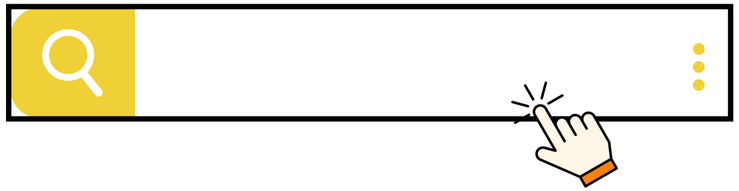
Phising


FUSION
They're gonna hack me using social engineering
REAL FUTURE

Vishing

Berpikir Kritis

Bersikaplah skeptis terhadap email, pesan, atau kiriman yang tampaknya terlalu bagus untuk menjadi kenyataan atau terlalu mendesak. Ingat, jika kedengarannya terlalu bagus untuk menjadi kenyataan, apakah itu benar!



Pikirkan sebelum mengklik tautan apa pun, membagikan informasi pribadi secara online, atau membuka lampiran yang mencurigakan. Tanyakan pada diri Anda sendiri apakah hal itu tampak sah dan apakah Anda mengharapkannya.

Verifikasi keaslian pengirim dan informasi yang diberikan sebelum mengambil tindakan apa pun. Percayai naluri Anda dan berhati-hatilah saat berbagi informasi secara online.

Ciri-ciri mencurigakan

01 Bahasa yang mendesak atau mengancam

02 Informasi pengirim yang mencurigakan

03 Permintaan informasi pribadi

04 Salah eja atau kesalahan tata bahasa

05 Tautan atau lampiran yang mencurigakan

06 Sapaan Umum

07 Too good to be true

Data Pribadi yang Perlu Diperhatikan

Tanda tangan digital	Salinan kartu identitas	Nomor telepon orang sekitar	Laporan medis atau info biometrik
Laporan rekening bank			Nomor ponsel
Kata sandi pribadi, PIN, atau data sensitif lainnya			Informasi laporan keuangan
Domisili atau alamat email			Kalender dengan rutinitas harian

Secure Your Privacy

PASSWORD SAFETY

Buat kata sandi yang kuat menggunakan kombinasi huruf, angka, dan simbol. Ubah kata sandi secara teratur untuk mencegah peretasan.

PHISHING SCAMS

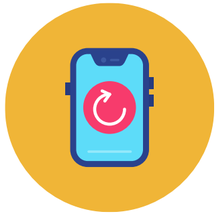
Waspadai email mencurigakan yang meminta informasi pribadi. Periksa kembali alamat email pengirim sebelum mengklik link apa pun.

SOCIAL MEDIA SAFETY

Jaga keamanan data perusahaan dan data pribadi Anda dengan tidak mempublikasikannya di media sosial.

KEEP YOUR DEVICES SECURE

Matikan perangkat atau aktifkan kunci layar saat perangkat tidak digunakan. Simpan, hapus, atau buang dokumen serta media penyimpanan yang mengandung informasi sensitif dengan aman



SOFTWARE UPDATES

Selalu perbarui perangkat lunak dan sistem operasi untuk mencegah kerentanan. Aktifkan pembaruan otomatis untuk kenyamanan dan keamanan.

BROWSING SAFETY

Pastikan mengakses situs web yang aman dan terpecaya, juga disarankan untuk menggunakan jaringan pribadi

Website untuk mengecek apakah email yang dimiliki sudah pernah bocor: https://haveibeenpwned.com/

Post Test

https://bit.ly/posttesHO2025

Terima Kasih!

Contact Us
+6282122293334

Visit Our Website
https://fittechinova.com/