PENABULU FOUNDATION
CIVIL SOCIETY RESOURCE ORGANIZATION

PROSEDUR OPERASI STANDAR (SOP)
STANDARD OPERATING PROCEDURE (SOP)

MANAJEMEN TEKNOLOGI INFORMASI (TI)
INFORMATION TECHNOLOGY (IT) MANAGEMENT

2025

LEMBAR PENGESAHAN / *APPROVAL SHEET*

No. Dokumen *Document No.*	009-Doc/LP/PB/VIII/2025
Nama Dokumen *Document Name*	Prosedur Operasi Standar (SOP) Manajemen Teknologi Informasi (TI) *Standard Operating Procedure (SOP) Information Technology (IT) Management*
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. TUJUAN

Prosedur Operasi Standar (SOP) ini bertujuan untuk memastikan bahwa pengelolaan Teknologi Informasi (TI) di Yayasan Penabulu berjalan dengan aman, efisien, transparan, dan akuntabel, serta mendukung pencapaian visi dan misi organisasi.

Secara lebih rinci, tujuan Prosedur Operasi Standar (SOP) ini adalah untuk:

a. Menyediakan pedoman yang jelas bagi seluruh karyawan dalam penggunaan, pengelolaan, dan pemeliharaan perangkat serta layanan TI.

b. Menjamin keamanan data, informasi, dan infrastruktur digital organisasi dari risiko kehilangan, kebocoran, atau penyalahgunaan.

c. Meningkatkan efisiensi kerja melalui pemanfaatan sistem, aplikasi, dan perangkat TI yang tepat guna dan berlisensi resmi.

d. Menciptakan mekanisme layanan TI (helpdesk) yang responsif dan terukur, sehingga kebutuhan karyawan dapat ditangani sesuai standar waktu layanan (SLA).

e. Menetapkan prosedur inventarisasi, distribusi, perawatan, serta pengembalian aset TI agar penggunaannya terkontrol dan terdokumentasi dengan baik.

f. Menumbuhkan budaya disiplin dan kesadaran karyawan terhadap penggunaan TI yang bertanggung jawab, etis, dan sesuai regulasi di Indonesia.

1. PURPOSE

This Standard Operating Procedure (SOP) aims to ensure that Information Technology (IT) management at the Penabulu Foundation is conducted in a secure, efficient, transparent, and accountable manner, while supporting the achievement of the organization's vision and mission.

More specifically, this SOP aims to:

a. Provide clear guidelines for all staff in the use, management, and maintenance of IT equipment and services.

b. Ensure the security of organizational data, information, and digital infrastructure against risks of loss, leakage, or misuse.

c. Improve work efficiency through the use of appropriate and officially licensed IT systems, applications, and devices.

d. Establish a responsive and measurable IT service (helpdesk) mechanism, ensuring staff needs are handled according to Service Level Agreement (SLA) standards.

e. Define procedures for inventory, distribution, maintenance, and return of IT assets to ensure controlled and well-documented usage.

f. Foster a culture of discipline and staff awareness regarding responsible, ethical, and regulation-compliant use of IT in Indonesia.

g. Mendukung kepatuhan organisasi terhadap standar tata kelola, regulasi nasional, serta kebijakan donor/mitra terkait perlindungan data dan keamanan informasi.

Dengan adanya Prosedur Operasi Standar (SOP) ini, diharapkan seluruh proses pengelolaan TI di Yayasan Penabulu dapat berjalan lebih terstruktur, konsisten, dan berkelanjutan, sehingga mampu mendukung kinerja organisasi secara optimal.

2. RUANG LINGKUP

Meliputi seluruh kegiatan IT: infrastruktur, jaringan, perangkat keras & lunak, keamanan siber, layanan pengguna (helpdesk), pengelolaan aset, pengadaan, pemeliharaan, backup & recovery, serta kepatuhan regulasi dan kebijakan privasi data.

3. PRINSIP-PRINSIP

- Keamanan dan privasi
- Ketersediaan (availability) dan keandalan (reliability)
- Kepatuhan terhadap regulasi dan standar (GDPR & UU ITE)
- Transparansi dan akuntabilitas
- Efisiensi dan keberlanjutan

4. KEBIJAKAN DAN PROSEDUR UTAMA

Dalam rangka menjaga kelancaran, keamanan, dan efisiensi pengelolaan Teknologi Informasi (TI) di Yayasan Penabulu, ditetapkan kebijakan umum sebagai berikut:

a. Manajemen Aset & Infrastruktur
   i. Seluruh perangkat (laptop, PC, printer, router, dan perangkat pendukung lainnya) wajib didata

g. Support organizational compliance with governance standards, national regulations, and donor/partner policies related to data protection and information security.

With this SOP in place, all IT management processes at the Penabulu Foundation are expected to operate in a more structured, consistent, and sustainable manner, thereby optimally supporting organizational performance.

2. SCOPE

This SOP covers all IT-related activities, including infrastructure, networks, hardware and software, cybersecurity, user services (helpdesk), asset management, procurement, maintenance, backup and recovery, as well as regulatory compliance and data privacy policies.

3. PRINCIPLES

- Security and privacy
- Availability and reliability
- Compliance with regulations and standards (GDPR & Indonesian Electronic Information and Transactions Law / UU ITE)
- Transparency and accountability
- Efficiency and sustainability

4. KEY POLICIES & PROCEDURES

To ensure smooth, secure, and efficient IT management at the Penabulu Foundation, the following general policies are established:

a. Asset & Infrastructure Management
   i. All devices (laptops, PCs, printers, routers, and other supporting equipment) must be recorded in

dan dicatat dalam daftar inventaris asset oleh tim TI/GA.

ii. Setiap perangkat diberi kode inventaris unik.

iii. Setiap perangkat/aset yang diberikan kepada karyawan baru harus disertai pengisian dan penandatanganan Formulir Peminjaman Aset TI.

iv. Pada saat karyawan mengundurkan diri atau kontraknya berakhir, perangkat/aset wajib dikembalikan dengan mengisi Formulir Pengembalian Aset TI. Sebelum diterima kembali, dilakukan pengecekan fisik untuk memastikan kelengkapan dan kondisi perangkat.

v. Hanya perangkat lunak resmi/berlisensi yang diperbolehkan diinstal pada perangkat organisasi.

vi. Perawatan rutin (update sistem operasi, patch keamanan, dan servis perangkat) dilakukan secara berkala minimal 3 bulan sekali oleh tim TI.

vii. Dilarang menggunakan perangkat/aset TI organisasi untuk kepentingan pribadi yang melanggar hukum atau bertentangan dengan kebijakan yayasan.

b. Layanan Pengguna / Helpdesk

i. Semua masalah atau kebutuhan terkait IT wajib dilaporkan melalui kanal resmi, yaitu grup WhatsApp khusus TI atau Formulir Online (Google Form Helpdesk TI).

ii. Setiap laporan yang masuk harus dicatat dalam log/daftar tiket helpdesk dan diberi nomor rujukan.

the IT asset inventory list by the IT/GA team.

ii. Each device must be assigned a unique inventory code.

iii. Any device/asset provided to new staff must be accompanied by completion and signing of the IT Asset Loan Form.

iv. Upon staff resignation or contract termination, all devices/assets must be returned using the IT Asset Return Form. A physical inspection is conducted prior to acceptance to ensure completeness and condition.

v. Only official/licensed software is permitted to be installed on organizational devices.

vi. Regular maintenance (operating system updates, security patches, and device servicing) must be conducted periodically, at least once every three months, by the IT team.

vii. Use of organizational IT devices/assets for personal purposes that violate the law or foundation policies is strictly prohibited.

b. User Services / Helpdesk

i. All IT-related issues or requests must be reported through official channels, namely the dedicated IT WhatsApp group or the Online Form (IT Helpdesk Google Form).

v. Each incoming report must be logged in the helpdesk ticket system and assigned a reference number.

iii. Tim TI melakukan analisis awal untuk menentukan prioritas dan tingkat keparahan masalah.
iv. SLA (Service Level Agreement) penanganan masalah ditetapkan sebagai berikut:
- Masalah ringan (contoh: instalasi software, setting printer) → ditangani dalam waktu maksimal 24 jam.
- Masalah sedang/berat (contoh: jaringan down, kerusakan server, gangguan sistem aplikasi) → ditangani dalam waktu maksimal 3 hari kerja, atau sesuai koordinasi lebih lanjut jika membutuhkan vendor eksternal.

v. Jika masalah tidak dapat ditangani dalam batas SLA, tim IT wajib memberikan pembaruan status dan estimasi waktu penyelesaian kepada pelapor.
vi. Laporan penyelesaian masalah disampaikan kembali kepada pelapor, dan tiket dinyatakan selesai/closed setelah ada konfirmasi.
vii. Data laporan masalah digunakan sebagai bahan evaluasi berkala untuk meningkatkan kualitas layanan IT.

vi. The IT team conducts an initial assessment to determine priority and severity.
vii. SLA (Service Level Agreement) is established to be as follows:
- Minor issues (e.g., software installation, printer setup): resolved within a maximum of 24 hours.
- Moderate/major issues (e.g., network outages, server failures, application system disruptions): resolved within a maximum of 3 working days, or subject to further coordination if external vendors are required.

viii. If an issue cannot be resolved within the SLA timeframe, the IT team must provide status updates and an estimated completion time to the reporter.
ix. Resolution reports are communicated back to the reporter, and tickets are marked as completed/closed upon confirmation.
x. Issue report data is used for periodic evaluation to improve IT service quality.

c. Keamanan Data & Akses
i. Password minimal 8 karakter, tidak digunakan ulang.
ii. Gunakan 2FA (Two-Factor Authentication) untuk email/akun penting.
iii. Akses data dibatasi sesuai kebutuhan kerja.
iv. Data sensitif harus disimpan di cloud organisasi (Google Drive/Box) dengan akses terbatas.

c. Data Security & Access
i. Passwords must be at least 8 characters long and not reused.
ii. Two-Factor Authentication (2FA) must be enabled for important email/accounts.
iii. Data access is restricted based on job responsibilities.
iv. Sensitive data must be stored in organizational cloud storage (Google Drive/Box) with restricted access.

d. Backup & Recovery
   i. Backup Data dilakukan secara rutin ke media penyimpanan yang aman, baik berupa cloud resmi organisasi (Google Drive/Box) maupun harddisk eksternal yang disimpan oleh tim TI. Backup dilakukan minimal 1 kali setiap bulan atau lebih sering sesuai kebutuhan.
   ii. Uji Pemulihan (Restore Test) wajib dilakukan secara berkala, minimal setiap 3–6 bulan sekali, untuk memastikan data yang dibackup dapat dipulihkan dengan baik dan tidak corrupt.
   iii. Prosedur Darurat:
      - Jika perangkat hilang, rusak, atau terkena serangan siber, data akan dipulihkan dari backup terakhir yang tersedia.
      - Tim IT bertanggung jawab melakukan langkah pemulihan serta mendokumentasikan proses recovery.
      - Jika diperlukan, recovery dilakukan dengan bantuan vendor eksternal atau penyedia layanan cloud.

e. Pengadaan dan Lisensi Software
   i. Semua software yang digunakan harus resmi/berlisensi, baik open source maupun berbayar.
   ii. Pengadaan software dilakukan sesuai prosedur pengadaan organisasi, dengan rekomendasi teknis dari tim TI.
   iii. Tim TI bertanggung jawab melakukan update/upgrade software secara berkala.

f. Kebijakan Penggunaan IT
   i. Email organisasi hanya untuk keperluan pekerjaan.

d. Backup & Recovery
   i. Data backups must be performed regularly to secure storage media, either official organizational cloud services (Google Drive/Box) or external hard drives maintained by the IT team. Backups must be conducted at least once per month or more frequently as needed.
   ii. Restore testing is mandatory and must be conducted periodically, at least once every 3–6 months, to ensure backed-up data can be restored properly and is not corrupted.
   iii. Emergency Procedures:
      - If a device is lost, damaged, or affected by a cyberattack, data will be restored from the most recent available backup.
      - The IT team is responsible for carrying out recovery steps and documenting the recovery process.
      - If necessary, recovery may involve external vendors or cloud service providers.

e. Software Procurement & Licensing
   i. All software used must be official/licensed, whether open-source or paid.
   ii. Software procurement follows organizational procurement procedures, with technical recommendations from the IT team.
   iii. The IT team is responsible for performing regular software updates and upgrades.

f. IT Usage Policy
   i. Organizational email accounts are for work-related purposes only.

ii. Dilarang menginstal software bajakan.
iii. BYOD (Bring Your Own Device) hanya diperbolehkan jika memenuhi standar keamanan (antivirus aktif, update sistem).
iv. Dokumen kerja harus disimpan di cloud organisasi, bukan akun pribadi.

g. Audit dan Evaluasi
   i. Audit aset TI dilakukan secara berkala, minimal setiap 6 (enam) bulan sekali, dengan menyusun Berita Acara Pemeriksaan Aset TI yang ditandatangani pihak terkait
   ii. Laporan hasil audit dan evaluasi wajib disampaikan kepada manajemen sebagai dasar pengambilan keputusan, tindak lanjut perbaikan, dan peningkatan berkelanjutan.

5. DOKUMEN & REVIEW

Prosedur Standar Oeprasional (SOP) terdokumentasi, mudah diakses, direvisi minimal setiap tahun atau saat ada perubahan besar.

6. DEFINISI ISTILAH

Untuk memudahkan pemahaman, beberapa istilah dalam SOP ini didefinisikan sebagai berikut:

a. TI (Teknologi Informasi)
Segala bentuk teknologi yang digunakan untuk mengelola data, informasi, komunikasi, dan sistem digital organisasi, termasuk perangkat keras, perangkat lunak, jaringan, dan layanan cloud.

b. SOP (Standard Operating Procedure / Prosedur Operasi Standar)

ii. Installation of pirated software is strictly prohibited.
iii. BYOD (Bring Your Own Device) is allowed only if security standards are met (active antivirus, updated system).
iv. Work documents must be stored in organizational cloud storage, not personal accounts.

g. Audit & Evaluation
   i. IT asset audits must be conducted periodically, at least once every six (6) months, by preparing an IT Asset Inspection Report signed by relevant parties.
   ii. Audit and evaluation reports must be submitted to management as a basis for decision-making, corrective actions, and continuous improvement.

5. DOCUMENTATION & REVIEW

This SOP must be documented, easily accessible, and reviewed/revised at least once a year or whenever significant changes occur.

6. DEFINITIONS OF TERMS

To facilitate understanding, the following terms are defined:

a. IT (Information Technology)
All technologies used to manage organizational data, information, communication, and digital systems, including hardware, software, networks, and cloud services.

b. SOP (Standard Operating Procedure)

Dokumen resmi yang berisi tata cara, aturan, dan prosedur kerja yang harus diikuti agar kegiatan berjalan konsisten, aman, dan terukur.

An official document containing work procedures, rules, and guidelines to ensure activities are conducted consistently, securely, and measurably.

c. **Aset TI**
Segala perangkat keras (hardware), perangkat lunak (software), jaringan, data, serta layanan digital yang dimiliki atau digunakan oleh organisasi.

c. **IT Assets**
All hardware, software, networks, data, and digital services owned or used by the organization.

d. **Formulir Peminjaman/Pengembalian Aset TI**
Dokumen administrasi resmi yang digunakan untuk mencatat distribusi dan pengembalian perangkat TI kepada/dari karyawan.

d. **IT Asset Loan/Return Form**
An official administrative document used to record the distribution and return of IT equipment to/from staff.

e. **Helpdesk / Layanan Pengguna**
Mekanisme layanan dukungan teknis untuk menangani masalah, kebutuhan, atau permintaan terkait penggunaan perangkat, aplikasi, maupun jaringan TI.

e. **Helpdesk / User Services**
A technical support service mechanism for handling issues, needs, or requests related to IT devices, applications, or networks.

f. **SLA (Service Level Agreement)**
Standar waktu layanan atau komitmen penyelesaian masalah TI, misalnya masalah ringan ditangani dalam <24 jam, masalah berat maksimal 3 hari.

f. **SLA (Service Level Agreement)**
A service time standard or commitment for resolving IT issues, e.g., minor issues within <24 hours, major issues within a maximum of 3 days.

g. **2FA (Two-Factor Authentication)**
Sistem keamanan login yang menggunakan dua lapisan verifikasi, biasanya kombinasi password dan kode OTP (One-Time Password) atau aplikasi authenticator.

g. **2FA (Two-Factor Authentication)**
A login security system using two layers of verification, typically a password combined with an OTP (One-Time Password) or authenticator app.

h. **Backup**
Salinan data yang disimpan di lokasi berbeda (cloud atau harddisk eksternal) untuk menghindari kehilangan data.

h. **Backup**
Copies of data stored in a separate location (cloud or external hard drive) to prevent data loss.

i. **Recovery**
Proses pemulihan data dari backup ketika terjadi kerusakan, kehilangan perangkat, atau serangan siber.

i. **Recovery**
The process of restoring data from backups in the event of damage, device loss, or cyberattacks.

j. **Vendor / Teknisi Mitra**
Pihak ketiga penyedia barang atau jasa terkait TI, seperti pemasok perangkat keras, software, atau layanan teknis.

k. **BYOD (Bring Your Own Device)**
Kebijakan penggunaan perangkat pribadi (laptop, HP) untuk bekerja, dengan syarat perangkat memenuhi standar keamanan organisasi.

l. **Patch Keamanan (Security Patch)**
Update perangkat lunak yang dirilis oleh pengembang untuk memperbaiki celah keamanan dan meningkatkan perlindungan sistem.

m. **Audit TI**
Proses pemeriksaan dan evaluasi terhadap aset, sistem, serta prosedur TI organisasi untuk memastikan kepatuhan, keamanan, dan efektivitasnya.

n. **Berita Acara Pemeriksaan Aset TI**
Dokumen hasil audit/inventarisasi yang berisi kondisi dan status aset TI, ditandatangani pihak terkait sebagai bukti resmi.

o. **Cloud Organisasi**
Layanan penyimpanan dan kolaborasi berbasis internet yang dimiliki/dikelola organisasi (contoh: Google Workspace/Drive, OneDrive, Box).

j. **Vendor / Partner Technician**
Third-party providers of IT-related goods or services, such as hardware suppliers, software vendors, or technical service providers.

k. **BYOD (Bring Your Own Device)**
A policy allowing the use of personal devices (laptops, mobile phones) for work, provided they meet organizational security standards.

l. **Security Patch**
A software update released by developers to fix security vulnerabilities and enhance system protection.

m. **IT Audit**
A process of examining and evaluating IT assets, systems, and procedures to ensure compliance, security, and effectiveness.

n. **IT Asset Inspection Report**
An audit/inventory document detailing the condition and status of IT assets, officially signed as evidence.

o. **Organizational Cloud**
Internet-based storage and collaboration services owned or managed by the organization (e.g., Google Workspace/Drive, OneDrive, Box).