KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

STANDAR OPERASIONAL PROSEDUR
Nomor: SOP/15/VIII/2022/PUSDATIN

TENTANG
PROSEDUR AKSES SISTEM INFORMASI

DIKELUARKAN DI JAKARTA
TAHUN 2022

BAB I
TUJUAN

1. Tujuan

   Tujuan dari pembuatan dokumen ini adalah untuk mengatur akses ke dalam sistem pengolahan informasi milik Pusdatin Kemhan RI yang dikelola oleh Bidang Pengembangan dan Pengelolaan Sistem Informasi Pertahan (Banglola Sisfohan), sehingga dapat mencegah akses oleh pihak yang tidak mempunyai wewenang.

BAB II
RUANG LINGKUP

2. Ruang Lingkup

   Akses ke semua sistem informasi Pusdatin Kemhan RI yang Bidang Pengembangan dan Pengelolaan Sistem Informasi Pertahan (Banglola Sisfohan) dikendalikan untuk membatasi akses hanya kepada para pemakai yang diberi hak dengan menggunakan proses *log-on* yang aman dan prosedur pembatasan sesi penggunaan sistem informasi *(session timeout).*

   Prosedur ini mengatur tahapan:

   a. Prosedur *Log-on.*

   b. Manajemen *Password.*

   c. Pencegahan penyalahgunaan fasilitas.

   d. Sinkronisasi jam.

   e. Pembatasan sesi penggunaan sumber daya computer.

   f. Otorisasi koneksi *eksternal*, *komputasi mobile networking.*

   g. Pembatasan akses ke *port remote diagnosic* dan konfigurasi.

   h. Proses peninjauan hak akses secara berkala.

   i. Peninjauan dan pemeliharaan catatan aktivitas jaringan secara berkala.

BAB III
DEFINISI

3. Definisi

a. *Log-on* adalah proses untuk mendapatkan hak akses menggunakan sumber daya sistem (komputer/ jaringan/ aplikasi) tujuan, dengan memasukkan identitas dari pengguna dan kata sandi (password).

b. *Log-out* adalah proses untuk mengakhiri sesi penggunaan sumber daya sistem (komputer/ jaringan/ aplikasi) setelah pengguna selesai melakukan kegiatannya.

c. *Session Time-out* adalah suatu aturan sistem komputer yang akan membatasi ketersediaan akses apabila sistem mendeteksi tidak adanya kegiatan user untuk suatu kurun waktu yang telah ditentukan. Secara otomatis pengguna akan diminta untuk melakukan log-on sebelum dapat memulai kembali kegiatannya yang terputus.

d. Sistem (mekanisme) AAA adalah sebuah model akses jaringan yang memisahkan tiga macam fungsi kontrol, yaitu *Authentication, Authorization, dan Accounting,* untuk diproses secara independen.

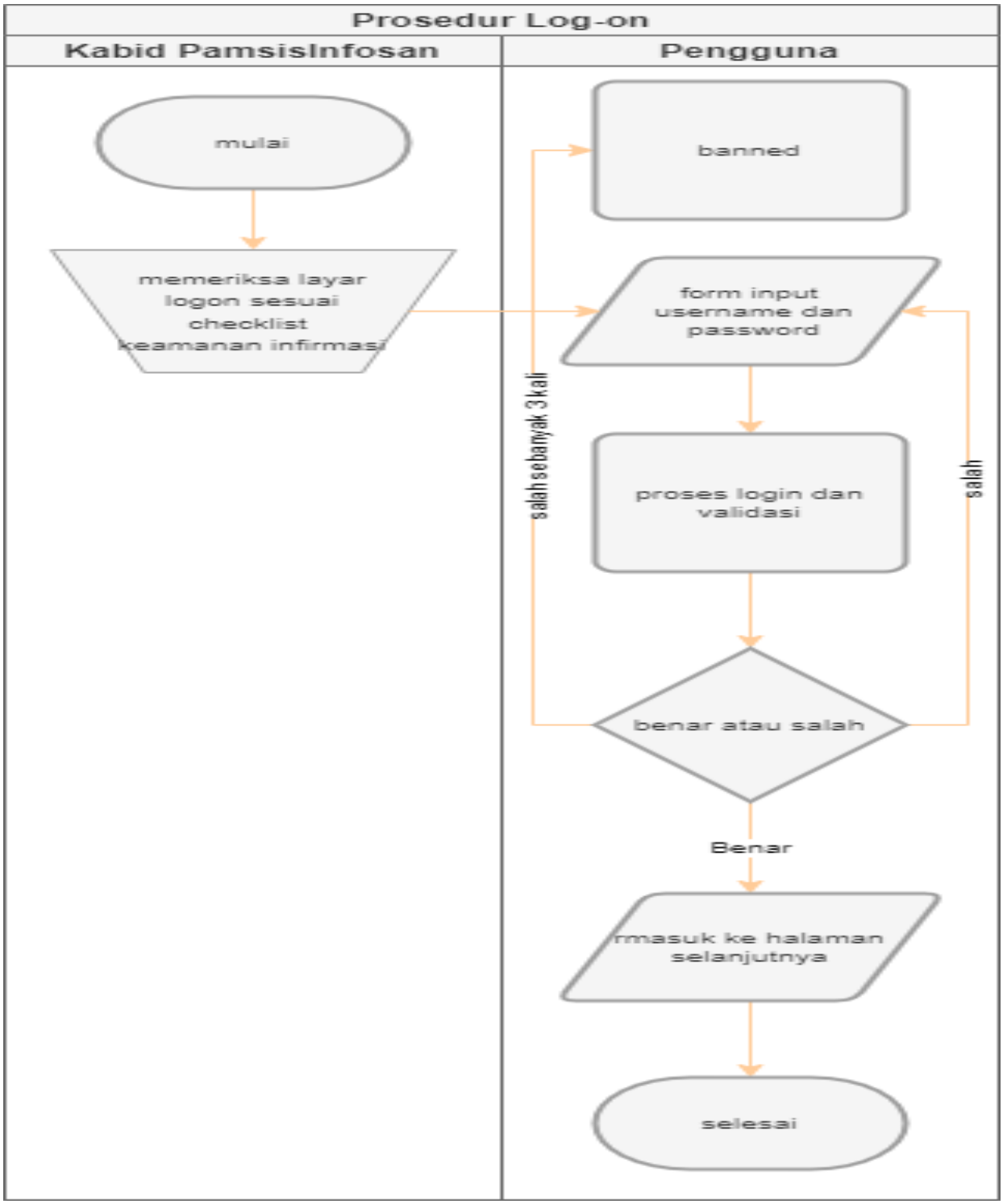
e. VPN *(Virtual Private Network)* adalah suatu koneksi antara satu jaringan dengan jaringan lainnya secara privat melalui jaringan publik (Internet). VPN disebut Virtual network karena menggunakan jaringan publik (Internet) sebagai media perantaranya alias bukan koneksi langsung. Dan disebut *private network* karena jaringannya bersifat privat, dimana hanya orang tertentu saja yang bisa mengaksesnya. Data yang dikirimkan pun terenkripsi sehingga aman dan tetap rahasia meskipun dikirim melalui jaringan publik.

f. *Active Directory* adalah layanan direktori yang dimiliki oleh sistem operasi jaringan Microsoft Windows server 2000, Windows server 2003 dan Windows Server 2008. *Active Directory* terdiri atas basis data dan juga layanan direktori. Basis data yang dimiliki oleh *Active Directory* menyimpan segala sumber daya yang terdapat di dalam jaringan, seperti halnya komputer yang telah tergabung ke sebuah domain, daftar akun pengguna dan kelompok pengguna, folder yang di-*share*, dan lain-lain. Sementara itu, layanan direktori yang dimilikinya membuat informasi yang disimpan di dalam basis data dapat diakses oleh pengguna.

BAB IV
PROSEDUR DAN TANGGUNG JAWAB

4. Prosedur dan Tanggung Jawab

Tabel 1. *Flowchart* Prosedur *Log-On*



a. Prosedur *Log-On*

Kabid Pamsisinfosan memastikan tampilan awal di layar monitor terkait *log-on* memenuhi persyaratan Keamanan Informasi, yaitu antara lain:

1) Tampilan di layar komputer tidak memperlihatkan petunjuk mengenai sistem operasi atau aplikasi tertentu, sampai *log-on* diselesaikan dengan sukses.

2) Layar tidak menyediakan pesan-pesan bantuan (misal, memberi contoh nama pengguna yang dapat dipakai) selama *log-on.*

3) Sistem membatasi waktu yang dibutuhkan untuk melakukan *log-on* (misal, 10 menit) dan, ketika batas itu terlewati, sistem mengakhiri *log-on.*

4) Setelah pengguna berhasil melalui *log-on*, layar akan menampilkan rincian tanggal dan waktu *log-on* sebelumnya yang dilakukan pengguna.

b. Manajemen *Password*

Kabid Pamsisinfosan memastikan manajemen *password* dilakukan dengan benar, antara lain memenuhi persyaratan berikut:

1) *Validasi* data pengguna dan *password* hanya dilakukan setelah semuanya dimasukkan. Jika terjadi kesalahan pengguna diminta untuk mencoba kembali.

2) Prosedur *log-on* hanya membatasi kesalahan *password* sebanyak tiga kali, setelah itu sistem akan memberitahu sistem administrator dan menolak usaha-usaha *log-on* lebih lanjut. Pengguna hanya akan diizinkan melakukan *log-on* kembali setelah sistem administrator melakukan identifikasi positif terhadap pengguna tersebut.

c. Pencegahan Penyalahgunaan Fasilitas

Tampilan layar sebelum atau pada saat *log-on* harus menjelaskan bahwa fasilitas pengolah informasi yang dipakai oleh pengguna adalah milik Pusdatin Kemhan RI yang dikelola oleh Departemen Teknologi Informasi dan hanya pengguna yang berwenang yang diijinkan memanfaatkan fasilitas tersebut. Setiap pengguna yang melanjutkan melakukan proses *log-on* adalah memang yang berwenang dan apabila terjadi penyalahgunaan wewenang pengguna bersedia menerima sanksi-sanksi yang berlaku.

d. Sinkronisasi Jam

1) Kabid Infratik memastikan pengendalian sinkronisasi jam

2) Kabid Infratik memastikan Jam dari semua sistem pengolahan informasi telah disinkronisasikan ke referensi sumber waktu tunggal.

e. Pembatasan Sesi Penggunaan Sumber Daya Computer

1) Para pemakai diwajibkan untuk melakukan log-out dari setiap sesi penggunaan difasilitas pengolah informasi, segera setelah kegiatannya di suatu sesi telah berakhir.

2) Apabila sistem mendeteksi tidak adanya kegiatan dalam satu sesi (misal, selama kurun waktu 10 menit), maka secara otomatis sistem akan mengakhiri sesi tersebut.

3) Otorisasi hak akses pada aplikasi, data, sistem operasi dan jaringan *computer.*

4) Pengguna melakukan akses pada aplikasi, data, sistem operasi dan jaringan *computer.*

5) Sistem teknologi informasi dan komunikasi (aplikasi, data, sistem operasi dan jaringan komputer) menampilkan layar *log in.*

6) Pengguna mengisi layar *login* dengan informasi nama pengguna dan *password* yang dimiliki.

7) Sistem teknologi informasi dan komunikasi (aplikasi, data, sistem operasi dan jaringan komputer) menggunakan informasi tersebut untuk diteruskan pada sistem AAA.

8) Sistem AAA bersama *database* dari *active directory* melakukan proses otentikasi dan otorisasi terhadap informasi nama pengguna dan *password* yang diberikan.

9) Sistem AAA memberikan hasil otentikasi dan otorisasi kepada pengguna, jika gagal pengguna ditolak masuk dengan menampilkan informasi pengguna tidak diperbolehkan melakukan akses sistem teknologi informasi dan komunikasi.

10) Sistem AAA memeberikan otorisasi kepada pengguna sesuai hasil otorisasi dengan menggunakan *database active directory*.

11) Pengguna yang sudah diotorisasi melanjutkan proses akses kepada sistem teknologi informasi dan komunikasi.

f. Otorisasi Koneksi *Eksternal, Komputasi Mobile Networking*

1) Pengguna menggunakan *VPN client* melakukan koneksi ke sistem *VPN Gateway.*

2) Pengguna melakukan akses pada aplikasi, data, sistem operasi dan jaringan computer.

3) Sistem Teknologi Informasi dan Komunikasi (Aplikasi, data, sistem operasi, dan jaringan komputer) menampilkan layar login.

4) Pengguna mengisi layar login dengan informasi nama pengguna dan password yang dimiliki.

5) Sistem Teknologi Informasi dan Komunikasi (aplikasi, data, sistem operasi dan jaringan komputer) menggunakan informasi tersebut untuk diteruskan pada sistem AAA.

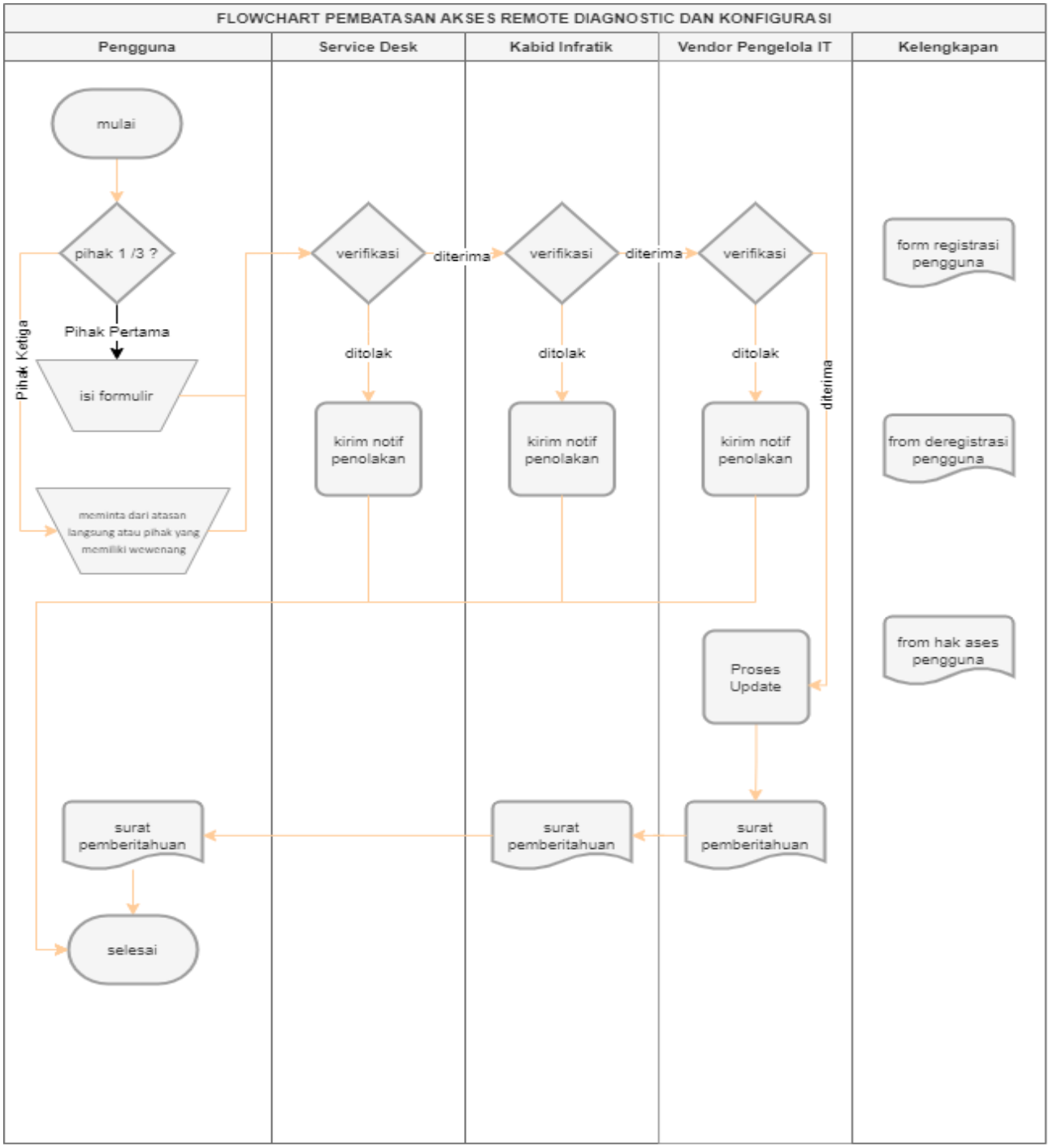
6) Sistem AAA bersama database dari *archive directory* melakukan proses otentikasi dan otorisasi terhadap informasi nama pengguna dan password yang diberikan.

7) Sistem AAA memberikan hasil otentikasi dan otorisasi kepada pengguna, jika gagal pengguna ditolak masuk dengan menampilkan informasi pengguna tidak diperbolehkan melakukan akses sistem Teknologi Informasi dan Komunikasi.

8) Sistem AAA memberikan otorisasi kepada pengguna sesuai hasil otorisasi dengan menggunakan database *active directory.*

9) Pengguna yang sudah diotorisasi melanjutkan proses akses kepada sistem Teknologi Informasi dan Komunikasi.

Tabel 2. Flowchart Pembatasan *Akses Romete Diagnostic* dan Konfigurasi



g. Pembatasan Akses Ke *Port Remote Diagnostic* dan Konfigurasi

1) Pengguna mengisi formulir perubahan akun sesuai .

2) Pengguna meminta dari atasan langsung atau pihak yang memiliki wewenang untuk mengotorisasi jika pengguna adalah pihak ke 3.

3) *Service desk* melakukan verifikasi terhadap kelengkapan dokumen yang diserahkan oleh pengguna.

4) *Service desk* melakukan verifikasi terhadap permintaan tersebut sesuai dengan kebijakan Sistem Manajemen Keamanan Informasi di Pusdatin Kemhan RI.

5) *Service desk* akan memberikan notifikasi kepada pengguna bahwa ada penolakan terhadap permintaan perubahan akun dan kata sandi.

6) Service desk meminta kepada pihak vendor pemelihara atau pihak pengelola sistem Teknologi Informasi dan Komunikasi untuk melakukan perubahan konfigurasi untuk pembatasan akses ke *port* konfigurasi dan *remote diagnostic.*

7) Kabid Pamsis Infosan atau *vendor* pemelihara akan melakukan verifikasi terhadap kelengkapan dokumen yang diserahkan oleh pengguna.

8) Kabid Infratik atau *vendor* pemelihara akan melakukan *Fchecking* terhadap permintaan.

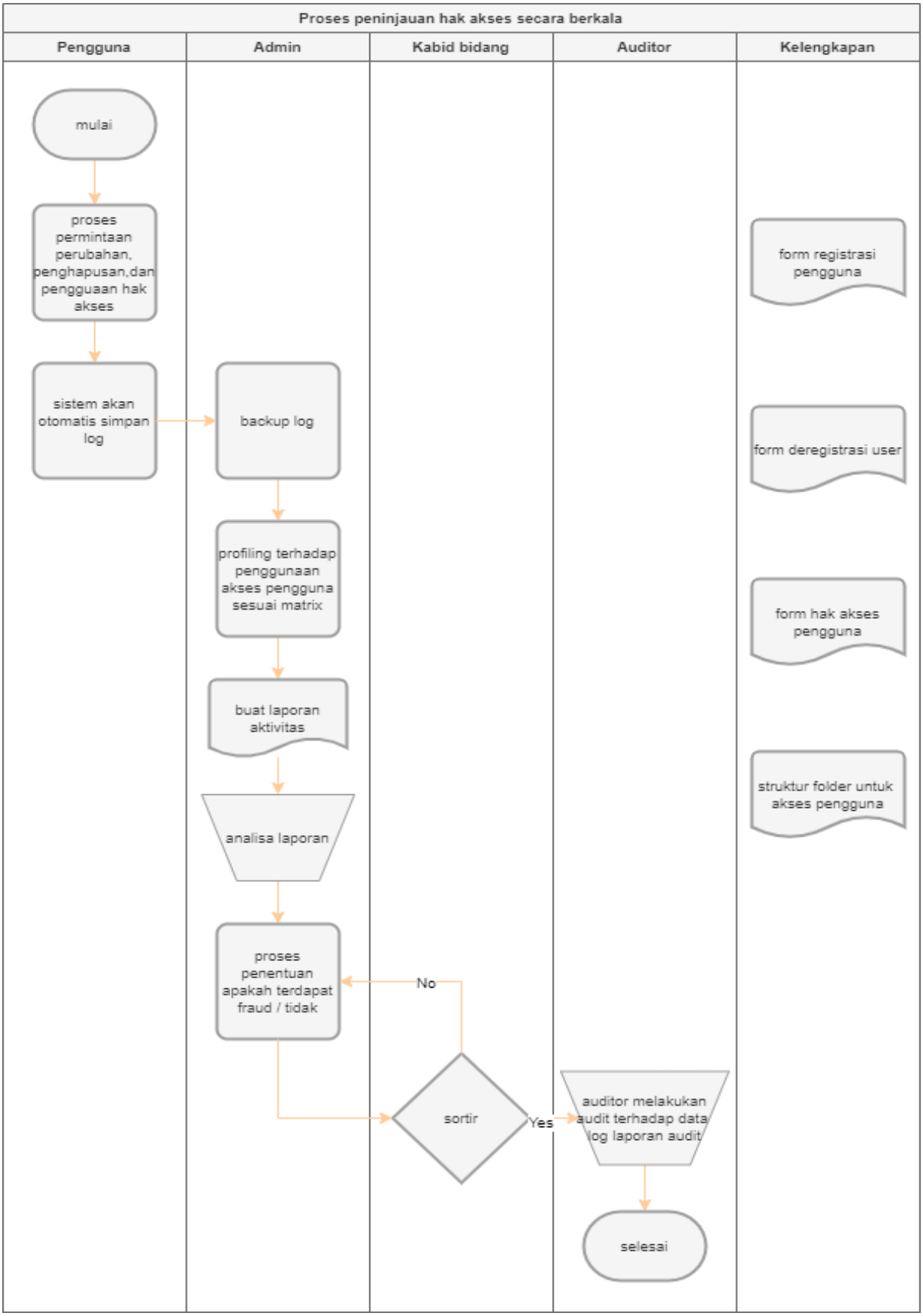
9) Kabid Infratik atau *vendor* pemelihara akan memberikan notifikasi kepada pengguna bahwa ada penolakan terhadap permintaan.

10) Kabid Infratik atau *vendor* pemelihara akan melakukan update konfigurasi sesuai dengan kebutuhan.

11) *Vendor* atau bidang Infra TIK akan memberikan surat pemberitahuan kepada Kabid Pamsisinfosan bahwa perubahan konfigurasi sudah dilakukan. Selanjutnya Kabid Pamsisinfosan akan menembuskan surat pemberitahuan tersebut kepada pengguna.

12) Pengguna melakukan *review* kembali terhadap pembatasan akses ke *port* konfigurasi dan *remote diagnostic* sesuai dengan aturan yang terdapat di dalam kebijakan *Information Security Management System* Pusdatin Kemhan RI.

Tabel 3. *Flowchart* Proses Pengajuan Hak Akases Secara Berkala



h. Proses Peninjauan Hak Akses Secara Berkala

1) Pengguna melakukan aktivitas permintaan, perubahan, penghapusan, dan penggunaan hak akses.

2) Sistem diharuskan untuk mencatat log aktivitas tersebut dari sistem AAA, sistem VPN dan *active directory.*

3) Admin pengguna melakukan *backup log data* sesuai dengan kebijakan dan standar pengelolaan data elektronik di lingkungan Pusdatin Kemhan RI.

4) Admin melakukan *profiling* terhadap penggunaan hak akses berdasarkan matrik akses pengguna .

5) Admin membuat laporan aktivitas pengguna dan hak aksesnya.

6) Admin melakukan analisis terhadap laporan.

7) Admin menentukan apakah terdapat *fraud* yang dilakukan oleh seorang pengguna.

8) Kabid terkait menentukan apakah data hasil analisa disampaikan kepada auditor.

9) Auditor melakukan audit terhadap data log laporan audit.

i. Peninjauan dan Pemeliharaan Catatan Aktivitas Jaringan Secara Berkala

1) Pengguna melakukan aktivasi jaringan.

2) Sistem diharuskan untuk mencatat log aktivitas tersebut dari sistem AAA, sistem VPN dan active directory dan catatan perangkat jaringan.

3) Admin melakukan backup log data sesuai dengan kebijakan dan standar pengelolaan data elektronik di lingkungan Pusdatin Kemhan RI.

4) Admin melakukan *profilling* terhadap catatan aktivitas jaringan.

5) Admin membuat laporan aktivitas jaringan.

6) Admin melakukan analisa terhadap laporan.

7) Admin menentukan apakah terdapat *fraud* yang dilakukan oleh seorang pengguna.

8) Atasan menentukan apakah data hasil analisis disampaikan kepada auditor.

9) Auditor melakukan audit terhadap data laporan audit *log.*

10) Auditor menentukan apakah telah terjadi fraud.

11) Auditor melaporkan kepada pengguna berdasarkan hasil audit untuk melakukan perbaikan.

BAB V
DOKUMEN PENDUKUNG

5. Dokumen Pendukung

- Prosedur Manajemen Akses Pengguna, *Registrasi*, dan *Deregistrasi* Nomor: SOP/15/VIII/2022/PUSDATIN

BAB VI
REKAMAN PENDUKUNG

6. Rekaman Pendukung

a. Formulir Registrasi User Nomor: LI/15A/VIII/2022/PUSDATIN.

b. Formulir Deregistrasi User Nomor: LI/15B/VIII/2022/PUSDATIN.

c. Formulir Hak Akses Pengguna Nomor: LI/15C/VIII/2022/ PUSDATIN.

d. Formulir Struktur Folder Untuk Akses Pengguna Nomor: LI/15D/VIII/2022/PUSDATIN

BAB VII
RUJUKAN

7. Rujukan

a. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Klausul 8. *Operation.*

b. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Klausul 8.1 *Operational Planning And Control.*

c. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.6.2 *Mobile Devices And Teleworking.*

d. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.6.2.1 *Mobile Device Policy.*

e. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.6.2.2 *Teleworking.*

f. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.1 *Business Requirements Of Access Control.*

g. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.1.1 *Access Control Policy.*

h. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.1.2 *Access To Networks And Network Services Similar To User Access Management.*

i. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2 *User Access Management.*

j. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2.1 *User Registration And De- Registration.*

k. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2.2 *User Access Provisioning.*

l. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2.3 *Management Of Privileged Access Rights.*

m. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2.4 *Management Of Secret Authentication Information Of Users (Similar To User Password Management).*

n. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2.5 *Review Of User Access Rights.*

o. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.2.6 *Removal Or Adjustment Of Access Rights.*

p. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.3 *User Responsibilities.*

q. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.3.1 *Use Of Secret Authentication Information Formerly "Password Use".*

r. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.4 *System And Application Access Control..*

s. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.4.1 *Information Access Restriction.*

t. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.4.2 *Secure Log-On Procedures.*

u. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.4.3 *Password Management System.*

v. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.4.1 *Event Logging.*

w. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.4.2 *Protection Of Log Information.*

x. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.4.3 *Administrator And Operator Logs.*

y. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.4.4 *Clock Synchronization.*

z. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.5 *Control Of Operational Software.*

aa. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.5.1 *Installation Of Software On Operational Systems.*

bb. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.13.1 *Network Security Management.*

cc. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.13.1.1 *Network Controls.*

dd. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.13.1.2 Security Of Network Services.

ee. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.13.1.3 *Segregation In Networks.*

BAB VIII
PENUTUP

8. Penutup

a. Demikian SOP Akses Sistem Operasi ini di buat, sebagai acuan dalam pengamanan informasi di Pusdatin.

b. Pedoman ini berlaku sejak di tandatangani dan ketentuan yang belum tercantum dalam pedoman ini akan diatur lebih lanjut dengan memperhatikan perkembangan Sistem Manajemen Keamanan Informasi.

c. Dokumen asli dari prosedur ini dipelihara dan dikendalikan oleh dokumen kontrol di Bidang Pamsisinfosan Pusdatin Kemhan RI.

d. Penggunaan dokumen asli ataupun dokumen salinan harus mengikuti aturan yang tertulis pada Dokumen Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN.

Dikeluarkan di Jakarta
Pada tanggal Agustus 2022

Kepala Pusat Data dan Informasi,

Rionardo
Brigadir Jenderal TNI

Lampiran

a. Formulir *Registrasi* User Nomor : LI/15A/VIII/2022/PUSDATIN.

b. Formulir *De Registrasi* User Nomor : LI/15B/VIII/2022/PUSDATIN.

c. Formulir Permintaan Hak Akses Nomor : LI/15C/VIII/2022/PUSDATIN.

d. Formulir *Folder* Akses Pengguna Nomor : LI/15D/VIII/2022/PUSDATIN

	KEMENTERIAN PERTAHANAN RI PUSAT DATA DAN INFORMASI	No. Dok	LI /15A/VIII/2022/PUSDATIN
		No. Rev	00
	REGISTRASI USER	Tgl	Agustus 2022
		Hal	

Petunjuk :

1. *Isilah semua data dengan lengkap pada Kolom A oleh Pemohon.*
2. *Mintalah persetujuan AtasanLangsung pada kolom C*
3. *Kirim Formulir ke Departemen IT untuk proses Registrasi*

A. DATA PEMOHON

Nama Lengkap : _____

NIK : _____

Departemen/Bagian : _____

B. JENIS PERMINTAAN

☐ E-Mail ☐ Internet ☐ Aplikasi System ☐ Other__

Alasan Permintaan : _____

Kolom dibawah ini diisi hanya untuk pengajuan Aplikasi System.

NO	APLIKASI	JENIS	LEVEL HAK AKSES	KETERANGAN

C. PERMINTAAN PEMOHON DAN PERSETUJUAN ATASAN LANGSUNG

Permintaan Pemohon

Dengan ini saya menyatakan mengerti dan menyetujui untuk mematuhi aturan yang berlaku selama saya memperoleh dan menggunakan hak akses informasi.

Tanda Tangan Pemohon

.....

Persetujuan Atasan Langsung

☐ Setuju ☐ Tidak Setuju

Tanda Tangan Atasan

.....

Nama :

Tanggal :

Nama : Tanggal :	
D. PERSETUJUAN BIDANG PAMSISINFOSAN DAN REALISASI	
Persetujuan Kabid Pamsisinfosan ☐ Disetujui ☐ Tidak Disetujui Alasan (jika ada) : Tanda Tangan Kabid Pamsisinfosan ..... Nama : Tanggal :	*Realisasi Permohonan* Tanggal Realisasi : _____ Tanda Tangan Admin ..... Nama : Tanggal :

Form ini disimpan oleh Bidang Pamsis Infosan

	KEMENTERIAN PERTAHANAN RI PUSAT DATA DAN INFORMASI	No. Dok	LI/15B/VIII/2022/PUSDATIN
		No. Rev	00
	DE REGISTRASI USER	Tgl	Agustus 2022
		Hal	1

Petunjuk :

1. *Isilah semua data secara lengkap*
2. *Mintalah persetujuan Atasan di kolom D*
3. *Kirim Formulir ke Bagian IT untuk di proses*

A. DATA PEMOHON

Nama Lengkap : _____

NIK : _____

Bidang/Bagian : _____

B. JENIS AKSES INFORMASI YANG DITUTUP

Alasan Penutupan Akses :

☐ Mutasi ☐ Pengunduran Diri

NO	NAMA AKSES	USER NAME	KETERANGAN

C. KETERANGAN MUTASI

Jabatan Lama :

Jabatan Baru :

Bagian : Bagian :

Akses Baru yang di butuhkan : _____

D. KETERANGAN PENGGUNAAN

Setuju ☐ Tidak Setuju

Tanda Tangan Pemohon Tanda Tangan Atasan

Nama : Tanggal :	Nama : Tanggal :
E. PERSETUJUAN Kabid Pamsisinfosan	
☐ Sukses ☐ Gagal Alasan (jika ada) : _____ Tanda Tangan Kabid Pamsisinfosan Nama : Tanggal :	

	KEMENTERIAN PERTAHANAN RI PUSAT DATA DAN INFORMASI	No. Dok	LI/15C/VIII/2022/PUSDATIN
		No. Rev	00
	FORMULIR PERMINTAAN HAK AKSES	Tgl	Agustus 2022
		Hal	1

PENANGGUNGJAWAB PUSDATIN	PENANGGUNGJAWAB PIHAK KE-III
Nama Petugas :	Nama Satker :
NIP/NRP :	Nama :
Jabatan :	NIP/NRP :
Telp :	Jabatan :
	Telp :

Tujuan/jenis akses :

☐ Collocation aplikasi baru

☐ Update aplikasi yang sudah ada

☐ Perbaikan aplikasi (bug)

☐ Lainnya _____

Ketentuan Penggunaan Hak Akses :

- User harus menyetujui dan mematuhi kebijakan keamanan informasi Pusat Data dan Infornasi Kementerian Pertahanan dan prosedur pengamanan terkait lainnya.
- User dilarang mengalihkan dan/atau meminjamkan hak akses kepada pihak lain.
- User dilarang menyalahgunakan akses untuk kepentingan selain penugasan.

Disiapkan oleh,

Petugas Pusdatin

Pemohon,

Mengetahui oleh,

Kasubbid Banglola Pusdatin

PENANGGUNG JAWAB PUSDATIN	PEMOHON
Nama Petugas :	Nama Satker :
NIP/NRP :	Nama :
Jabatan :	NIP/NRP :
Telp :	Jabatan :
	Telp :

Struktur Folder Akses Pengguna untuk :

- ☐ Struktural
  - ☐ Eselon II
    - ☐ Kapusdatin
  - ☐ Eselon III
    - ☐ Tata Usaha
    - ☐ Infrastruktur TIK
    - ☐ Banglola Sisfohan
    - ☐ Pamsisinfosan
  - ☐ Eselon IV
    - ☐ Tata Usaha
    - ☐ Infrastruktur TIK
    - ☐ Banglola Sisfohan
    - ☐ Pamsisinfosan
- ☐ Analis
  - ☐ Madya
  - ☐ Muda
- ☐ Fungsional (Pranata Komputer)
  - ☐ Madya
  - ☐ Muda
  - ☐ Ahli
  - ☐ Terampil
- ☐ Staf
  - ☐ Adminnistrasi
    - ☐ Keuangan
    - ☐ Dokumen
    - ☐ Umum
  - ☐ SDM
- ☐ Pihak Ke 3

Ketentuan Penggunaan Hak Akses :

- User harus menyetujui dan mematuhi kebijakan keamanan informasi Pusat Data dan Infornasi Kementerian Pertahanan dan prosedur pengamanan terkait lainnya.
- User dilarang mengalihkan dan/atau meminjamkan hak akses kepada pihak lain.
- User dilarang menyalahgunakan akses untuk kepentingan selain penugasan.
- Untuk dapat mengakses File Server, client harus Login Windows menggunakan user yang terdaftar sebagai user domain
- Tiap user hanya dapat meng-akses folder sesuai dengan Departemen-nya masing-masing atau folder "External" bagian lain dengan terlebih dahulu didaftarkan haknya pada folder tsb.

- Folder "Confidential" hanya dapat diakses oleh Kabid dan user tertentu di Departemen-nya masing-masing yang direkomendasikan oleh Kabid.
- Folder "Documents" terdiri dari 2 folder di dalamnya, yaitu:
- Folder "External", disediakan untuk menyimpan informasi yang dapat diakses oleh user yang ada di Departemen-nya dan user Departemen lain yang terlebih dahulu didaftarkan haknya untuk dapat mengaksesnya.
- Folder "Internal", disediakan untuk menyimpan informasi yang dapat diakses hanya oleh user yang ada di Departemen-nya masing-masing

Disiapkan oleh,

Petugas Pusdatin

Pemohon,

Mengetahui oleh,

Kasubbid Banglola Pusdatin