PEMERINTAH KABUPATEN SLEMAN

KAPANEWON SEYEGAN

STANDAR OPERASIONAL PROSEDUR (S O P)

MANAJEMEN KEAMANAN INFORMASI

Nomor SOP	138/12.a
Tanggal Pembuatan	6 Januari 2024
Revisi Nomor SOP Revisi Tanggal SOP Revisi	1 02/SOP SYGN/XII/2025 2 Desember 2025
Tanggal Pengesahan SOP Revisi	2 Desember 2025
Pengesahan	Panewu Seyegan, AGUNG ENDARTA, S.Sos, M.Si Pembina Tingkat I, IV/b
Nama SOP	Manajemen Keamanan Informasi Kapanewon Seyegan

Dasar Hukum	Tujuan
1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Kepala Badan Pertanahan Nasional Republik Indonesia Nomor 1 Tahun 2010 tentang Standar Pelayanan dan Pengaturan Pertanahan; 3. Peraturan Bupati (Perbup) Kabupaten Sleman Nomor 55.30 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas Dan Fungsi, Serta Tata Kerja Kapanewon, dan;	Dokumen ini dibuat dalam rangka melakukan peninjauan hak akses secara berkala. Hal ini diperlukan untuk memastikan bahwa hak akses yang sudah diberikan digunakan secara benar dan tidak disalahgunakan, semua ini sebagai tambahan pengendali untuk memberikan bantuan dalam menjamin kerahasiaan *(confidentiality),* keutuhan *(integrity),* dan ketersediaan *(availability)* aset informasi agar selalu terjaga dan terpelihara dengan baik.
Ruang Lingkup	**Kualifikasi Pelaksana**
Ruang lingkup dari prosedur ini adalah pengendalian akses untuk pengamanan aset yang berkaitan dengan informasi dan fasilitas pengolahan informasi di Kapanewon Seyegan.	1. Panewu : Pendidikan minimal S1 2. Panewu Anom : Pendidikan minimal S1 3. Kepala Subbagian Umum dan Kepegawaian : Pendidikan minimal S1 4. Petugas : Pendidikan minimal SLTA Pengetahuan : 1. Memahami persyaratan pelayanan dan pengendalian akses 2. Memahami Komputer Diklat : 1. Pelayanan Prima, Komputer

Peran dan Tanggung Jawab	Peralatan/Perlengkapan
1. Panewu Seyegan bertanggung jawab untuk memberikan arahan dan tujuan yang terkait dengan pengendalian akses. 2. Panewu Anom bertanggung jawab untuk mengawasi seluruh proses dan kegiatan yang terkait dengan pengendalian akses. 3. Kepala Subbagian Umum dan Kepegawaian yang mewakili setiap jawatan harus mengambil tanggung jawab lebih lanjut untuk memastikan adanya pengendalian akses dengan cara senantiasa memperbarui matriks akses setiap pegawai maupun vendor yang berada di bawah kendalinya.	1. Komputer 2. Printer 3. Pulpen
Peringatan	**Pencatatan dan Pendataan**
Jika SOP Manajemen Keamanan Informasi tidak dilaksanakan sesuai ketentuan, maka akan terjadi : 1. Kebocoran data 2. Penyalahgunaan sistem 3. Ancaman keamanan siber 4. Kehilangan integritas data 5. Gangguan operasional	1. Matriks Akses 2. Form Permohonan dan Penutupan Akses 3. Form Reviu Akses

Kebijakan Umum	Lanjutan Kebijakan Umum
1. Persyaratan Bisnis untuk Kendali Akses a. Pengelolaan akses informasi dan fasilitas informasi harus dibatasi untuk menjamin kualitas informasi dan persyaratan bisnis yang aman terpenuhi. 2. Manajemen Akses Pengguna dan Tanggung Jawab Pengguna a. Setiap user harus menggunakan User ID masing-masing agar dapat mempertanggungjawabkan setiap tindakannya atas aset informasi Kapanewon Seyegan. Penggunaan User ID secara bersamaan *(sharing)* sangat dilarang. b. Hak akses semua pegawai dan pengguna pihak eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus pada saat pemutusan hubungan kerja, kontrak atau perjanjian, atau disesuaikan pada saat perubahan. c. Kata sandi yang digunakan sebagai informasi otentikasi harus berkualitas dengan panjang minimum delapan huruf ditlengkapi dengan karakter dan angka. d. User harus menjaga kerahasiaan mengenai informasi otentikasi, memastikan bahwa informasi tersebut tidak disebarluaskan. e. Adanya sanksi atas penyalahgunaan hak akses. 3. Kendali Akses Sistem dan Aplikasi a. Adanya pembatasan waktu koneksi ke dalam sistem aplikasi untuk memberikan keamanan untuk risiko yang tinggi dan mengurangi peluang akses yang tidak sah.	b. Sistem manajemen kata sandi harus interaktif dan harus memastikan adanya kata sandi yang berkualitas. 4. Penggunaan *Removable Media* a. Penggunaan peralatan pemrosesan dan penyimpanan informasi elektronik seperti hardisk eksternal harus dibatasi. b. Data yang tersimpan dalam removable media yang tidak akan digunakan kembali harus dihapus secara permanen dan dipastikan tidak dapat dimunculkan kembali. c. File yang tersimpan dalam removable media pada saat dinas sebaiknya segera disalin dalam PC pada saat pegawai berada di kantor. d. Pegawai harus selalu melakukan scanning virus terhadap removable media (Hardisk Eksternal) untuk mencegah adanya kerusakan informasi akibat ancaman virus. e. Pemindahan *removable media* berisi informasi keluar lingkungan Kapanewon Seyegan menjadi tanggung jawab dari pegawai untuk melindungi informasi sesuai dengan klasifikasi Informasi yang terkandung di dalamnya. f. *Removable Media* yang dapat digunakan sebagai media backup adalah external harddisk dan tempat penyimpanan media tersebut harus secara aman dan terlindungi. g. Removable media yang sudah rusak atau tidak digunakan lagi harus dimusnahkan secara fisik sehingga informasi yang mungkin masih ada didalamnya tidak dapat diambil kembali.

5. Penggunaan Email dan Internet

a. Fasilitas Email / internet diprioritaskan untuk mendukung pelaksanaan tugas dengan memperhatikan keterkaitan dengan pelaksanaan tugas pegawai dan Pengamanan Informasi.

b. Setiap Pegawai Kapanewon Seyegan yang menggunakan e-mail :

1) Tidak boleh membocorkan Informasi Rahasia milik Kapanewon Seyegan dan melakukan perbuatan melanggar hukum, terindikasi SARA, provokasi, kepentingan politik, pornografi, pencemaran nama baik dan atau pelecehan seksual.

2) Memastikan bahwa file yang di-download dari internet dan e-mail telah diperiksa dan dibersihkan dari Malicious Code (virus, worm, trojan, spyware, dan lain-lain) sebelum digunakan.

3) Tidak mengakses situs-situs internet dan menggunakan fitur/layanan di internet dan e-mail yang dilarang.

4) Berhati-hati dalam memberikan Informasi pribadi seperti password, PIN, e-mail address, tanggal lahir, dan lain sebagainya.

5) Berhati-hati dalam memberikan informasi pribadi melalui fasilitas email

6) Melaksanakan pengamanan terhadap Informasi Rahasia yang dikirimkan melalui email dengan metode pengamanan yang memadai.

7) Mewaspadai adanya berbagai risiko dalam penggunaan e-mail seperti, spoofing, spamming, atau phishing.

6. Ketentuan Pengelolaan Password

a. *Password* minimum terdiri dari 8 karakter kombinasi angka, huruf, dan karakter spesial (seperti: !@#$).

b. Pengguna harus mengganti *default password* yang diberikan saat pertama kali mendapatkan hak akses.

c. *Password* tidak boleh diberitahukan kepada orang lain dan ditulis di media yang mudah terlihat orang lain.

d. *Password* diganti secara berkala atau segera diganti bila diduga telah diketahui orang lain. Periode penggantian *password*:

a) untuk pengguna biasa (seperti: email, web, komputer: minimum 180 hari).

b) untuk pengguna sistem (seperti: root, admin server/ aplikasi): minimum 90 hari).

e. Seluruh *default password* dan *password* dari vendor harus diganti segera setelah instalasi selesai atau sistem diserahkan ke Kapanewon Seyegan.

f. Hak akses akan direset atau dinonaktifkan jika tak pernah digunakan selama 90 hari secara berturut-turut. Untuk mengaktifkannya kembali, pengguna harus mengajukan pendaftaran kembali kepada Bidang Terkait .

Prosedur Perubahan Registrasi Akses

No	Aktivitas	Dokumen	Pemohon	Panewu	Bidang Terkait	Tim Operasional Teknis
1	Mengirim surat permohonan perubahan hak akses	Form Permohonan Akses	Mulai			
2	Mendisposisi surat permohonan pada bidang terkait	Form Permohonan Akses				
3	Memberikan disposisi surat pada Tim Operasional Teknis	Form Permohonan Akses				
4	Mengkaji surat permohonan dan membuat surat balasan	Form Permohonan Akses				Disetujui?
5	Membuat perubahan dan memberikan tanggung jawab perubahan hak akses	1.Matriks Akses 2. Form Reviu Akses				Ya
6	Update Matriks Akses	Matriks Akses			Tidak	Selesai

Prosedur De-registrasi

No	Aktivitas	Dokumen	Pemohon	Panewu	Bidang Terkait	Tim Operasional Teknis
1	Mengirim surat permohonan penutupan hak akses	Form Penutupan Akses	Mulai			
2	Mendisposisi surat permohonan pada bidang terkait	Form Penutupan Akses				
3	Memberikan disposisi kepada Tim Operasional Teknis	Form Penutupan Akses				
4	Mengkaji surat permohonan dan membuat surat balasan	Form Penutupan Akses				Disetujui?
5	Menghapus data akses	1.Matriks Akses 2. Form Reviu Akses			Tidak	Ya
6	Update Matriks Akses	Matriks Akses				Selesai

Formulir Matriks Akses

MATRIKS AKSES

No	Nama	Posisi	Bidang	Email	Aset Informasi			Aset Virtual	Aset Fisik						Keterangan
					Data Pegawai	*Keuangan*	Pajak	Web Kapanewon Seyegan	PC Operator PPID	Router	Printer	CCTV	Finger Print	Scanner	
1															
3															
4															
5															
6															
7															
8															
9															
10															

Peran	Simbol	Keterangan
User	U	Hanya dapat memakai saja tidak dapat memodifikasi
Admin	A	Dapat memodifikasi tetapi tidak keseluruhan
Super Admin	S	Super admin dapat memodifikasi keseluruhan yang ada
Tidak ada akses	O	Tidak ada hak akses

Formulir Review Akses

FORM REVIEW AKSES

No	Periode yang Direview	Tanggal yang Direview	Hak Akses yang Direview	Hasil Review	Tindak Lanjut	PIC
1						
2						
3						
4						
5						
6						
7						
8						

PEMERINTAH KABUPATEN SLEMAN
KAPANEWON SEYEGAN
ꦏꦥꦤꦼꦮꦺꦴꦤ꧀ ꦱꦺꦪꦒꦤ꧀
Terwilen, Margodadi, Seyegan, Sleman,Yogyakarta, 55561
Telepon (0274) 4364755, Faksimile (0274) 4364704
Laman: seyegan.slemankab.go.id, Surel: kecseyegan@slemankab.go.id

Formulir Permohonan dan Penutupan Akses

Nama Karyawan :

Bidang :

Jabatan :

Tanggal Masuk :

Jenis Permohonan : □ **Pembukaan** □ **Perubahan** □ **Penutupan**

A. Perangkat Lunak

No	Nama Perangkat Lunak	Nama Email/Account/Aplikasi	Hak Akses
1			
2			
3			
4			
5			
6			

B. Perangkat atau Aset Lainnya

	Perangkat/Aset	Nama Email/*Account*	Hak Akses

Sleman, ...

Diajukan Oleh	Disetujui Oleh
….	…..