



KOMISI PEMILIHAN UMUM  
KOTA SERANG

KEPUTUSAN KOMISI PEMILIHAN UMUM KOTA SERANG  
NOMOR 144 TAHUN 2023  
TENTANG

STANDAR OPERASIONAL PROSEDUR PENGAMANAN SISTEM KOMPUTER DAN  
INFORMASI DAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA  
PEMILIHAN UMUM TAHUN 2024 DI KOMISI PEMILIHAN UMUM  
KOTA SERANG

KETUA KOMISI PEMILIHAN UMUM KOTA SERANG

- Menimbang :
- a. bahwa dalam rangka meningkatkan pengamanan sistem komputer dan informasi dan sistem manajemen keamanan informasi pada Pemilihan Umum Tahun 2024 di Komisi Pemilihan Umum Kota Serang;
  - b. bahwa berdasarkan ketentuan Pasal 1 dan Pasal 40 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai peran pemerintah dan instansi dalam hal kepentingan pengamanan data;
  - c. bahwa berdasarkan ketentuan Pasal 39 Undang-Undang 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menyebutkan sistem keamanan dibuat untuk pencegahan data pribadi yang yang diakses dengan secara tidak sah;
  - d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c perlu menetapkan Keputusan Komisi Pemilihan Umum Kota Serang tentang Standar Operasional Prosedur Pengamanan Sistem Komputer dan Informasi dan Sistem Manajemen Keamanan Informasi Pada Pemilihan

dan...

Umum Tahun 2024 di Komisi Pemilihan Umum Kota Serang;

- Mengingat :
1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
  2. Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 6109) sebagaimana telah diubah dengan Undang-Undang Nomor 7 tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2022 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 54, Tambahan Lembaran Negara Republik Indonesia Nomor 6832);
  3. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
  4. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
  5. Peraturan Komisi Pemilihan Umum Nomor 8 Tahun 2019 tentang Tata Kerja Komisi Pemilihan Umum, Komisi Pemilihan Umum Provinsi, dan Komisi Pemilihan Umum Kabupaten/Kota (Berita Negara Republik Indonesia Tahun 2019 Nomor 320) sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Komisi Pemilihan Umum Nomor 12 dengan...

Tahun 2023 tentang Perubahan Kelima atas Peraturan Komisi Pemilihan Umum Nomor 8 Tahun 2019 tentang Tata Kerja Komisi Pemilihan Umum, Komisi Pemilihan Umum Provinsi, dan Komisi Pemilihan Umum Kabupaten/Kota (Berita Negara Republik Indonesia Tahun 2023 Nomor 377);

6. Peraturan Komisi Pemilihan Umum Nomor 3 Tahun 2022 tentang Tahapan dan Jadwal Penyelenggaraan Pemilihan Umum (Berita Negara Republik Indonesia Tahun 2022 Nomor 574);

MEMUTUSKAN :

Menetapkan : KEPUTUSAN KOMISI PEMILIHAN UMUM KOTA SERANG TENTANG STANDAR OPERASIONAL PROSEDUR PENGAMANAN SISTEM KOMPUTER DAN INFORMASI DAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA PEMILIHAN UMUM TAHUN 2024 DI KOMISI PEMILIHAN UMUM KOTA SERANG.

KESATU : Menetapkan Standar Operasional Prosedur Pengamanan Sistem Komputer dan Informasi dan Sistem Manajemen Keamanan Informasi Pada Pemilihan Umum Tahun 2024 di Komisi Pemilihan Umum Kota Serang sebagaimana tercantum dalam Lampiran Keputusan yang merupakan bagian tidak terpisahkan dari Keputusan ini .

KEDUA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Serang  
pada tanggal 23 Oktober 2023

PARAF KOORDINASI	TANGGAL
Sekretaris	
Kepala Sub Bagian Hukum dan Sumber Daya Manusia	 23/10 - 2023
Kepala Sub Bagian Perencanaan, Data dan Informasi	 25/10 <sup>23</sup>

KETUA KOMISI PEMILIHAN UMUM  
KOTA SERANG,



LAMPIRAN

KEPUTUSAN KOMISI PEMILIHAN UMUM KOTA  
SERANG NOMOR 144 TAHUN 2023

TENTANG STANDAR OPERASIONAL PROSEDUR  
PENGAMANAN SISTEM KOMPUTER DAN  
INFORMASI DAN SISTEM MANAJEMEN KEAMANAN  
INFORMASI PADA PEMILIHAN UMUM TAHUN 2024  
DI KOMISI PEMILIHAN UMUM KOTA SERANG

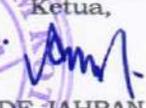


STANDAR OPERASIONAL PROSEDUR  
KOMISI PEMILIHAN UMUM KOTA SERANG  
NOMOR 144 TAHUN 2023

STANDAR OPERASIONAL PROSEDUR PENGAMANAN SISTEM KOMPUTER DAN  
INFORMASI (SIBER) DAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)  
PADA PEMILIHAN UMUM TAHUN 2024 DI KOMISI PEMILIHAN UMUM  
KOTA SERANG



**KOMISI PEMILIHAN UMUM  
KOTA SERANG**

 <b>KOMISI PEMILIHAN UMUM KOTA SERANG</b>	NOMOR SOP	: 935/TIK.03-SD/3673/3/2023
	TANGGAL PEMBUATAN	: 23 Oktober 2023
	TGL REVISI	: .....
	TANGGAL PENGESAHAN	: 23 Oktober 2023
	DISAHKAN OLEH	Ketua,  ADE JAHRAN
	NAMA SOP	<b>STANDAR OPERASIONAL PROSEDUR PENGAMANAN SISTEM KOMPUTER DAN INFORMASI DAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA PEMILIHAN UMUM TAHUN 2024 DI KOMISI PEMILIHAN UMUM KOTA SERANG</b>
DASAR HUKUM	KUALIFIKASI PELAKSANA	
<ol style="list-style-type: none"> <li>1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Tambahkan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Tambahkan Lembaran Negara Republik Indonesia Nomor 5952);</li> <li>2. Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 6109) sebagaimana telah diubah dengan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2022 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 224, Tambahan Lembaran Negara Nomor 6832);</li> <li>3. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196);</li> <li>4. Peraturan Komisi Pemilihan Umum Nomor 8 Tahun 2019 tentang Tata Kerja Komisi Pemilihan Umum, Komisi Pemilihan Umum Provinsi, dan Komisi Pemilihan Umum Kabupaten/Kota (Berita Negara Republik Indonesia Tahun 2019 Nomor 320) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Komisi Pemilihan Umum Nomor 5 Tahun 2022 tentang Perubahan Keempat atas Peraturan Komisi Pemilihan Umum Nomor 8 Tahun 2019 tentang Tata Kerja Komisi Pemilihan Umum, Komisi Pemilihan Umum Provinsi, dan Komisi Pemilihan Umum Kabupaten/Kota (Berita Negara Republik Indonesia Tahun 2022 Nomor 984);</li> <li>5. Peraturan Komisi Pemilihan Umum Nomor 3 Tahun 2022 tentang Tahapan dan Jadwal Penyelenggaraan Pemilihan Umum (Berita Negara Republik Indonesia Tahun 2022 Nomor 574);</li> <li>6. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551)</li> </ol>	<ol style="list-style-type: none"> <li>A. PENGAMANAN SISTEM KOMPUTER DAN INFORMASI (SIBER) <ol style="list-style-type: none"> <li>1. Pengamanan Aplikasi dan Pengembangan Sistem;</li> <li>2. Pengamanan Data Center dan Jaringan;</li> <li>3. Pengamanan Pengoperasian;</li> <li>4. Pengamanan Fisik (lanjutan);</li> <li>5. Audit (lanjutan);</li> </ol> </li> <li>B. SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) <ol style="list-style-type: none"> <li>1. Kemanan Teknologi Informasi (TIK);</li> <li>2. Kemanan Fisik;</li> <li>3. Sistem Manajemen;</li> <li>4. Pengelolaan Berkelanjutan.</li> </ol> </li> </ol>	
KETERKAITAN	PERALATAN / PERLENGKAPAN	
1. SOP Layanan Informasi Publik	<ol style="list-style-type: none"> <li>1. Form Tanggapan dan Masukan Masyarakat;</li> <li>2. Komputer;</li> <li>3. Internet.</li> </ol>	
PERINGATAN	PENCATATAN DAN PENDATAAN	

<p>C. 1. Jika tidak dilaksanakan Pengamanan Sistem Komputer Dan Informasi (SIBER) maka timbul potensi ancaman/serangan pada server/aplikasi kepemiluan KPU</p>	<ol style="list-style-type: none"> <li>1. Pengamanan Aplikasi dan Pengembangan Sistem dilakukan dengan cara : <ol style="list-style-type: none"> <li>a. Pengelolaan basis data</li> <li>b. Integritas Data</li> <li>c. Kerahasiaan Data</li> <li>d. Ketersediaan Data</li> <li>e. Metodology pengembangan aplikasi</li> <li>f. Pengendalian perubahan aplikasi</li> <li>g. Penanganan program/koding bermasalah</li> </ol> </li> <li>2. Pengamanan Data Center dan Jaringan, dilakukan dengan cara : <ol style="list-style-type: none"> <li>a. Teknologi pengamanan yang digunakan</li> <li>b. Pemilihan Protokol Jaringan</li> <li>c. Perangkat keamanan</li> <li>d. Teknik Kriptografi</li> <li>e. Model dan Arsitektur Keamanan</li> <li>f. Digital Signature</li> <li>g. Privillage, Firewall, Performance Test, Pentest test, Backup</li> </ol> </li> <li>3. Pengamanan Pengoperasian, dilakukan dengan cara : <ol style="list-style-type: none"> <li>a. Pemisahan Tugas dan Wewenang</li> <li>b. Alur pertanggungjawaban</li> <li>c. Perekrutan SDM</li> <li>d. Kontrol input dan output data</li> <li>e. Kontrol pengelolaan perubahan data</li> </ol> </li> </ol>
<p>2. Jika tidak dilaksanakan Sistem Manajemen Keamanan Informasi (SMKI) maka tidak terlindunginya kerahasiaan, integritas dan ketersediaan informasi, tidak dapat mengendalikan resiko keamanan informasi, tidak memiliki kontrol organisasi terhadap lingkungan proses bisnisnya, tidak ootuh terhadap hukum dan undang-undang seperti UU ITE, dll.</p>	<ol style="list-style-type: none"> <li>1. Personil di lingkungan KPU Provinsi/KIP Aceh dan KPU/KIP Kabupaten/Kota yang menggunakan aset informasi milik satuan kerja (satker) harus bertanggung jawab terhadap penggunaan aset informasi yang sesuai dengan prinsip keamanan informasi yaitu: <ol style="list-style-type: none"> <li>a. Menggunakan aset informasi dengan benar untuk menghindari risiko kehilangan atau kerusakan;</li> <li>b. Menjaga kerahasiaan aset informasi dan informasi yang tersimpan;</li> <li>c. Melindungi aset informasi terhadap akses yang tidak sah atau tidak memiliki otoritas; dan</li> <li>d. Tidak menggunakan aset informasi untuk kepentingan yang bertentangan dengan etika, peraturan, dan hukum yang berlaku serta merugikan satuan kerja (satker) di masing-masing daerah.</li> </ol> </li> <li>2. Semua aset informasi harus dilakukan identifikasi dan inventarisasi;</li> <li>3. Semua aset informasi harus ditetapkan penanggungjawabnya;</li> <li>4. Semua aset informasi hanya boleh digunakan untuk kepentingan satuan kerja (satker);</li> <li>5. Informasi pada satuan kerja (satker) harus diklasifikasikan sesuai dengan persyaratan hukum, nilai, kritikalitas, dan kerentanan terhadap pengungkapan atau pemodifikasian yang tidak sah. Klasifikasi informasi terbagi menjadi 3 kelas, yaitu: Rahasia, Terbatas dan Publik;</li> <li>6. Media yang dapat dipindahkan (<i>removable media</i>) seperti CD, <i>Portable Harddisk</i>, <i>Flash Disk</i>, dan <i>Tape Backup</i>, yang menyimpan informasi rahasia harus disimpan di <b>lokasi yang aman</b>, yaitu lokasi yang telah ditentukan;</li> <li>7. <b>Flash Disk tidak boleh</b> digunakan untuk menyimpan informasi rahasia secara permanen. Jika <i>flash disk</i> digunakan untuk pertukaran informasi rahasia, maka informasi rahasia tersebut harus segera dihapus setelah pertukaran dilakukan;</li> <li>8. Jika aset informasi akan dipindahtanggankan keluar dari lingkungan satuan kerja (satker), maka informasi yang disimpan harus <b>diformat atau dihapus</b> dengan metode yang aman;</li> <li>9. Media yang dapat dipindahkan (<i>removable media</i>) yang telah dan atau tidak dapat dibaca oleh sistem komputer atau mengalami kerusakan harus <b>dihancurkan secara fisik</b>;</li> <li>10. KPU Provinsi/ KIP Aceh dan KPU/ KIP Kabupaten/ Kota wajib mengganti kata sandi (<i>password</i>) email secara berkala minimal <b>1 kali setiap 3 bulan</b>;</li> <li>11. Seluruh <i>Administrator Cpanel Website</i> dan <i>Administrator</i> pengelola website KPU Provinsi/ KIP Aceh dan KPU/ KIP Kabupaten/ Kota wajib mengganti kata sandi (<i>password</i>) secara berkala minimal <b>1 kali setiap bulan</b>.</li> <li>12. Pembuatan kata sandi (<i>password</i>) harus terdiri dari : <ol style="list-style-type: none"> <li>a. Kombinasi huruf kapital, huruf kecil, dan karakter khusus;</li> <li>b. Sulit ditebak, tetapi mudah diingat oleh pengguna;</li> <li>c. Bukan merupakan kata atau akronim dari nama sendiri atau kerabat, tanggal lahir, alamat rumah, dan sebagainya;</li> <li>d. Tidak sama dengan nama akun pengguna, baik sebagian atau seluruhnya; dan</li> <li>e. Tidak sama dengan 3 sandi (<i>password</i>) terakhir yang telah diganti.</li> </ol> </li> <li>13. Pengguna hak akses <b>tidak boleh</b> membagi atau memberitahukan kata sandi (<i>password</i>);</li> <li>14. Kata sandi (<i>password</i>) <b>tidak boleh</b> dituliskan ditempat yang mudah terlihat;</li> </ol>

15. Kata sandi (*password*) default harus diganti;
  16. Hak akses semua pengguna harus dilakukan peninjauan secara berkala;
  17. Hak akses pengguna yang telah **tidak berwenang** harus segera ditutup atau **dihapus**;
  18. Pengguna hak akses **tidak boleh memilih** mengingat kata sandi (***remember password***) dalam tampilan *login*;
  19. Setiap personil wajib menjaga perangkat (*komputer dan gawai*) tetap aman dengan melakukan hal-hal sebagai berikut:
    - a. Menginstal dan melakukan pembaruan Antivirus;
    - b. Memastikan media yang bisa dipindahkan (*removable media*) seperti *flash disk* tetap aman;
    - c. Menggunakan aplikasi resmi dan berlisensi;
    - d. Menggunakan enkripsi;
    - e. Melakukan pencadangan data secara rutin;
  20. Selalu mengunci perangkat (*komputer dan gawai*) jika sedang tidak digunakan;
  21. Melakukan pengamanan pada koneksi jaringan internet di lingkungan satuan kerja (*satker*) dengan melakukan hal-hal sebagai berikut:
    - a. Mengaktifkan fungsi ***firewall*** pada *router*;
    - b. Gunakan protokol **WPA2** pada kata sandi WiFi;
  22. Akses internet WiFi (*wireless*) disediakan kepada pegawai untuk melakukan akses informasi yang berkaitan dengan operasional dan kompetensi dalam pelayanan jasa teknologi;
  23. Pemasangan perangkat keras WiFi (*wireless*) harus mendapatkan persetujuan dari Kepala Bagian/ Sub Bagian terkait;
  24. Pengguna akses internet dilarang melakukan pengunduhan informasi dengan ekstensi **“.exe”**, **“.com”**, dan ekstensi lainnya yang dapat dieksekusi karena memiliki risiko terdapat *malware* (perangkat lunak berbahaya);
- Sumber :  
Surat Edaran KPU RI No 3 Tahun 2022  
Tentang Penerapan Kebijakan Sistem Manajemen Keamanan Informasi.

**FLOWCHART STANDAR OPERASIONAL PROSEDUR (SOP)**  
**PENGAMANAN SISTEM KOMPUTER DAN INFORMASI (SIBER) PADA PEMILU TAHUN 2024**

NO	KEGIATAN	PELAKSANAAN					KELENGKAPAN	WAKTU	OUTPUT
		ADMIN/OPERATOR KPU KOTA SERANG	KEPALA SUB BAGIAN KPU KOTA SERANG	SEKRETARIS KPU KOTA SERANG	KOORDINATOR DIVISI KPU KOTA SERANG	KETUA KPU KOTA SERANG			
1.	Pengamanan Aplikasi dan Pengembangan Sistem						1. Komputer; 2. Jaringan internet; 3. Flashdisk/Hardisk Eksternal 4. Data/Unduhan Aplikasi	1. Rapat Pleno 120 Menit 2. Koordinasi 30 menit  <b>Total Waktu 150 Menit</b>	1. Pengelolaan basis data; 2. Integritas Data; 3. Kerahasiaan Data; 4. Ketersediaan Data; 5. Metodology pengembangan aplikasi; 6. Pengendalian perubahan aplikasi; 7. Penanganan program/koding bermasalah
2.	Pengamanan Data Center dan Jaringan						1. Komputer; 2. Jaringan internet; 3. Flashdisk/Hardisk Eksternal 4. Data/Unduhan Aplikasi	1. Rapat Internal 60 Menit 2. Pelaksanaan 30 Menit  <b>Total Waktu 90 Menit</b>	1. Teknologi pengamanan yang digunakan; 2. Pemilihan Protokol Jaringan; 3. Perangkat keamanan; 4. Teknik Kriptografi; 5. Model dan Arsitektur Keamanan; 6. Digital Signature; 7. Privillage, Firewall, Performance Test, Pentest test, Backup
3.	Pengamanan Pengoperasian, dilakukan dengan cara : a. Pemisahan Tugas dan Wewenang; b. Alur pertanggungjawaban; c. Perekrutan SDM; d. Kontrol input dan output data; e. Kontrol pengelolaan perubahan data						1. Komputer; 2. Jaringan internet; 3. Flashdisk/Hardisk Eksternal 4. Data/Unduhan Aplikasi	1. Rapat Internal 30 Menit 2. Koordinasi 10 Menit 3. Pelaksanaan 30 Menit  <b>Total Waktu 70 Menit</b>	1. Pemisahan Tugas dan Wewenang; 2. Alur pertanggungjawaban; 3. Perekrutan SDM; 4. Kontrol input dan output data; 5. Kontrol pengelolaan perubahan data

Keterangan ;

1. Simbol Kapsul/Terminator ( ) untuk mendeskripsikan kegiatan mulai dan berakhir;

**FLOWCHART STANDAR OPERASIONAL PROSEDUR (SOP)**  
**SISTEM MANAJEMEN KEAMANAN INFORMASI PADA PEMILIHAN UMUM TAHUN 2024**

NO	KEGIATAN	PELAKSANAAN					KELENGKAPAN	WAKTU	OUTPUT
		ADMIN/OPERATOR/ SDM KPU KOTA SERANG	KEPALA SUB BAGIAN KPU KOTA SERANG	SEKRETARIS KPU KOTA SERANG	KOORDINATOR DIVISI KPU KOTA SERANG	KETUA KPU KOTA SERANG			
1.	Kemanan Teknologi Informasi (TIK);						1. Arsip Fisik; 2. Percakapan; 3. File Digital; 4. Rekaman	1. Rapat Pleno 60 Menit 2. Koordinasi 30 menit; 3. Pelaksanaan 60 Menit  <b>Total Waktu 150 Menit</b>	1. Perlindungan data pribadi 2. <b>Aplikasi</b> , Audit Aplikasi oleh ITSA oleh BSSN 3. <b>Infrastruktur</b> , memperhatikan Penerapan ISO 27001:2013 dan SE KPU No 3 Tahun 2022
2.	Kemanan Fisik;						1. brankas, lemari arsip) 2. pengawasan dari CCTV ataupun dari petugas keamanan); 3. gembok, fingerprint, biometric, kartu akses)	3. Koordinasi 10 Menit 4. Pelaksanaan 60 Menit  <b>Total Waktu 70 Menit</b>	1. Informasi ditempatkan pada tempat yang terlindungi dari berbagai ancaman dan risiko ( 2. Terdapat pengawasan/monitoring terhadap aset informasi yang dilindungi 3. Menerapkan kunci keamanan pada tempat penyimpanan informasi
3.	Sistem Manajemen;						1. Arsip Fisik; 2. Percakapan; 3. File Digital; 4. Rekaman Data/Unduhan Aplikasi 5. Informasi ditempatkan pada tempat yang terlindungi dari berbagai ancaman dan risiko (contoh : brankas, lemari arsip) 6. aset informasi yang dilindungi (contoh : pengawasan dari CCTV ataupun dari petugas keamanan); 7. kunci keamanan pada tempat penyimpanan informasi (contoh : gembok, fingerprint, biometric, kartu akses)	1. Koordinasi 10 Menit 2. Pelaksanaan 30 Menit  <b>Total Waktu 40 Menit</b>	1. Penertiban SOP dan Petunjuk Teknis terkait Pengelolaan Informasi 2. Pengelompokan informasi berdasarkan klasifikasi data (Rahasia, Terbatas, Terbuka) 3. Pembentukan CSIRT 4. Pembentukan Gugus Tugas Keamanan Siber

4	Pengelolaan Berkelanjutan.					<ol style="list-style-type: none"> <li>1. Arip Fisik;</li> <li>2. Percakapan;</li> <li>3. File Digital;</li> <li>4. Rekaman Data/Unduhan Aplikasi</li> <li>5. Informasi ditempatkan pada tempat yang terlindungi dari berbagai ancaman dan risiko (contoh : brankas, lemari arsip)</li> <li>6. aset informasi yang dilindungi (contoh : pengawasan dari CCTV ataupun dari petugas keamanan);</li> <li>7. kunci keamanan pada tempat penyimpanan informasi (contoh : gembok, fingerprint, biometric, kartu akses)</li> </ol>	<ol style="list-style-type: none"> <li>1. Rapat Pleno 60 Menit</li> <li>2. Koordinasi 30 menit;</li> <li>3. Pelaksanaan 60 Menit</li> </ol> <p style="text-align: center;"><b>Total Waktu 150 Menit</b></p>	<ol style="list-style-type: none"> <li>1. Pendokumentasian mitigasi insiden</li> <li>2. Peningkatan <i>Awareness</i> Keamanan Informasi melalui pencegahan, penanggulangan dan evaluasi</li> </ol>
---	----------------------------	--	--	--	--	---	---	--

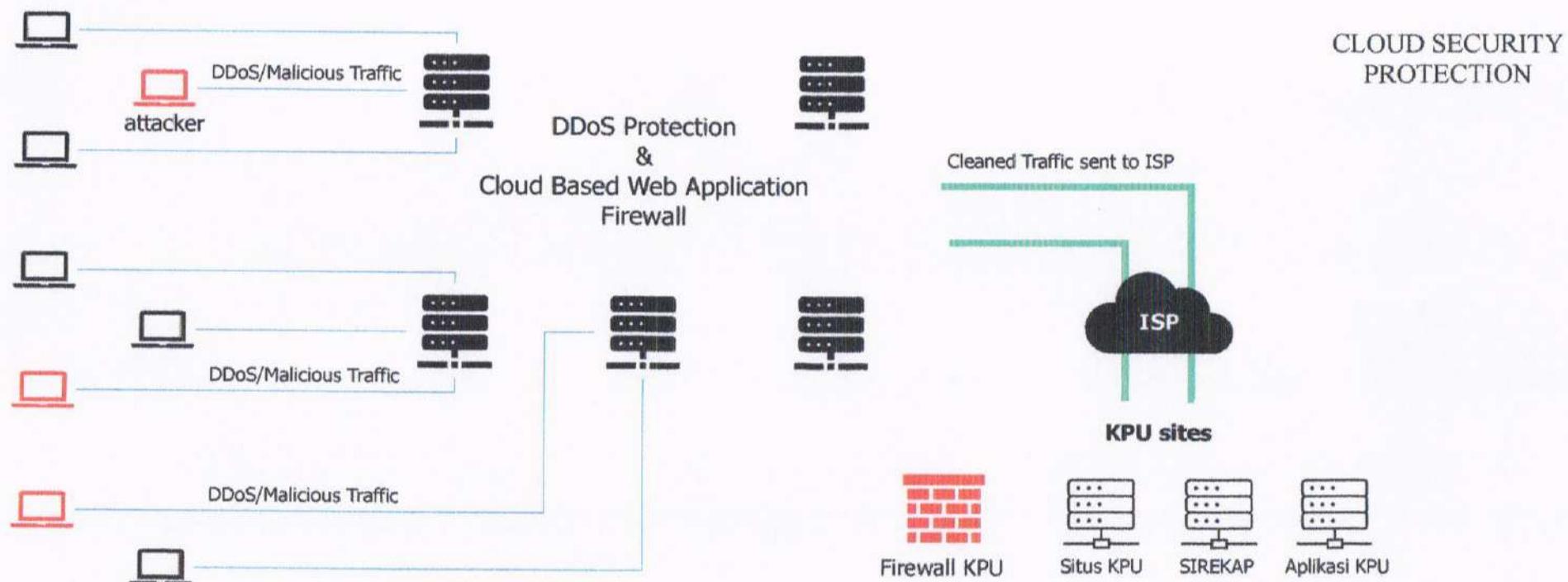
Keterangan ;

1. Simbol Kapsul/*Terminator* ( ■ ) untuk mendeskripsikan kegiatan mulai dan berakhir;

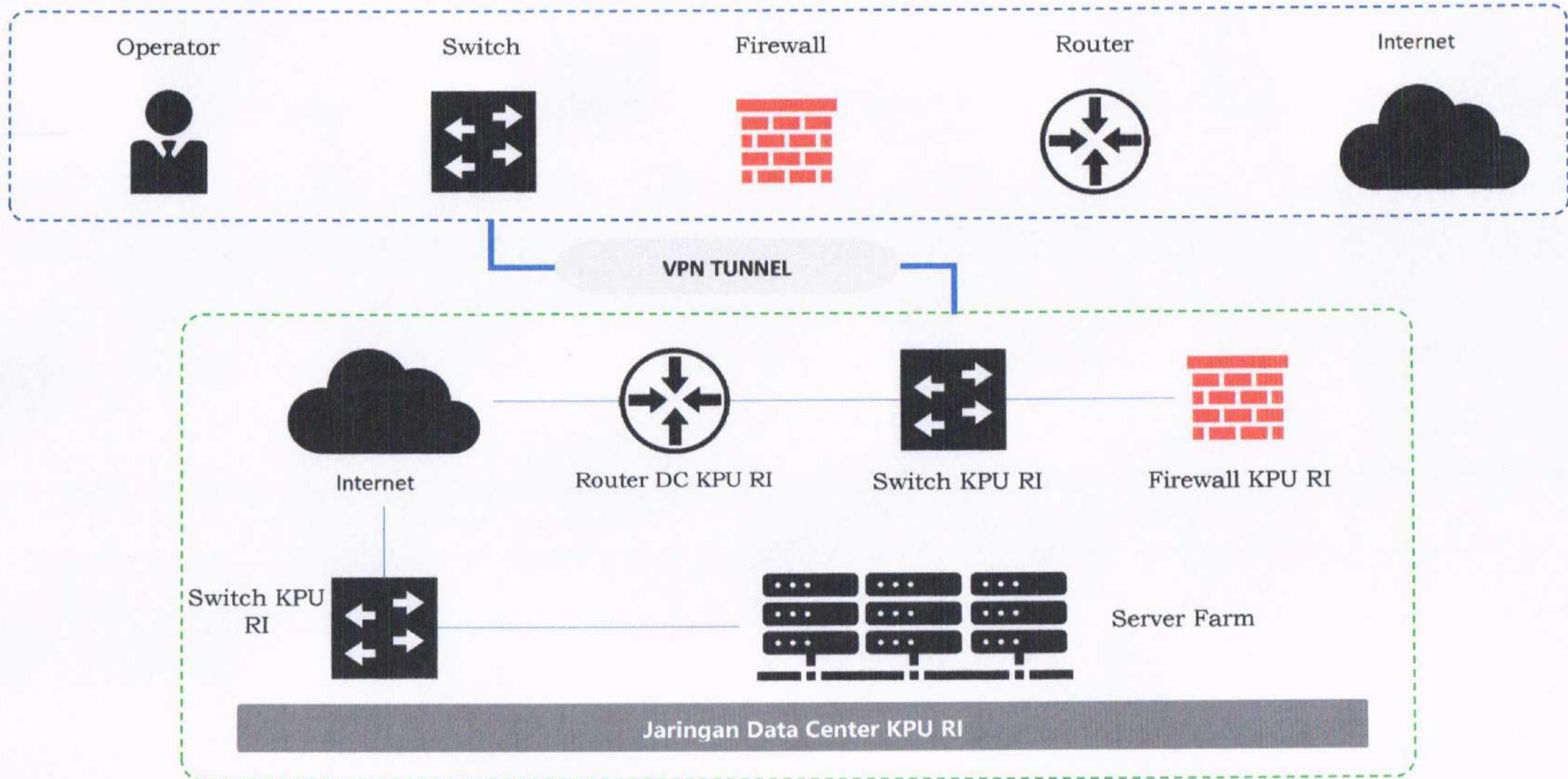
## **SISTEM INFORMASI DALAM TAHAPAN PELAKSANAAN PEMILU SERENTAK TAHUN 2024**

- 1 SIDALIH  
SISTEM INFOMASI DAFTAR PEMILIH  
Sistem yang membantu KPU dan Badan Adhoc dalam mengelola tahapan pemutakhiran Data Pemilih
- 2 SIPOL  
SISTEM INFORMASI PARTAI POLITIK  
Sistem yang mendukung dalam pengelolaan tahapan pendaftaran verifikasi dan penetapan parpol peserta Pemilu
- 3 SIDAPIL  
SISTEM INFORMASI DAERAH PEMILIHAN  
Sistem yang membantu KPU dalam mengelola dan menyusun Dapil DPRD Kab/Kota berserta jumlah alokasi kursinya berdasarkan 7 prinsip penataan dapil menggunakan peta digital
- 4 SILON  
SISTEM INFORMASI PENCALONAN  
Sistem yang mendukung dalam pengelolaan tahapan pencalonan DPR, DPD, DPRD Provinsi, DPRD Kab/Kota, Presiden dan Wakil Presiden serta Kepala Daerah
- 5 SILOG  
SISTEM INFORMASI LOGISTIK  
Sistem yang membantu KPU dan badan Adhoc dalam manajemen pengelolaan logistik kebutuhan Pemilu
- 6 SIDAKAM  
SISTEM INFOMASI DANA KAMPANYE  
Sistem yang mendukung dalam pengelolaan dana kampanye dan jadwal kampanye Parpol dan Peserta Pemilu
- 7 SIREKAP  
SISTEM INFORMASI REKAPITULASI  
Sistem yang mendukung dalam pengelolaan tahapan rekapitulasi hasil penghitungan suara
- 8 SIAKBA  
SISTEM INFORMASI ANGGOTA KPU DAN BADAN ADHOC  
Sistem Informasi Anggota KPU dan Badan Adhoc yang membantu KPU dalam pengelolaan data anggota KPU dan Badan Adhoc

# ARSITEKTUR KEAMANAN TI KPU



## JARINGAN INTERNET KPU KABUPATEN/KOTA



## PENGESAHAN

1. Standar Operasional Prosedur ini dibuat untuk dilaksanakan setiap bagian sebagaimana struktur organisasi yang telah ditetapkan.
2. Untuk mengantisipasi keadaan kahar, perubahan/revisi dapat dilakukan selama pelaksanaan Standar Operasional Prosedur ini.
3. Perubahan tidak berlaku untuk tahapan kegiatan yang sudah selesai dilaksanakan.
4. Perubahan terhadap ruang lingkup dan penanggung jawab kegiatan mengakibatkan Standar Operasional Prosedur ini batal seluruhnya.
5. Standar Operasional Prosedur ini berlaku pada saat ditandatangani.

Ditetapkan di Serang  
pada tanggal 23 Oktober 2023

KETUA KOMISI PEMILIHAN UMUM

KOTA SERANG,  
  
ADE JAHRAN

PARAF KOORDINASI		TANGGAL
Sekretaris		
Kepala Sub Bagian Hukum dan Sumber Daya Manusia		23/10 - 23
Kepala Sub Bagian Perencanaan, Data dan Informasi		23/10 23