PENABULU FOUNDATION
CIVIL SOCIETY RESOURCE ORGANIZATION

PEDOMAN PENA BULU
PENA BULU GUIDELINES

KEBIJAKAN DAN PROSEDUR PERLINDUNGAN DATA
DATA PROTECTION POLICY AND PROCEDURES

2025

LEMBAR PENGESAHAN / *APPROVAL SHEET*

No. Dokumen *Document No.*	008-Doc/LP/PB/VIII/2025
Nama Dokumen *Document Name*	Kebijakan dan Prosedur Perlindungan Data / Data Protection Policy and Procedures
Tanggal Pengesahan *Date of Approval*	1 Agustus 2025 *1 August 2025*

Versi / *Version*	Tanggal / *Date*	Deskripsi / *Description*
V1	1 Agustus 2025 *1 August 2025*	Dokumen awal *Initial Document*

Diajukan oleh: *Submitted by:*	Diperiksa oleh: *Reviewed by:*	Disetujui oleh: *Approved by:*
		
Eko Kurniawan Komara	**Hadi Prayitno**	**Damayanti Buchori**
Direktur Eksekutif *Executive Director*	Pengawas *Supervisory*	Ketua Pembina Chair of Governing Board

DAFTAR ISI / *TABLE OF CONTENT*

1. PENDAHULUAN

Yayasan Penabulu adalah organisasi masyarakat sipil yang bekerja untuk memperkuat kapasitas dan keberlanjutan lembaga-lembaga non-profit di Indonesia. Dalam menjalankan mandatnya, Penabulu secara rutin mengumpulkan, menyimpan, memproses, dan membagikan data pribadi dari berbagai pihak, termasuk penerima manfaat, donor, mitra pelaksana, staf, relawan, konsultan, serta penyedia jasa.

Kami menyadari bahwa data pribadi merupakan aset yang memiliki nilai strategis sekaligus memerlukan perlindungan ketat. Perlindungan ini tidak hanya menjadi kewajiban hukum, tetapi juga merupakan komitmen moral yang mendasari seluruh interaksi kami dengan para pemangku kepentingan. Kepercayaan yang diberikan kepada kami harus dijaga melalui pengelolaan data yang aman, transparan, dan bertanggung jawab.

Kebijakan ini dirancang sebagai kerangka kerja yang memandu seluruh staf, mitra, dan pihak ketiga yang bekerja atas nama Yayasan Penabulu dalam melaksanakan kegiatan pemrosesan data pribadi. Dokumen ini menguraikan prinsip-prinsip, peran dan tanggung jawab, prosedur, serta mekanisme pengawasan untuk memastikan setiap pengelolaan data dilakukan:

a. **Sesuai hukum:** Mematuhi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), peraturan nasional terkait, serta standar internasional seperti General Data Protection Regulation (GDPR).

b. Aman: Menggunakan langkah-langkah teknis dan prosedural untuk mencegah kehilangan, kerusakan, atau kebocoran data.

1. INTRODUCTION

Penabulu Foundation is a civil society organization that works to strengthen the capacity and sustainability of non-profit institutions in Indonesia. In carrying out its mandate, Penabulu routinely collects, recordkeeping, processes, and shares personal data from various parties, including beneficiaries, donors, implementing partners, staff, volunteers, consultants, and service providers.

We recognize that personal data is an asset that holds strategic value and requires strict protection. Such protection is not only a legal obligation but also a moral commitment that underpins all our interactions with stakeholders. The trust placed in us must be safeguarded through secure, transparent, and responsible data management.

This policy is designed as a framework that guides all staff, partners, and third parties working on behalf of Penabulu Foundation in carrying out personal data processing activities. This document outlines the principles, roles and responsibilities, procedures, and oversight mechanisms to ensure that all data management is conducted:

a. **Lawfully:** Complying with Law Number 27 of 2022 on Personal Data Protection (PDP), relevant national regulations, and international standards such as the General Data Protection Regulation (GDPR).

b. **Securely:** Using technical and procedural measures to prevent data loss, damage, or breaches.

c. **Transparan:** Memberikan informasi yang jelas kepada subjek data mengenai cara dan alasan data mereka diproses.

d. **Bertanggung jawab:** Menerapkan sistem pencatatan, audit, dan pelaporan yang dapat dipertanggungjawabkan.

Dengan diberlakukannya kebijakan ini, Penabulu berkomitmen untuk:

a. Melindungi hak dan kebebasan setiap individu yang datanya kami kelola.

b. Mengintegrasikan perlindungan data ke dalam semua tahapan perencanaan dan pelaksanaan program.

c. Mendorong budaya organisasi yang menghargai privasi dan keamanan informasi.

Kebijakan ini berlaku untuk semua unit kerja, proyek, dan kegiatan yang melibatkan pemrosesan data pribadi, baik dalam bentuk fisik maupun digital, di semua lokasi operasional Yayasan Penabulu.

2. TUJUAN

Kebijakan ini bertujuan untuk:

a. Menetapkan standar perlindungan data yang tinggi dan konsisten di seluruh kegiatan Penabulu.

b. Melindungi hak privasi setiap individu yang datanya dikelola oleh organisasi.

c. Memberikan panduan praktis bagi staf, mitra, dan pihak ketiga dalam menangani data pribadi.

c. **Transparently:** Providing clear information to data subjects regarding how and why their data is processed.

d. **Accountably:** Implementing accountable recording, auditing, and reporting systems.

With the enforcement of this policy, Penabulu is committed to:

a. Protecting the rights and freedoms of every individual whose data we manage.

b. Integrating data protection into all stages of program planning and implementation.

c. Promoting an organizational culture that values privacy and information security.

This policy applies to all work units, projects, and activities involving the processing of personal data, whether in physical or digital form, across all operational locations of Penabulu Foundation.

2. PURPOSE

This policy aims to:

a. Establish high and consistent data protection standards across all Penabulu activities.

b. Protect the privacy rights of every individual whose data is managed by the organization.

c. Provide practical guidance for staff, partners, and third parties in handling personal data.

d. Menjamin kepatuhan terhadap semua peraturan perlindungan data yang berlaku.

d. Ensure compliance with all applicable data protection regulations.

3. RUANG LINGKUP

Kebijakan ini berlaku untuk seluruh individu dan entitas yang bekerja atas nama Penabulu, termasuk pengurus, staf tetap dan kontrak, relawan, konsultan, mitra pelaksana, serta vendor atau penyedia jasa.

Cakupan kebijakan meliputi semua bentuk data pribadi, baik yang disimpan secara fisik, digital, audio, maupun visual, dan mencakup seluruh siklus hidup data mulai dari pengumpulan, penyimpanan, penggunaan, transfer, hingga penghapusan.

3. SCOPE

This policy applies to all individuals and entities working on behalf of Penabulu, including board members, permanent and contract staff, volunteers, consultants, implementing partners, as well as vendors or service providers.

The scope of the policy covers all forms of personal data, whether stored physically, digitally, in audio, or visual formats, and includes the entire data lifecycle from collection, storage, use, transfer, through to deletion.

4. PRINSIP-PRINSIP PERLINDUNGAN DATA

Kami memproses data pribadi berdasarkan tujuh prinsip utama:

a. **Kepatuhan Hukum**
Semua pemrosesan data dilakukan dengan dasar hukum yang jelas, seperti persetujuan, pelaksanaan kontrak, atau kewajiban hukum.

b. **Transparansi**
Subjek data selalu diinformasikan mengenai tujuan, cara penggunaan, dan hak-hak mereka melalui Privacy Notice yang jelas.

c. **Minimasi Data**
Kami hanya mengumpulkan data yang benar-benar diperlukan untuk tujuan tertentu.

d. **Akurasi**
Kami memastikan data selalu benar, lengkap, dan diperbarui secara berkala.

4. DATA PROTECTION PRINCIPLES

We process personal data based on seven core principles:

a. **Lawfulness**
All data processing is carried out on a lawful basis, such as consent, contract fulfillment, or legal obligation.

b. **Transparency**
Data subjects are always informed of the purposes, methods of use, and their rights through clear Privacy Notices.

c. **Data Minimazation**
We only collect data that is strictly necessary for specific purposes.

d. **Accuracy**
We ensure that data is accurate, complete, and regularly updated.

e. **Batas Retensi**
Data hanya disimpan selama diperlukan, sesuai dengan Retention Schedule resmi.

f. **Akuntabilitas**
Kami mencatat semua aktivitas pemrosesan data dan siap diaudit kapan saja.

5. PERAN DAN TANGGUNG JAWAB

Perlindungan data adalah tanggung jawab bersama, namun dengan pembagian peran yang jelas:

a. **Direktur Eksekutif** bertanggung jawab penuh atas penerapan kebijakan ini dan penyediaan sumber daya yang diperlukan.

b. **Data Protection Officer (DPO)** mengawasi kepatuhan, menjadi penghubung dengan otoritas perlindungan data, dan mengelola Register Pemrosesan Data.

c. **Data Protection Focal Point (DPFP)** di setiap unit kerja memastikan kebijakan diterapkan sehari-hari, menjadi titik kontak untuk pelaporan insiden, dan menangani permintaan hak subjek data.

d. **Manajer Unit** mengendalikan hak akses staf dan memastikan pelatihan dijalankan.

e. **Tim IT** mengelola infrastruktur teknologi yang aman, melakukan backup rutin, dan memantau keamanan sistem.

f. **Seluruh Staf dan Mitra** wajib mematuhi kebijakan ini, menjaga kerahasiaan data, dan segera melaporkan setiap insiden.

e. **Security**
Data is retained only as long as necessary, in accordance with the official Retention Schedule.

f. **Accountability**
We document all data processing activities and remain audit-ready at all times.

5. ROLES AND RESPONSIBILITIES

Data protection is a shared responsibility, but with clearly defined roles:

a. The **Executive Director** is fully responsible for implementing this policy and providing necessary resources.

b. The **Data Protection Officer (DPO)** oversees compliance, acts as liaison with data protection authorities, and manages the Data Processing Register.

c. The **Data Protection Focal Point (DPFP)** in each work unit ensures daily implementation of the policy, serves as the contact point for incident reporting, and handles data subject rights requests.

d. **Unit Managers** control staff access rights and ensure required trainings are completed.

e. The **IT Team** manages secure technology infrastructure, performs routine backups, and monitors system security.

f. **All Staff and Partners** must comply with this policy, maintain data confidentiality, and immediately report any incidents.

g. **Vendor/Pihak Ketiga** hanya boleh memproses data berdasarkan perjanjian tertulis dan tunduk pada standar keamanan Penabulu.

6. PENGELOLAAN DATA

a. Pengumpulan Data
Setiap pengumpulan data harus memiliki dasar hukum yang sah. Untuk data sensitif seperti informasi kesehatan atau biometrik, diperlukan persetujuan tertulis yang jelas dari subjek data. Formulir pengumpulan wajib memuat Privacy Notice yang menjelaskan tujuan, dasar hukum, masa retensi, dan hak-hak subjek data.

b. Penyimpanan Data
Data digital disimpan di server aman dengan enkripsi AES-256 dan kontrol akses berbasis peran (role-based access control). Data fisik disimpan di lemari terkunci di ruangan dengan akses terbatas. Sistem penyimpanan cloud hanya digunakan jika penyedia memiliki sertifikasi keamanan seperti ISO 27001.

c. Penggunaan Data
Data hanya digunakan sesuai tujuan awal yang disetujui. **Setiap penggunaan data untuk tujuan baru memerlukan persetujuan ulang dari subjek data**. Penggunaan signifikan harus dicatat di Usage Log.

d. Pembaruan Data
Data diverifikasi dan diperbarui minimal satu kali setahun untuk menjaga akurasi.

e. Retensi dan Pemusnahan
Data disimpan sesuai jadwal retensi resmi. Setelah masa retensi berakhir, data digital dihapus secara permanen

g. **Vendors/Third** Parties may only process data based on a written agreement and are subject to Penabulu's security standards.

6. PENGELOLAAN DATA

a. Data Collection
All data collection must have a valid legal basis. For sensitive data such as health or biometric information, explicit written consent from the data subject is required. Collection forms must include a Privacy Notice explaining the purpose, legal basis, retention period, and data subject rights.

b. Data Storage
Digital data is stored on secure servers with AES-256 encryption and role-based access control. Physical data is stored in locked cabinets within restricted-access rooms. Cloud storage systems may only be used if the provider holds security certifications such as ISO 27001.

c. Data Use
Data may only be used for the original approved purposes. **Any new purpose of use requires renewed consent from the data subject.** Significant uses must be recorded in the Usage Log.

d. Data Updating
Data is verified and updated at least once a year to maintain accuracy.

e. Retention and Disposal
Data is retained according to the official retention schedule. Once the retention period expires, digital data is

(secure delete), sedangkan data fisik dimusnahkan dengan penghancur dokumen (cross-cut shredder) atau metode pembakaran aman.

permanently deleted (secure delete), while physical data is destroyed using a cross-cut shredder or safe burning methods.

Daftar Retensi Dokumen Organisasi / *Organizational Document Retention Schedule*

1. Dokumen Korporasi & Legal / *Corporate & Legal Documents*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Akta pendirian & perubahan	Permanen	Kewajiban hukum	Arsip permanen
Deed of establishment & amendments	*Permanent*	*Legal obligation*	*Permanent archive*
Izin usaha, registrasi organisasi	Selama berlaku + 5 tahun	Regulasi izin usaha	Arsip / musnahkan
Business licenses, organizational registrations	*Validity period + 5 years*	*Licensing regulations*	*Archive/Dispose*
Perjanjian & kontrak dengan pihak ketiga	Masa berlaku + 5 tahun	KUHPerdata, risiko hukum	Musnahkan / arsip digital
Agreements & contracts with third parties	*Validity period + 5 years*	*Civil Code, legal risk*	*Dispose /Digital Archive*
Kebijakan & SOP internal	Selama berlaku + 5 tahun setelah revisi	Tata kelola organisasi	Arsipkan digital
Internal policies & SOPs	*Validity period + 5 years*	*Organizational governance*	*Digital archive*

2. Dokumen Keuangan & Pajak / *Financial & Tax Documents*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Laporan keuangan tahunan	10 tahun	UU Perpajakan	Arsipkan digital, fisik bisa dimusnahkan
Annual financial reports	*10 Years*	*Tax Law*	*Digital archive, physical copies may be disposed*
Bukti transaksi (invoice, kwitansi, bukti transfer)	10 tahun	UU Perpajakan	Musnahkan setelah periode

Transaction evidence (invoices, receipts, transfer proofs)	*10 Years*	*Tax Law*	*Dispose after period*
Laporan audit eksternal	10 tahun	Regulasi akuntansi	Arsipkan
External audit reports	*10 Years*	*Accounting Regulations*	*Archive*
Laporan pajak & bukti setoran	10 tahun	UU Perpajakan	Musnahkan setelah periode
Tax reports & payment receipts	*10 Years*	*Tax Law*	*Dispose after period*

3. Dokumen Sumber Daya Manusia (HR) / *Human Resources (HR) Documents*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Data personal staf (CV, identitas)	5 tahun setelah resign	UU Ketenagakerjaan, UU PDP	Hapus / musnahkan
Staff personal data (CV, identification)	*5 years after resignation*	*Labor Law, PDP Law*	*Delete / Dispose*
Kontrak kerja & perjanjian PKWT	Masa berlaku + 5 tahun	UU Ketenagakerjaan	Musnahkan
Employment contracts & fixed-term agreements	*Validity period + 5 years*	*Labor Law*	*Dispose*
Evaluasi kinerja & catatan disiplin	5 tahun setelah resign	Praktik HR	Hapus
Performance evaluations & disciplinary records	*5 years after resignation*	*HR practice*	*Delete*
Payroll, slip gaji, BPJS	5–10 tahun	UU Pajak & Ketenagakerjaan	Musnahkan
Payroll, payslips, social security (BPJS)	*5–10 years*	*Tax & Labor Law*	*Dispose*
Data kesehatan kerja / medical check up	5–10 tahun	Aturan K3	Hapus / musnahkan
Payroll, payslips, social security (BPJS)	*5–10 years*	*CHS regulations*	*Delete / Dispose*

4. Dokumen Program / Proyek / *Program / Project Documents*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Proposal proyek	5 tahun setelah proyek selesai	Praktik donor/organisasi	Arsipkan digital
Project proposals	*5 years after project completion*	*Donor/organizational practice*	*Digital archive*
Laporan donor (narrative, financial)	5–10 tahun	Ketentuan donor	Arsipkan digital
Donor reports (narrative, financial)	*5–10 years*	*Donor requirements*	*Digital archive*
Monitoring & Evaluasi (Monev)	5 tahun setelah proyek selesai	Praktik NGO	Arsipkan digital
Monitoring & Evaluation (M&E)	*5 years after project completion*	*NGO practice*	*Digital archive*
Data penerima manfaat	Selama proyek + 2 tahun	UU PDP, donor	Hapus/anonymize
Beneficiaries data	*Project duration + 2 years*	*PDP Law, donor*	*Delete / anonymize*

5. Administrasi & Komunikasi / *Administration and Communication*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Notulen rapat manajemen	Permanen	Tata kelola	Arsip permanen
Management meeting minutes	*Permanent*	*Governance*	*Permanent archive*
Notulen rapat staf rutin	3 tahun	Praktik organisasi	Hapus
Regular staff meeting minutes	*3 Years*	*Organizational practice*	*Delete*
Surat masuk/keluar	5 tahun	Praktik umum arsip	Arsip digital, musnahkan fisik
Incoming/outgoing correspondence	*5 Years*	*Common archiving practice*	*Digital archive, dispose physical copies*
Email kerja staf	6 bulan setelah resign	Praktik IT + PDP/GDPR	Hapus/anonymize
Staff work emails	*6 months after resignation*	*IT practice + PDP/GDPR*	*Delete / anonymize*
Chat/korespondensi internal	1 – 2 tahun	Praktik komunikasi	Hapus

(Teams/Slack/WA resmi)			
Internal chats/correspondence (Teams/Slack/Official WA)	1 – 2 *Years*	*Communication practice*	*Delete*

6. IT & Data Digital / *IT & Digital Data*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Log akses sistem (login, penggunaan)	1 – 2 tahun	Praktik keamanan TI	Hapus/anonymize
System access logs (login, usage)	1 – 2 *Years*	*IT security practice*	*Delete / anonymize*
Backup server/email	6 bulan – 1 tahun	Praktik keamanan TI	Overwrite / hapus
Server/email backups	*6 months – 1 year*	*IT security practice*	*Overwrite / delete*
Data pengguna (akun staf)	Maks. 6 bulan setelah resign	UU PDP/GDPR	Hapus/anonymize
User data (staff accounts)	*Max. 6 months after resignation*	*PDP/GDPR Law*	*Delete / anonymize*
Password, credential, token	Selama berlaku	Praktik keamanan TI	Hapus segera setelah tidak berlaku
Passwords, credentials, tokens	*Validity period*	*IT security practice*	*Delete immediately once invalid*

7. Dokumentasi & Publikasi / *Documentation & Publication*

Jenis Dokumen *Document Type*	Retensi *Retention*	Dasar Hukum / Catatan *Legal Basis / Notes*	Tindakan Akhir *Final Action*
Laporan tahunan organisasi	Permanen	Arsip historis	Arsip permanen
Annual organizational reports	*Permanent*	*Historical archive*	*Permanent archive*
Publikasi, artikel, hasil riset	Permanen	Knowledge management	Arsip permanen
Publications, articles, research outputs	*Permanent*	*Knowledge management*	*Permanent archive*
Foto & video kegiatan	Selama relevan + 5 tahun	UU PDP (jika ada identitas individu)	Arsipkan / hapus sesuai izin
Activity photos & videos	*As long as relevant + 5 years*	*PDP Law (if identifiable individuals)*	*Archive / delete based on consent*

f. Akses dan Kontrol Internal

i. Akses ke data pribadi hanya diberikan berdasarkan prinsip least privilege (sebatas kebutuhan pekerjaan).
ii. Semua aktivitas akses dicatat dalam audit log dan ditinjau secara berkala.
iii. Penggunaan perangkat pribadi untuk mengakses data organisasi harus mengikuti prosedur keamanan BYOD (Bring Your Own Device).

g. Anonimisasi dan Pseudonimisasi

i. Data yang digunakan untuk keperluan analisis, riset, atau publikasi eksternal harus dianonimkan atau dipseudonimkan untuk mengurangi risiko identifikasi individu.
ii. Standar teknis anonimisasi ditetapkan oleh Tim IT dan disetujui oleh DPO.

h. Data Pribadi Sensitif (Special Category Data)

i. Data sensitif (misalnya kesehatan, orientasi seksual, keyakinan agama, data biometrik) hanya boleh diproses dengan persetujuan eksplisit dan perlindungan tambahan.
ii. Penyimpanan data sensitif wajib menggunakan enkripsi kuat, serta akses terbatas hanya untuk staf berwenang.

i. Transfer Internal & Tracking

i. Setiap pemindahan data antar-unit dicatat dalam Data Transfer Log untuk menjamin akuntabilitas.

f. Internal Access and Control

i. Access to personal data is granted solely based on the principle of least privilege (limited to operational necessity).
ii. All access activities are recorded in an audit log and reviewed periodically.
iii. The use of personal devices to access organizational data must comply with BYOD (Bring Your Own Device) security procedures.

g. Anonymization and Pseudonymization

i. Data used for analysis, research, or external publications must be anonymized or pseudonymized to reduce the risk of individual identification.
ii. Technical standards for anonymization are defined by the IT Team and approved by the DPO.

h. Sensitive Personal Data (Special Category Data)

i. Sensitive data (e.g., health, sexual orientation, religious beliefs, biometric data) may only be processed with explicit consent and additional safeguards.
ii. Storage of sensitive data must use strong encryption, with access restricted to authorized personnel only.

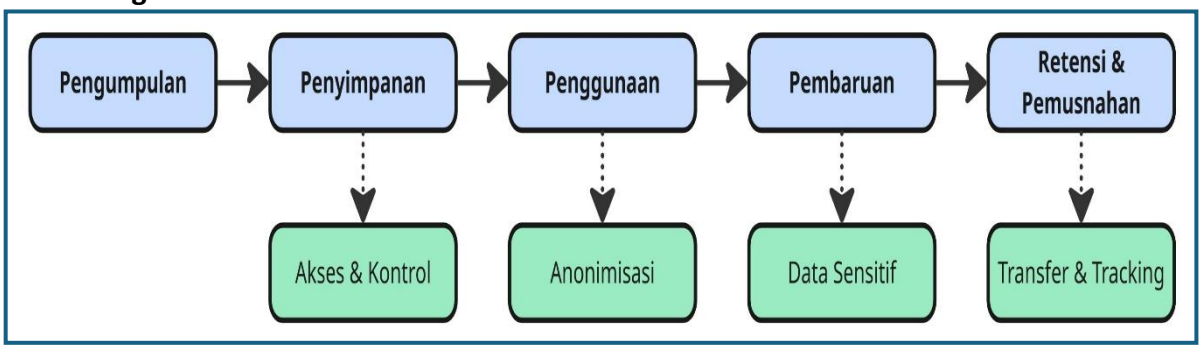
i. Internal Transfers & Tracking

i. All data transfers between units must be logged in the Data Transfer Log to ensure accountability.

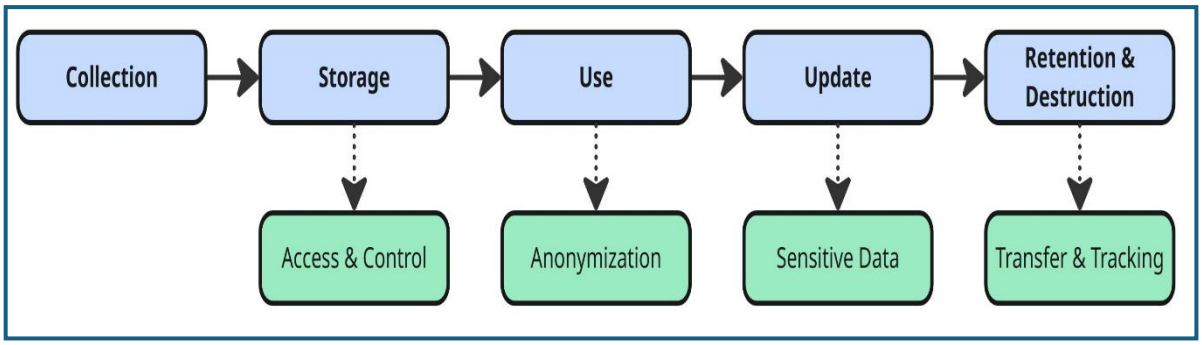
ii. Sistem LOPO digunakan sebagai kanal resmi pertukaran dokumen/data, untuk mencegah penggunaan media tidak aman (misalnya email pribadi atau perangkat eksternal tidak terenkripsi).

ii. The LOPO system is used as the official channel for document/data exchange to prevent the use of insecure media (e.g., personal email or unencrypted external devices).

Alur Pengelolaan Data



Data Managemet Flow



a. **Alur Utama di Atas (biru muda):**
   i. Menunjukkan siklus hidup data pribadi: **Pengumpulan → Penyimpanan → Penggunaan → Pembaruan → Retensi & Pemusnahan.**
   ii. Ini adalah jalur standar bagaimana data pribadi dikelola dari awal hingga akhir.
   iii. Kotak Hijau di Bawah (kontrol tambahan):
   iv. Bukan tahap alur, tapi **aturan/pengaman** yang **selalu melekat** pada tahap penyimpanan & penggunaan.

a. **Explanation of Main Flow (light blue):**
   i. Shows the lifecycle of personal data: **Collection → Storage → Use → Updating → Retention & Disposal**
   ii. This is the standard pathway for how personal data is managed from beginning to end.
   iii. Explanation of Supporting Boxes (green):
   iv. These are not flow stages, but **permanent controls** that **apply mainly** during storage & use.

v. Jadi, panah putus-putus dari kotak atas ke bawah artinya: setiap tahap itu **harus memperhatikan kontrol tambahan.**

b. **Penyimpanan → Akses & Kontrol (🔑):**
Data yang disimpan harus diatur siapa yang boleh mengakses (hanya orang tertentu, prinsip least privilege).

c. **Penggunaan → Anonimisasi (🙈):**
Kalau data dipakai untuk analisis/publikasi, identitas harus dihapus agar tidak melanggar privasi.

d. **Penggunaan → Data Sensitif (⚠️):**
Jika data yang digunakan sensitif (kesehatan, biometrik, agama), ada aturan khusus: enkripsi, persetujuan eksplisit.

e. **Pembaruan/Retensi → Transfer & Tracking (📩):**
Kalau data dipindahkan antar-unit, harus tercatat di data transfer log supaya akuntabel

7. HAK SUBJEK DATA

Kami menjamin hak-hak berikut bagi setiap subjek data:

a. Hak untuk mengakses salinan data pribadi mereka.
b. Hak untuk memperbaiki data yang tidak akurat.
c. Hak untuk menghapus data yang tidak lagi relevan.
d. Hak untuk membatasi pemrosesan data.
e. Hak untuk menolak pemrosesan data untuk tujuan tertentu.

v. The dashed arrows from the upper boxes indicate that **each stage must consider these additional controls.**

b. **Storage → Access & Control (🔑):**
Stored data must be governed by strict access rights (only specific persons under the least privilege principle).

c. **Use → Anonymization (🙈):**
When data is used for analysis/publication, identities must be removed to avoid privacy violations.

d. **Use → Sensitive Data (⚠️):**
If the data is sensitive (health, biometrics, religion), special requirements apply: encryption, explicit consent.

e. **Updating/Retention → Transfer & Tracking (📩):**
If data is transferred between units, the transfer must be recorded in the Data Transfer Log for accountability.

7. DATA SUBJECT RIGHTS

We guarantee the following rights for each data subject:

a. The right to access a copy of their personal data.
b. The right to correct inaccurate personal data.
c. The right to delete data that is no longer relevant.
d. The right to restrict the processing of data.
e. The right to object to data processing for specific purposes.

f. Hak untuk memindahkan data ke pihak lain (data portability).
g. Hak untuk menerima pemberitahuan jika terjadi pelanggaran data yang berisiko tinggi.

Setiap permintaan hak subjek data harus diajukan secara tertulis, diverifikasi identitasnya, dan diproses dalam waktu maksimal 14 hari kerja.

a. Mekanisme Permintaan Hak Subjek Data

i. Permintaan harus diajukan secara tertulis (email resmi, formulir internal, atau surat).
ii. Identitas pemohon diverifikasi melalui dokumen sah atau mekanisme otentikasi sebelum diproses.
iii. Semua permintaan dicatat dalam Data Subject Request Log oleh DPFP.

b. Batas Waktu dan Proses

i. Permintaan diproses dalam waktu maksimal 14 hari kerja (mengikuti kebijakan Penabulu) atau 30 hari kalender untuk keselarasan dengan GDPR.
ii. Jika membutuhkan perpanjangan waktu, subjek data akan diberitahu alasan keterlambatan.

c. Penolakan Permintaan

i. Permintaan dapat ditolak bila:
   - Mengganggu hak dan kebebasan pihak lain.
   - Bertentangan dengan kewajiban hukum (misalnya data wajib disimpan untuk audit/otoritas).
ii. Penolakan harus disertai alasan tertulis kepada subjek data.

f. The right to transfer data to another party (data portability).
g. The right to receive notification if a high-risk data breach occurs.

All data subject requests must be submitted in writing, identity-verified, and processed within a maximum of 14 working days.

a. Mechanism for Data Subject Rights Requests

i. Requests must be submitted in writing (official email, internal form, or letter).
ii. The requester's identity must be verified through valid documents or authentication mechanisms before processing.
iii. All requests must be logged in the Data Subject Request Log by the DPFP.

b. Timeframes and Process

i. Requests are processed within 14 working days (following Penabulu policy) or 30 calendar days for GDPR alignment.
ii. If an extension is required, the data subject will be informed of the reason for the delay.

c. Request Rejection

i. A request may be rejected if:
   - It interferes with the rights and freedoms of others.
   - It contradicts legal obligations (e.g., data must be retained for audit or authority compliance).
ii. Penolakan harus disertai alasan tertulis kepada subjek data.

d. Saluran Pengaduan

i. Jika subjek data tidak puas dengan tanggapan, mereka dapat mengajukan keberatan ke DPO Yayasan Penabulu.

ii. Subjek data juga berhak mengajukan keluhan langsung ke otoritas perlindungan data nasional sesuai UU No. 27/2022.

d. Complaint Channels

i. If the data subject is not satisfied with the response, they may file an objection to the DPO of Penabulu Foundation.

ii. Data subjects also have the right to file a complaint directly to the national data protection authority under Law No. 27/2022.

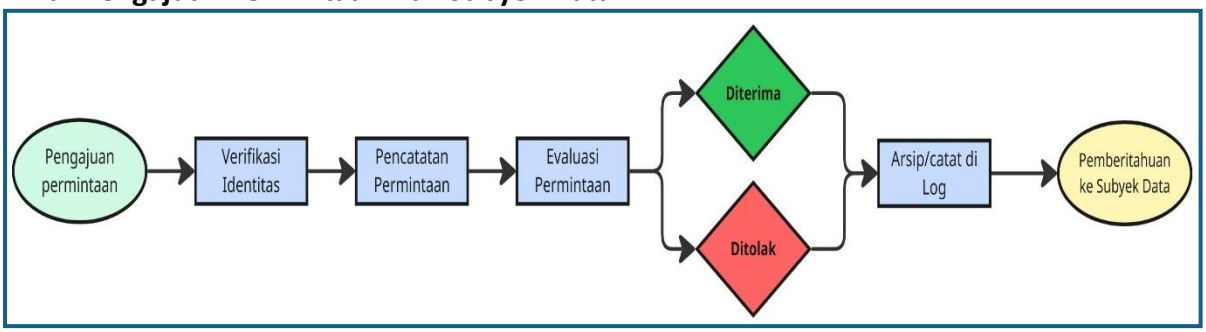
e. Hak atas Informasi dalam Proses Otomatis

i. Jika ada keputusan berbasis automated processing (misalnya profil risiko, seleksi otomatis), subjek data berhak meminta penjelasan, menolak, atau meminta intervensi manusia.

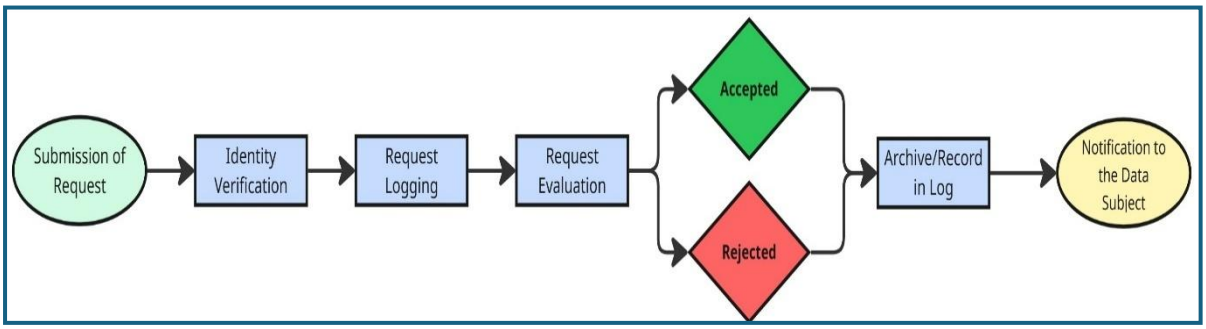
e. Rights Regarding Automated Processing

i. If there is a decision based on automated processing (e.g., risk profiling, automated selection), the data subject has the right to request an explanation, object, or request human intervention.

Alur Pengajuan Permintaan Hak Subyek Data



Data Subject Rights Request Flow



8. TRANSFER DATA

Transfer data internal mengikuti prinsip minimasi dan keamanan. Transfer kepada pihak ketiga hanya dilakukan berdasarkan perjanjian tertulis yang memuat ketentuan kerahasiaan dan keamanan data. Transfer internasional hanya dilakukan jika negara penerima memiliki tingkat perlindungan data yang setara atau lebih tinggi, terdapat Data Transfer Agreement, dan persetujuan tertulis dari subjek data telah diperoleh.

a. Klasifikasi dan Jenis Transfer

i. Internal Transfer: perpindahan data antar unit, proyek, atau cabang Penabulu → wajib dicatat dalam Data Transfer Log.
ii. Eksternal Transfer: kepada mitra, donor, vendor, atau otoritas hukum → wajib melalui perjanjian resmi (Data Processing Agreement/Data Sharing Agreement).
iii. Cross-Border Transfer: ke luar negeri → hanya jika negara penerima memiliki adequacy decision atau perlindungan setara.

b. Mekanisme Keamanan Transfer

i. Transfer digital harus menggunakan saluran terenkripsi (misalnya SFTP, VPN, atau platform cloud bersertifikat ISO 27001).
ii. Larangan keras penggunaan email pribadi, media penyimpanan tidak terenkripsi, atau aplikasi pesan instan tidak resmi.
iii. Transfer fisik (dokumen/arsip) harus menggunakan kurir

8. DATA TRANSFER

Internal data transfers follow the principles of minimization and security. Transfers to third parties are only conducted based on a written agreement that includes confidentiality and data security provisions. International transfers are only permitted if the receiving country provides an equal or higher level of data protection, a Data Transfer Agreement is in place, and written consent from the data subject has been obtained.

a. Classification and Types of Transfers

i. Internal Transfer: movement of data between Penabulu units, projects, or branches → must be recorded in the Data Transfer Log.
ii. External Transfer: to partners, donors, vendors, or legal authorities → must follow official agreements (e.g., Data Processing Agreement / Data Sharing Agreement).
iii. Cross-Border Transfer: overseas transfers → only allowed if the receiving country has an adequacy decision or equivalent protections.

b. Transfer Security Mechanisms

i. Digital transfers must use encrypted channels (e.g., SFTP, VPN, or ISO 27001-certified cloud platforms).
ii. Strict prohibition on using personal email, unencrypted media storage, or unofficial messaging applications.
iii. Physical transfers (documents/archives) must use trusted couriers with security seals.

terpercaya dengan segel keamanan.

c. Prinsip Need-to-Know dan Minimasi Data

i. Hanya data minimum yang dibutuhkan yang boleh ditransfer.
ii. Sebelum transfer, dilakukan Data Transfer Risk Assessment untuk menilai risiko kebocoran atau penyalahgunaan.

d. Dokumentasi dan Transparansi

i. Semua transfer data dicatat dalam Transfer Register yang dikelola oleh DPO.
ii. Subjek data diinformasikan jika datanya ditransfer ke pihak ketiga, terutama bila lintas negara.

e. Kewajiban Pihak Ketiga

i. Pihak ketiga penerima data wajib:
   - Menyediakan bukti mekanisme keamanan yang memadai.
   - Menandatangani kontrak perlindungan data sesuai GDPR/UU PDP.
   - Tidak melakukan sub-transfer tanpa izin tertulis Penabulu.

f. Audit & Review Transfer

i. Audit tahunan untuk mengevaluasi kepatuhan semua pihak terhadap perjanjian transfer.
ii. Review rutin terhadap vendor atau mitra yang menerima data untuk memastikan standar keamanan tetap berlaku.

c. Need-to-Know and Data Minimization Principle

i. Only the minimum necessary data may be transferred.
ii. Before transfer, a Data Transfer Risk Assessment must be conducted to evaluate leakage or misuse risks.

d. Documentation and Transparency

i. All data transfers must be recorded in the Transfer Register managed by the DPO.
ii. Data subjects must be informed if their data is transferred to third parties, especially for cross-border transfers.

e. Obligations of Third Parties

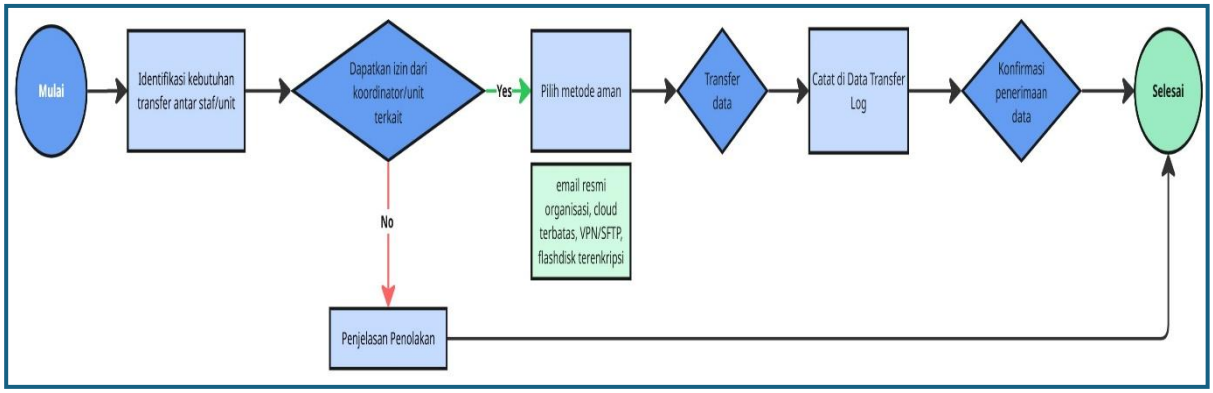
i. Third-party data recipients are required to:
   - Provide evidence of adequate security mechanisms.
   - Sign a data protection contract in accordance with GDPR / PDP Law.
   - Not conduct sub-transfers without Penabulu's written approval.

f. Transfer Audit & Review

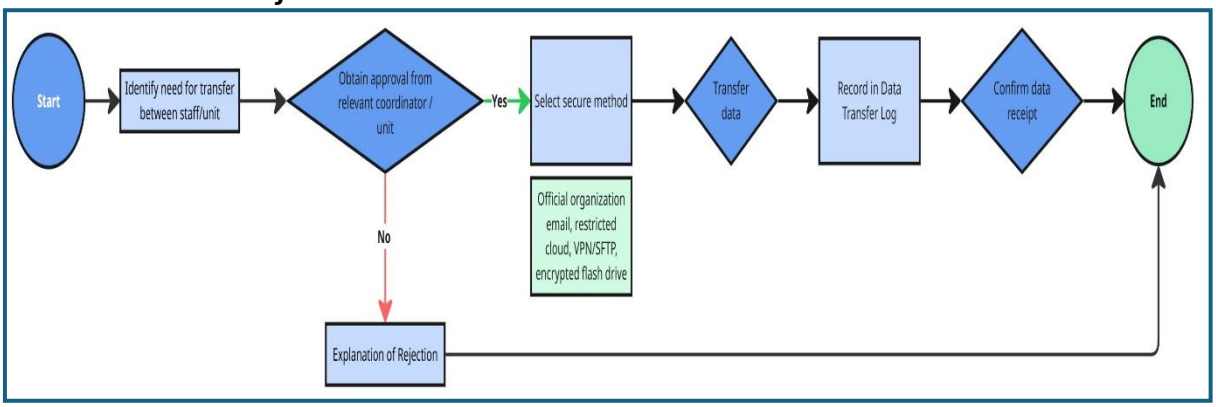
i. Annual audits to evaluate parties' compliance with transfer agreements.
ii. Regular reviews of vendors or partners receiving data to ensure security standards remain enforced.

PENABULU

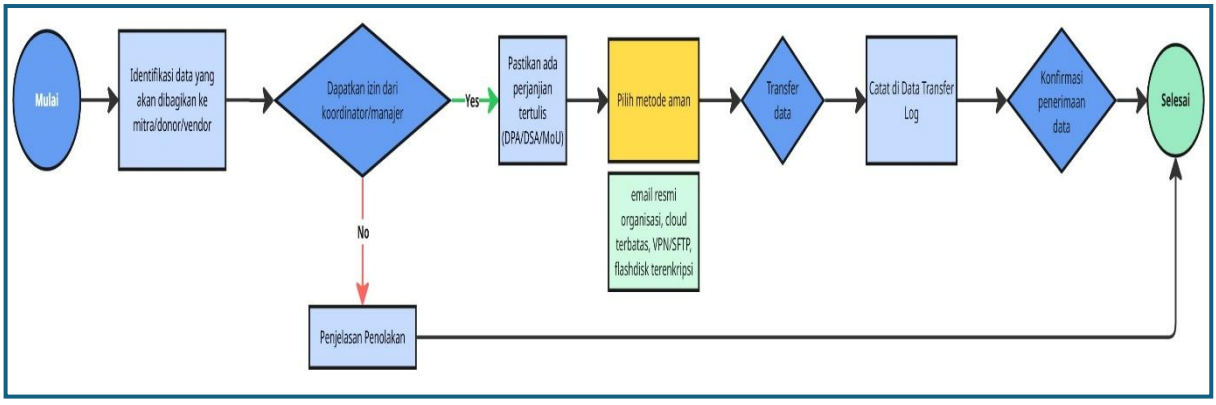
Alur transfer data Internal



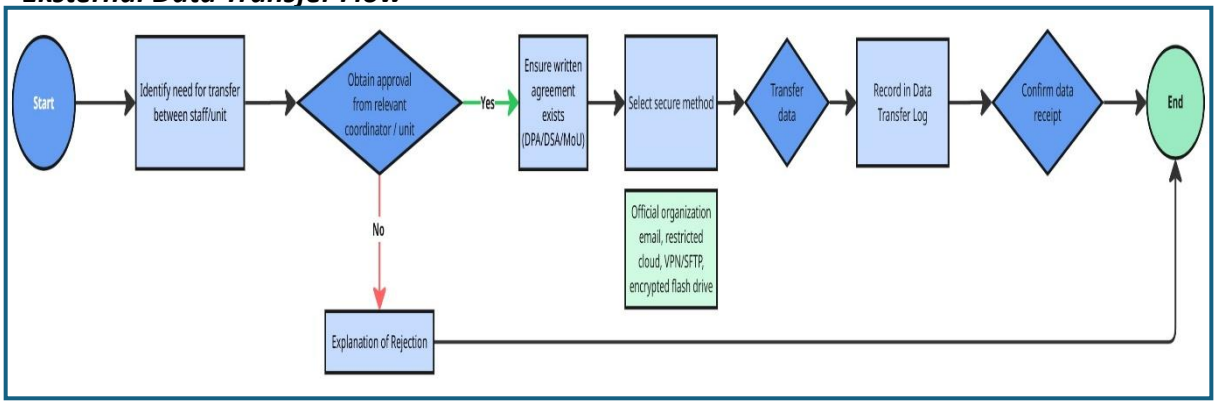
Internal Data Transfer Flow



Alur transfer data Eksternal



Eksternal Data Transfer Flow



1. **Transfer Data Internal**

Mulai
→ Identifikasi kebutuhan transfer antar staf/unit
→ Dapatkan izin dari koordinator/unit terkait
→ Pilih metode aman (email resmi organisasi, cloud terbatas, VPN/SFTP, flashdisk terenkripsi)
→ Transfer data
→ Catat di **Data Transfer Log**
→ Konfirmasi penerimaan data
Selesai

2. **Transfer Data Eksternal**

Mulai
→ Identifikasi data yang akan dibagikan ke mitra/donor/vendor
→ Dapatkan persetujuan dari koordinator/manajer
→ Pastikan ada perjanjian tertulis **(DPA/DSA/MoU)**
→ Pilih metode aman (folder cloud resmi, akses terbatas, dokumen fisik tersegel)
→ Transfer data
→ Catat di Data Transfer Log
→ Konfirmasi penerimaan data
Selesai

9. KEAMANAN DATA

a. **Keamanan Fisik**
   i. **Kontrol Akses Ruangan:**
      - Hanya staf berwenang yang dapat masuk ke ruang penyimpanan data.
      - Akses diatur dengan kunci elektronik, kartu identitas, atau sidik jari.

1. **Internal Data Transfer**

Start
→ Identify need for transfer between staff/unit
→ Obtain approval from relevant coordinator/unit
→ Select secure method (official organizational email, restricted cloud, VPN/SFTP, encrypted flash drive)
→ Transfer data
→ Record in **Data Transfer Log**
→ Confirm data receipt
End

2. **External Data Transfer**

Start
→ Identify data to be shared with partner/donor/vendor
→ Obtain approval from coordinator/manager
→ Ensure written agreement exists **(DPA/DSA/MoU)**
→ Select secure method (official cloud folder, restricted access, sealed physical documents)
→ Transfer data
→ Record in **Data Transfer Log**
→ Confirm data receipt
End

9. DATA SECURITY

a. **Physical Security**
   i. **Room Access Control:**
      - Only authorized staff may enter data storage rooms.
      - Access is regulated through electronic locks, ID cards, or biometric authentication.

ii. **Penyimpanan Arsip Fisik:**
- Arsip disimpan di lemari besi/lemari terkunci dengan log akses.
- Dokumen sensitif (misalnya data kesehatan, investigasi) diberi label "Confidential" dan dipisahkan dari arsip umum.

iii. **Sistem Pengawasan**
- Area dengan data sensitif dilengkapi CCTV 24/7 dengan rekaman disimpan minimal 90 hari.
- Pengawasan manual dilakukan secara berkala oleh staf keamanan.

iv. **Proteksi Bencana:**
- Ruang arsip dilengkapi sensor kebakaran, sistem pemadam otomatis, dan perlindungan dari banjir atau kelembaban berlebih.

b. **Keamanan Digital**

i. **Enkripsi:**
- Data disimpan dengan enkripsi minimal AES-256 dan dikirim melalui protokol aman (TLS 1.3 atau setara).

ii. **Autentikasi & Akses:**
- Seluruh akun staf dilindungi Multi-Factor Authentication (MFA).
- Prinsip least privilege diterapkan: akses hanya sesuai peran.
- Password dikelola dengan kebijakan kuat (minimal 12 karakter, kombinasi huruf,

ii. **Physical Archive Storage:**
- Archives are stored in a safe/locked cabinet with an access log.
- Sensitive documents (e.g., health data, investigations) are labeled "Confidential" and separated from general archives.

iii. **Surveillance Systems:**
- Areas containing sensitive data are equipped with 24/7 CCTV with recordings retained for at least 90 days.
- Manual supervision is periodically conducted by security personnel.

iv. **Disaster Protection:**
- Archive rooms are equipped with fire detectors, automatic extinguishing systems, and protection against floods or excessive humidity.

b. **Digital Security**

i. **Encryption:**
- Data must be stored using a minimum of AES-256 encryption and transmitted via secure protocols (TLS 1.3 or equivalent).

ii. **Authentication & Access:**
- All staff accounts must use Multi-Factor Authentication (MFA).
- The principle of least privilege applies: access must align with job roles.
- Passwords must comply with strong policy requirements (minimum 12 characters, mix

angka, simbol) dan diperbarui setiap 90 hari.

iii. **Backup & Recovery:**
- Backup dilakukan setiap minggu, disimpan di lokasi terpisah (on-premise dan cloud).
- Uji pemulihan (restore test) dilakukan minimal 2 kali setahun.

iv. **Monitoring & Logging:**
- Semua akses ke data sensitif dicatat dalam audit log.
- Log ditinjau secara rutin oleh Tim IT dan DPO.
- Sistem deteksi intrusi (IDS/IPS) digunakan untuk memantau serangan siber.

c. **Keamanan Pihak Ketiga**

i. **Evaluasi Keamanan (Due Diligence):**
- Sebelum bekerja sama, vendor wajib mengisi Vendor Security Assessment Form.
- Penilaian mencakup sertifikasi keamanan (ISO 27001, SOC 2, atau setara), enkripsi, serta prosedur insiden mereka.

ii. **Perjanjian Pemrosesan Data (Data Processing Agreement – DPA):**
- DPA wajib ditandatangani sebelum vendor dapat mengakses atau memproses data.
- DPA harus mencakup klausul: kerahasiaan, retensi data, mekanisme audit, serta

of letters, numbers, symbols) and be updated every 90 days.

iii. **Backup & Recovery:**
- Backups must be performed weekly and stored in separate locations (on-premise and cloud).
- Recovery tests must be conducted at least twice a year.

iv. **Monitoring & Logging:**
- All access to sensitive data must be recorded in audit logs.
- Logs must be routinely reviewed by the IT Team and the DPO.
- Intrusion Detection/Prevention Systems (IDS/IPS) must be used to monitor cyber-attacks.

c. **Third-Party Security**

i. **Security Evaluation (Due Diligence):**
- Before collaboration, vendors must complete the Vendor Security Assessment Form.
- Evaluation includes security certifications (ISO 27001, SOC 2, or equivalent), encryption, and incident response procedures.

ii. **Data Processing Agreement (DPA):**
- A DPA must be signed before a vendor can access or process data.
- The DPA must include clauses on confidentiality, data retention, audit mechanisms, and incident reporting obligations within 72 hours.

kewajiban pelaporan insiden maksimal 72 jam.

iii. **Monitoring Vendor:**
- Audit vendor dilakukan minimal setahun sekali.
- Vendor dengan akses kritis harus menyediakan bukti kepatuhan keamanan secara berkala.

iv. **Sub-kontraktor:**
- Vendor tidak boleh menyerahkan data kepada pihak ketiga lain tanpa persetujuan tertulis Yayasan Penabulu**.**

d. Alur Keamanan Data Penabulu

1. Keamanan Fisik

→ Batasi akses ruangan penyimpanan data (hanya staf berwenang, gunakan kunci/kartu/sidik jari).
→ Simpan arsip di lemari terkunci; dokumen sensitif diberi label **Rahasia**
→ Area sensitif diawasi dengan CCTV / patroli staf keamanan.
→ Ruang arsip dilengkapi proteksi bencana (sensor asap, APAR, anti-lembap).

2. Keamanan Digital

→ Simpan data dengan enkripsi (AES-256).
→ Kirim data melalui protokol aman (TLS/SFTP/VPN).
→ Lindungi akun staf dengan **MFA** & password kuat (12 karakter, kombinasi).
→ Terapkan prinsip **least privilege** (akses sesuai peran).

iii. **Vendor Monitoring:**
- Vendor audits must be conducted at least annually.
- Vendors with critical access must provide periodic proof of security compliance.

iv. **Sub-contractors:**
- Vendors may not transfer data to third parties without written approval from Yayasan Penabulu.

d. Penabulu Data Security Flow

1. Physical Security

→ Restrict access to data storage rooms (authorized staff only, using locks/cards/biometrics).
→ Store archives in locked cabinets; sensitive documents labeled **Confidential.**
→ Sensitive areas monitored with CCTV / security patrols.
→ Archive rooms equipped with disaster protection (smoke detectors, extinguishers, humidity control).

2. Digital Security

→ Store data with encryption (AES-256).
→ Transmit data via secure protocols (TLS/SFTP/VPN).
→ Protect staff accounts with **MFA** & strong passwords (12 characters, mix).
→ Apply **least privilege** principle (role-based access).

→ Backup data mingguan → simpan di lokasi berbeda (lokal & cloud).
→ Uji restore data 2x setahun.
→ Catat semua akses di audit log.
→ Tim IT & DPO rutin meninjau log + aktifkan sistem deteksi serangan (IDS/IPS).

→ Weekly data backups → stored in separate locations (local & cloud).
→ Conduct restore tests twice per year.
→ Log all sensitive access in audit logs.
→ IT Team & DPO periodically review logs + enable intrusion detection systems (IDS/IPS).

3. **Keamanan Pihak Ketiga**
   → Evaluasi vendor dengan Vendor Security Assessment Form.
   → Pastikan ada sertifikasi keamanan / standar (ISO 27001, SOC 2, dsb.).
   → Tanda tangani **Data Processing Agreement (DPA)** sebelum akses data.
   → Pastikan klausul DPA mencakup: kerahasiaan, retensi data, audit, laporan insiden ≤ 72 jam.
   → Audit vendor minimal 1x setahun.
   → Larangan: vendor tidak boleh sub-kontrak data tanpa izin tertulis Penabulu.

3. **Third-Party Security**
   → Evaluate vendors using Vendor Security Assessment Form.
   → Verify certifications/standards (ISO 27001, SOC 2, etc.).
   → Sign a **Data Processing Agreement (DPA)** before granting data access.
   → Ensure DPA includes: confidentiality, retention, audit, incident report ≤ 72 hours.
   → Audit vendors at least once a year.
   → Restriction: vendors may not subcontract data without Penabulu's written approval.

10. PENANGANAN INSIDEN DATA

Jika terjadi insiden seperti kehilangan perangkat, kebocoran data, atau akses tidak sah, staf wajib melapor ke DPFP dalam waktu maksimal 2 jam. DPFP kemudian melapor ke DPO dalam 24 jam. DPO akan menilai tingkat risiko dan, jika insiden berdampak tinggi, memberi tahu otoritas perlindungan data dalam waktu maksimal 72 jam. Semua insiden dicatat dalam Incident Log dan dianalisis untuk mencegah terulangnya kejadian.

a. **Definisi Insiden Data**
   Insiden data mencakup antara lain:
   i. Kehilangan perangkat (laptop, USB, ponsel) yang berisi data pribadi.

10. HANDLING OF DATA INCIDENTS

If an incident occurs such as device loss, data breach, or unauthorized access, staff must report to the DPFP within a maximum of 2 hours. The DPFP then reports to the DPO within 24 hours. The DPO will assess the risk level and, if the incident has high impact, notify the data protection authority within a maximum of 72 hours. All incidents must be recorded in the Incident Log and analyzed to prevent recurrence.

a. **Definition of Data Incidents**
   Data incidents include, among others:
   i. Loss of devices (laptops, USB drives, mobile phones) containing personal data.

ii. Akses tidak sah atau pencurian akun.
iii. Kebocoran data melalui email, cloud, atau sistem internal.
iv. Serangan siber (malware, phishing, ransomware).
v. Kesalahan internal (misalnya mengirim data ke penerima yang salah).

ii. Unauthorized access or account theft.
iii. Cyber-attacks (malware, phishing, ransomware).
iv. Internal errors (e.g., sending data to the wrong recipient).

b. Prosedur Pelaporan Awal

i. **Waktu Pelaporan:** Setiap staf wajib melaporkan ke Data Protection Focal Point (DPFP) dalam maksimal 2 jam sejak mengetahui insiden.
ii. **Media Pelaporan:** Telepon darurat, email resmi insiden (misalnya incident@penabulu.org), atau formulir digital khusus.
iii. **Isi Laporan Awal:** Jenis insiden, lokasi, sistem/akun terdampak, data yang mungkin terlibat.

b. Initial Reporting Procedure

i. **Reporting Time:** Each staff member must report to the Data Protection Focal Point (DPFP) within a maximum of 2 hours after becoming aware of the incident.
ii. **Reporting Channels:** Emergency phone, official incident email (e.g., incident@penabulu.org), or a dedicated digital form.
iii. **Initial Report Content:** Type of incident, location, affected system/account, and potentially involved data.

c. Tindak Lanjut DPFP

i. Memvalidasi laporan insiden dalam waktu 4 jam.
ii. Mengambil langkah darurat (first aid), misalnya menonaktifkan akun, memutus akses jaringan, atau mengamankan perangkat.
iii. Melaporkan ke Data Protection Officer (DPO) dalam waktu 24 jam dengan ringkasan awal.

c. DPFP Follow-up Actions

i. Validate the reported incident within 4 hours.
ii. Take emergency (first aid) measures such as disabling accounts, cutting off network access, or securing devices.
iii. Report to the Data Protection Officer (DPO) within 24 hours with an initial summary.

d. Peran DPO dan Tim Respons

i. **Analisis Risiko:** Menentukan tingkat keparahan insiden (rendah, sedang, tinggi).
ii. **Koordinasi:** Membentuk Incident Response Team (IRT) terdiri dari DPO, Tim IT, Manajer Unit terkait, dan DPFP.
iii. **Dokumentasi:** Semua langkah dicatat dalam Incident Log.

d. Role of the DPO and Response Team

i. **Risk Analysis:** Determine incident severity level (low, medium, high).
ii. **Coordination:** Form an Incident Response Team (IRT) consisting of the DPO, IT Team, relevant Unit Manager, and DPFP.
iii. **Documentation:** All steps must be recorded in the Incident Log.

e. **Notifikasi Regulator & Subjek Data**
   i. Jika insiden berdampak tinggi, DPO wajib memberi tahu otoritas perlindungan data dalam waktu maksimal 72 jam.
   ii. Jika insiden berisiko serius pada individu, subjek data terdampak wajib diberi tahu segera dengan isi: jenis insiden, data terdampak, potensi risiko, serta langkah pencegahan yang disarankan.

f. **Pemulihan & Mitigasi**
   i. Tim IT melakukan pemulihan sistem (system restore) dari backup.
   ii. Data yang terdampak diperbaiki atau dipulihkan.
   iii. Akses sementara dibatasi hingga kondisi aman.
   iv. Subjek data diberi panduan mitigasi risiko (misalnya mengganti password, waspada phishing).

g. **Evaluasi & Pencegahan Ulang**
   i. Setelah insiden ditutup, DPO melakukan Root Cause Analysis untuk menemukan penyebab utama.
   ii. Menyusun Corrective and Preventive Actions (CAPA), misalnya:
      - Perbaikan SOP.
      - Peningkatan sistem keamanan
      - Pelatihan staf tambahan
   iii. Laporan akhir disimpan dalam Incident Report Repository dan diaudit secara berkala.

e. **Notification to Regulators & Data Subjects**
   i. If the incident has high impact, the DPO must notify the data protection authority within a maximum of 72 hours.
   ii. If the incident poses serious risk to individuals, affected data subjects must be notified immediately, including information on: type of incident, impacted data, potential risks, and recommended preventive actions.

f. **Recovery & Mitigation**
   i. The IT Team performs system recovery (system restore) from backup.
   ii. Affected data is corrected or restored.
   iii. Access is temporarily restricted until secure conditions are restored.
   iv. Data subjects are provided with risk mitigation guidance (e.g., changing passwords, phishing awareness).

g. **Evaluation & Recurrence Prevention**
   i. After an incident is closed, the DPO conducts a Root Cause Analysis to identify the primary cause.
   ii. Corrective and Preventive Actions (CAPA) are developed, such as:
      - SOP improvements
      - Security system enhancement
      - Additional staff training
   iii. The final report is stored in the Incident Report Repository and audited periodically.

h. Uji Simulasi

i. Simulasi penanganan insiden (tabletop exercise atau drill) dilakukan minimal 1 kali setahun untuk menguji kesiapan staf.

h. Simulation Drills

i. Incident response simulations (tabletop exercises or drills) must be conducted at least once a year to test staff preparedness.

11. PELATIHAN DAN AUDIT

a. **Pelatihan Staf Baru:** setiap staf wajib mengikuti pelatihan dasar perlindungan data dalam 7 hari kerja sejak bergabung, mencakup prinsip GDPR, UU PDP, serta praktik pengelolaan data di Penabulu.

b. **Pelatihan Berkala:** dilakukan **setahun sekali** untuk seluruh staf dan mitra, dengan pembaruan regulasi, studi kasus nyata, serta simulasi insiden. Staf yang memegang peran khusus (DPO, IT, DPFP) mendapat pelatihan lanjutan sesuai kebutuhan teknis.

c. **Audit Internal:** dilaksanakan **minimal 1 kali setahun** untuk menilai kepatuhan, efektivitas kontrol keamanan, dan kelengkapan dokumentasi. Hasil audit dituangkan dalam laporan resmi dan ditindaklanjuti dengan rencana perbaikan.

d. **Audit Eksternal:** dapat dilakukan oleh donor, regulator, atau pihak ketiga independen untuk memastikan standar global terpenuhi. Rekomendasi audit digunakan sebagai dasar perbaikan sistem.

e. **Review Kebijakan:** dilakukan **setiap 2 tahun** atau segera bila ada perubahan regulasi, dipimpin oleh DPO dan disahkan oleh Direktur Eksekutif.

f. **Simulasi Insiden:** setidaknya **1 kali setahun**, organisasi mengadakan latihan

11. TRAINING AND AUDIT

a. **New Staff Training:** Every staff member must undergo basic data protection training within 7 working days of joining, covering GDPR principles, PDP Act requirements, and data management practices at Penabulu.

b. **Periodic Training:** Conducted annually for all staff and partners, including regulatory updates, real case studies, and incident simulations. Staff with special roles (DPO, IT, DPFP) receive advanced training as needed.

c. **Internal Audit:** Conducted **at least once a year** to assess compliance, control effectiveness, and documentation completeness. Audit results must be documented and followed by improvement plans.

d. **External Audit:** May be conducted by donors, regulators, or independent third parties to confirm compliance with global standards. Recommendations are used to enhance the system.

e. **Policy Review:** Conducted **every 2 years** or sooner if regulatory changes occur, led by the DPO and approved by the Executive Director.

f. **Incident Simulation:** At least **once a year,** the organization performs incident

penanganan insiden untuk menguji kesiapan staf dan sistem.

handling drills to test staff and system readiness.

12. PENEGAKAN KEPATUHAN

Pelanggaran kebijakan ini dapat mengakibatkan sanksi berupa teguran, pembatasan akses, hingga pemutusan hubungan kerja atau kontrak, serta pelaporan kepada otoritas yang berwenang.

a. **Prinsip:** setiap pelanggaran perlindungan data ditangani serius, adil, dan transparan.

b. **Mekanisme:** pelanggaran dapat terdeteksi lewat audit, laporan staf, atau pengaduan; DPFP melakukan investigasi awal, lalu DPO dan Direksi menindaklanjuti sesuai tingkat pelanggaran.

c. **Kategori & Sanksi:**
   i. Ringan → teguran, pelatihan ulang.
   ii. Sedang → pembatasan akses, catatan kinerja.
   iii. Berat → pemutusan hubungan kerja/kontrak, pelaporan ke otoritas.

d. **Pihak Ketiga:** vendor atau mitra yang melanggar dapat dikenakan sanksi hingga pemutusan kontrak dan dilaporkan ke otoritas bila serius.

e. **Dokumentasi:** semua pelanggaran dicatat dalam Compliance Log dan dilaporkan berkala.

f. **Perlindungan Pelapor:** identitas pelapor dijaga, tanpa risiko pembalasan.

12. COMPLIANCE ENFORCEMENT

Violations of this policy may result in sanctions ranging from warnings and access restrictions to termination of employment or contracts, and reporting to competent authorities.

a. **Principle:** All data protection violations must be handled seriously, fairly, and transparently.

b. **Mechanism:** Violations may be detected through audits, staff reports, or complaints; DPFP conducts initial investigation, followed by DPO and Management handling according to severity.

c. **Categories & Sanctions**:
   i. Minor → warnings, retraining.
   ii. Moderate → access restrictions, performance records.
   iii. Severe → termination of employment/contract, reporting to authorities.

d. **Third Parties:** Vendors or partners who violate may be sanctioned up to contract termination and reported to authorities if serious.

e. **Documentation:** All violations are recorded in the Compliance Log and reported periodically.

f. **Whistleblower Protection**: Reporter identities must be protected, with no risk of retaliation.