POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.09/1.1/8137.1/2019
	TANGGAL PEMBUATAN	13 November 2019
	TANGGAL REVISI	
	TANGGAL EFEKTIF	
	DISAHKAN OLEH	Direktur Satino, SKM., MScN NIP. 196101021989031001

KEBIJAKAN PENGENDALIAN HAK AKSES PADA AREA LAYANAN PUBLIK POLTEKKES SURAKARTA

KEBIJAKAN PENGENDALIAN HAK AKSES

Pada Area Layanan Publik di Poltekkes Surakarta

1. Pendahuluan

Informasi merupakan aset yang sangat penting bagi Satker penyelenggara layanan publik, dan karenanya perlu dilindungi dari ancaman yang dapat mengganggu kelangsungan bisnisnya.

Penggunaan fasilitas TI selain memudahkan proses pekerjaan juga mengandung risiko bila tidak digunakan dan dikelola dengan tepat

Penggunaan TI harus dikelola sedemikian rupa sehingga memberi manfaat sebesar - besarnya dengan kemungkinan risiko yang rendah.

Kebijakan ini didokumentasikan sebagai panduan untuk melindungi informasi dari ancaman keamanan informasi yang meliputi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dan mengurangi dampak dari terjadinya insiden keamanan

2. Tujuan

Menjamin persyaratan akses kontrol terhadap informasi dan fasilitas sistem informasi (aplikasi, sistem operasi, internet, email dan akses ruang Data Center / *Disaster Recovery Center*) didefinisikan dengan tepat

3. Ruang lingkup

Akses lojik atau fisik terhadap informasi dan fasilitas sistem informasi yang dikelola dalam menyelenggarakan pelayanan publik. pegawai, kontraktor, vendor, konsultan, atau pihak ketiga lainnya yang memerlukan akses ke sistem informasi

3.2 Kebijakan

- Pemberian setiap hak akses, baik lojik maupun fisik(seperti ruang DC/DRC) harus dibatasi berdasarkan tugas pokok dan fungsi (tupoksi) pengguna dan harus disetujui minimum oleh pejabat setingkat Eselon III
- Tingkatan akses harus diberikan dengan prinsip minimum yang cukup untuk memenuhi kebutuhan pengguna.
- Pemberian hak akses yang tingkatannya tinggi (root, super user atau administrator) hanya diberikan kepada karyawan yang benar-benar kompeten, memiliki pengalaman kerja di bagian TI minimum 3 tahun, dan harus disetujui minimum oleh pejabat setingkat Eselon III
- Hak akses pengguna yang menjalani mutasi atau tidak lagi bekerja di instanai harus segera di non-aktifkan maksimum 7 (hari) setelah tanggal yang ditetapkan.
- Hak akses tidak boleh dipinjamkan kepada pengguna lain.
- Seluruh hak akses pengguna akan direview setiap 6 (enam) bulan sekali.
- Tata cara pendaftaran, penutupan dan peninjauan hak akses diatur dalam Prosedur Pengendalian Hak Akses.
  Setiap pengecualian terhadap kebijakan ini hanya dapat dilakukan atas persetujuan pejabat setingkat Eselon III

- **Akses Pihak Ketiga :**
  - Vendor, konsultan, mitra, atau pihak ketiga lainnya yang melakukan akses fisik atau lojik ke dalam aset harus menandatangani Ketentuan/Persyaratan Menjaga Kerahasiaan Informasi.
  - Hak akses pihak ketiga hanya diberikan berdasarkan kepentingan yang disahkan melalui kerjasama atau kontrak.
  - Seluruh hak akses pihak ketiga harus dibatasi waktunya, dicatat dan ditinjau penggunaannya (log).
  - Seluruh akses yang disediakan bagi pelanggan harus mematuhi kebijakan keamanan informasi.
  - Seluruh koneksi pihak ketiga ke dalam network harus dibatasi hanya terhadap host dan/atau aplikasi tertentu yang ditetapkan oleh Satuan Kerja TI.

- **Pengelolaan Password**
  - Password **minimum** terdiri dari 8 karakter kombinasi angka dan huruf serta tidak boleh menggunakan karakter yang mudah ditebak.
  - Pengguna harus mengganti default password yang diberikan saat pertama kali mendapatkan hak akses.
  - Password tidak boleh: diberitahukan kepada orang lain dan atau ditulis di media yang mudah terlihat orang lain.
  - Password diganti secara berkala atau segera diganti bila diduga telah diketahui orang lain.
  - Periode penggantian password:
    - untuk pengguna biasa (seperti: email, web, komputer: minimum setiap 180 hari (6 bulan)
    - untuk pengguna sistem (seperti: root, admin server/aplikasi): minimum setiap 60 hari (2 bulan)
  - Seluruh default password dan password dari vendor harus diganti segera setelah instalasi selesai atau sistem diserahkan
  - Hak akses akan direset atau dinonaktifkan jika tak pernah digunakan selama 90 hari secara berturut-turut. Untuk mengaktifkannya kembali, pengguna harus mengajukan pendaftaran kembali sesuai Prosedur Pengendalian Hak Akses