KEMENTERIAN KESEHATAN REPUBLIK INDONESIA

GERMAS Gerakan Masyarakat Hidup Sehat

BLU SPEED

BerAKHLAK

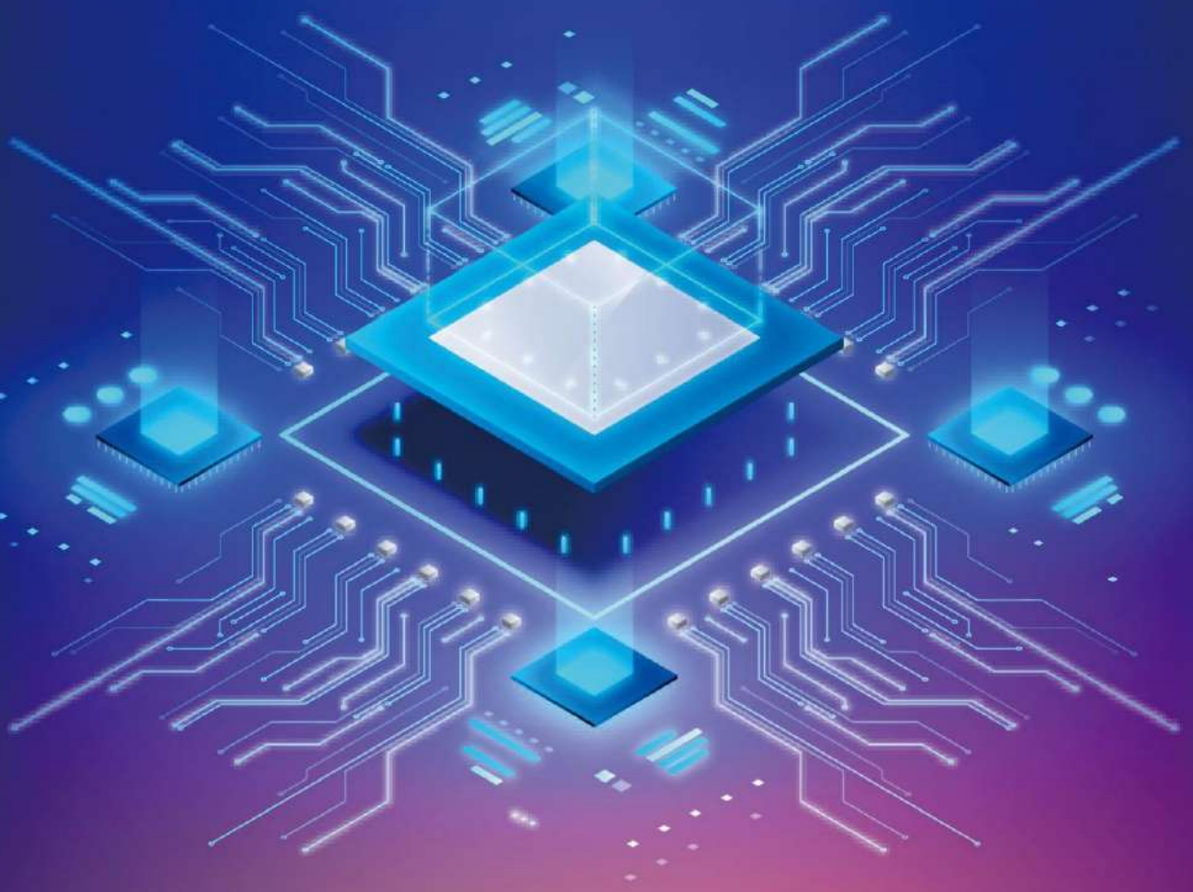
#bangga melayani bangsa

POLTEKNIK KESEHATAN SURAKARTA

STANDAR OPERASIONAL PROSEDUR (SOP)

UNIT TEKNOLOGI INFORMASI

POLTEKKES KEMENKES SURAKARTA



POLTEKKES KEMENKES SURAKARTA

JL. LETJEN SUTOYO, MOJOSONGO, JEBRES
SURAKARTA 57178
TELP. 0271-856929 FAX. 0271-855388

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan kelancaran dalam penyusunan Standar Operasional Prosedur (SOP) Unit Teknologi Informasi Poltekkes Kemenkes Surakarta. SOP ini merupakan penentu jalur teknis dan outcome suatu pelayanan dan pengembangan yang ada di Unit TI, sebagaimana terangkum dalam tugas dan fungsi Unit TI itu sendiri antara lain:

1. Menyediakan layanan fasilitas teknologi dan informasi
2. Menyediakan pengelolaan data dan informasi yang terintegrasi
3. Menyediakan sistem jaringan internet dan intranet sebagai fasilitas utama dalam pengaliran data dan informasi
4. Mengembangkan sistem informasi yang terintegrasi
5. Melakukan pelatihan guna menjamin terlaksananya pemanfaatan hardware dan software
6. Melakukan koordinasi dengan sub unit IT (PIC) di masing-masing jurusan

Unit TI sangat penting untuk mendukung terlaksananya sistem tata kelola yang baik, sehingga dalam menjalankan tugas dan fungsinya Unit TI harus terkendali sesuai dengan visi misi yang telah dicanangkan sewaktu Unit TI dibentuk, maka Standar Operasional Prosedur (SOP) adalah alur yang harus diikuti dalam setiap layanan dan pengembangan yang akan dilakukan sehingga tercipta pelayanan yang prima dan berkualitas, serta merupakan salah satu point dalam capaian kinerja Unit TI.

Semoga Standar Operasional Prosedur (SOP) yang telah disusun dan dibukukan dapat bermanfaat bagi kita semua terkhusus dalam memberikan pelayanan kepada segenap sivitas akademika Poltekkes Kemenkes Surakarta.

Surakarta, 26 Mei 2023
Direktur Poltekkes Kemenkes Surakarta,

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL TENAGA KESEHATAN

Sudiro, S.Kp, Ners, M.Pd
NIP. 196801041989031002

DAFTAR STANDAR OPERASIONAL PROSEDUR (SOP)

UNIT TEKNOLOGI INFORMASI

POLTEKKES KEMENKES SURAKARTA

SOP IT			
No	**Nama SOP**	**Tanggal Terbit**	**Tanggal Revisi**
1	SOP *Host to Host* Pembayaran Mahasiswa	DP.03.04/I.01/015.4/2017 3 Januari 2017	IR.01.02/1/2743/2023 26 Juni 2023
2	SOP Kartu Rencana Studi (KRS) Online	DP.03.04/I.01/015.5/2017 3 Januari 2017	IR.01.02/1/2731/2023 26 Juni 2023
3	SOP Pemeliharaan Jaringan Internet	DP.03.04/I.01/015.6/2017 3 Januari 2017	IR.01.02/1/2742/2023 26 Juni 2023
4	SOP Upload Materi Sistem Informasi Akademik (SIA)	DP.03.04/I.01/015.7/2017 3 Januari 2017	IR.01.02/1/2730/2023 26 Juni 2023
5	SOP Sistem Informasi Manajemen Aset	DP.03.04/1.1/7487.2/2019 8 Oktober 2019	IR.01.02/1/2760/2023 27 Juni 2023
6	Prosedur Sistem Manajemen Keamanan (*Security Awareness*) Sistem Informasi	DP.03.04/1.1/7487.1/2019 8 Oktober 2019	-
7	Kebijakan Pengendalian Hak Akses pada Area Layanan Publik Poltekkes Surakarta	DP.03.04/1.1/8137.1/2019 13 November 2019	-
8	SOP Informasi Keterbukaan Publik Melalui Website dan Media Sosial	DP.03.04/1.1/8137.2/2019 13 November 2019	-
9	SOP Pemenuhan Permintaan Akses	DP.03.04/1.1/8911/2019 9 Desember 2019	-
10	SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi	DP.03.04/1.1/8912/2019 9 Desember 2019	-
11	Prosedur Pengelolaan Akses Layanan Teknologi Informasi	DP.03.04/1.1/8913/2019 9 Desember 2019	-
12	Pedoman Teknik Pengendalian dan Pengelolaan Sistem Informasi di Lingkungan Politeknik Kesehatan Surakarta	DP.03.04/1.1/8914/2019 9 Desember 2019	-
13	SOP Hak Akses Ruang Server dan Mesin Server	DP.03.04/1.1/119/2020 2 Januari 2020	-
14	SOP Layanan *Troubleshooting* Server	IR.02/1/2376/2023 26 Mei 2023	-

SOP IT			
No	**Nama SOP**	**Tanggal Terbit**	**Tanggal Revisi**
15	SOP Layanan Pemeliharaan *Hardware* dan *Software* TI	IR.02/1/2375/2023 26 Mei 2023	-
16	SOP Permintaan Penambahan *Bandwidth*	IR.02/1/2374/2023 26 Mei 2023	-
17	SOP Pengembangan Sistem Informasi	IR.02/1/2373/2023 26 Mei 2023	-
18	SOP Manajemen Keamanan Sistem Informasi (SI)	IR.01.02/1/2704/2023 22 Juni 2023	-

LAMPIRAN STANDAR OPERASIONAL PROSEDUR (SOP)

UNIT TEKNOLOGI INFORMASI

POLTEKKES KEMENKES SURAKARTA

POLTEKKES KEMENKES SURAKARTA

JL. LETJEN SUTOYO, MOJOSONGO, JEBRES, SURAKARTA 57127

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.01.02/1/2743/2023
	Tanggal Pembuatan	3 Januari 2017
	Tanggal Revisi	26 Juni 2023
	Tanggal Efektif	26 Juni 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	***Host to Host* Pembayaran Mahasiswa**

Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi; 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	1. Prosedur ini berlaku bagi pelaksanaan *host to host* pembayaran di lingkungan Poltekkes Kemenkes Surakarta
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP KRS Online	1. Komputer/Laptop 2. Jaringan internet 3. Lembar tagihan mahasiswa aktif dan token pembayaran
Peringatan :	**Pencatatan dan Pendataan :**
1. Penambahan token pembayaran apabila token yang tersedia telah habis dan masih ada calon pendaftar yang ingin mendaftar 2. Masa pembayaran dapat diperpanjang apabila diperlukan 3. Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana				Mutu Baku			Keterangan
		Ka Unit IT	Bank	Bendahara Penerima	Mahasiswa/ Calon Pendaftar	Kelengkapan	Waktu	*Output*/*Outcome*	
1	Identifikasi kinerja dan monitoring server pembayaran dan server *host to host*					Laptop dengan aplikasi winbox dan form catatan	1 jam	Server selalu on dan terjaga koneksi dengan bank	
2	Memasukkan setting tagihan baik registrasi, her registrasi dan sipenmaru					Lembar tagihan, aplikasi pembayaran	2 minggu	Tagihan masuk ke server	
3	Mahasiswa melakukan pembayaran, apabila ada kendala status belum terbayar di aplikasi segera berkoordinasi dengan bendahara penerima dan Ka Unit IT melalui operator prodi masing-masing				Ya Tidak	Slip pembayaran	Sesuai waktu pembayaran	Slip pembayaran yang telah terverifikasi bank	
4	Melakukan pengecekan yang belum terbayar apabila mahasiswa memang telah membayar disertai dengan bukti slip pembayaran terverifikasi berkoordinasi dengan bank dan aplikasi support					Aplikasi pembayaran dan *host to host* dengan bank	1 jam	Hasil pengecekan aplikasi pembayaran dan *host to host* dengan bank	Tergantung tingkat kendala yang muncul maksimal 1x24 jam
5	Registrasi/her registrasi dapat melakukan proses berikutnya yaitu KRS online					Registrasi/her registrasi	1 jam	KRS online	

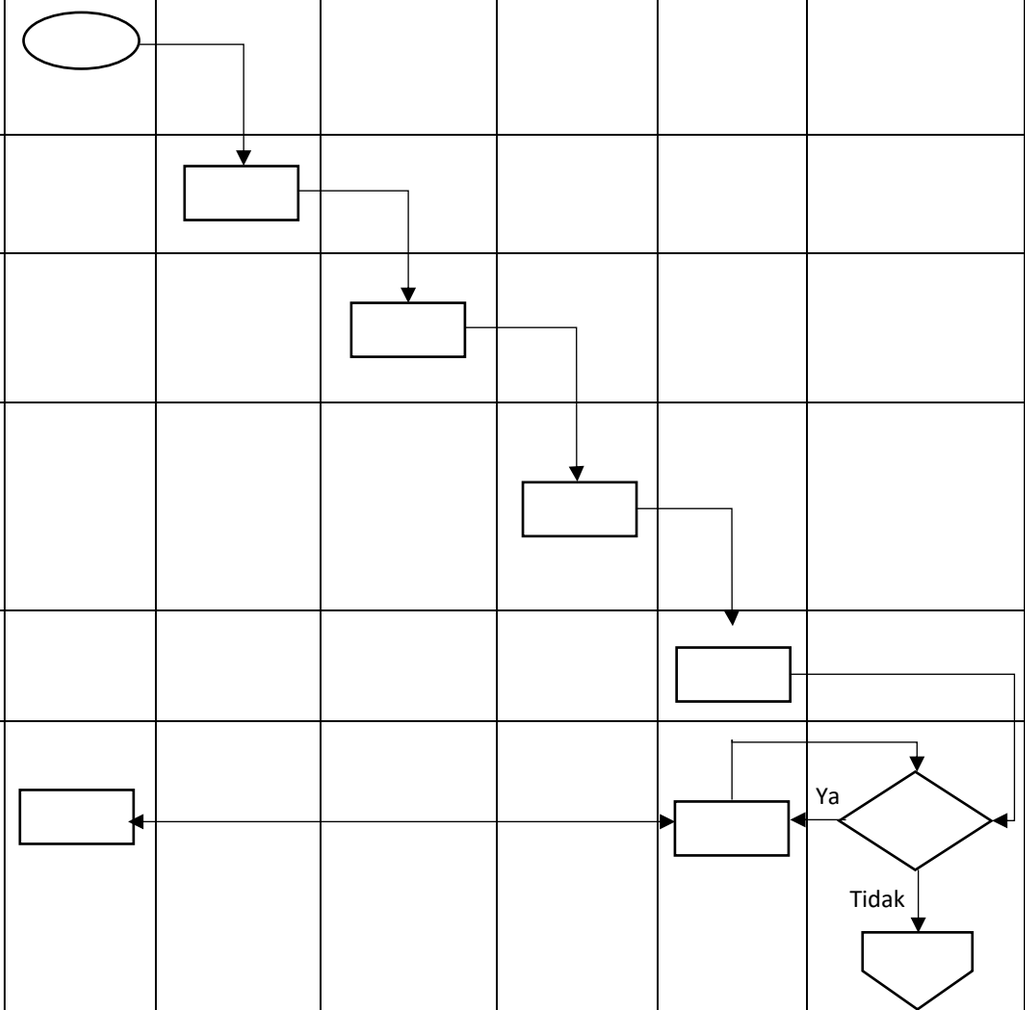
Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.01.02/1/2731/2023
	Tanggal Pembuatan	3 Januari 2017
	Tanggal Revisi	26 Juni 2023
	Tanggal Efektif	26 Juni 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Kartu Rencana Studi (KRS) Online**

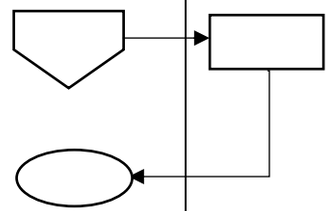
Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi; 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	1. Mengetahui tugas dan fungsi serta mekanisme pelaksanaan KRS online di tiap awal semester
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP *Host to Host* Pembayaran Mahasiswa 2. SOP Upload Materi Kuliah SIA	1. Komputer/Laptop 2. Jaringan internet 3. Data mahasiswa dan PBM semester yang akan berjalan 4. Aplikasi Sistem Informasi Akademik (SIA)
Peringatan :	**Pencatatan dan Pendataan :**
1. Keterlambatan dalam pengambilan KRS online 2. Perpanjangan waktu pengambilan KRS online 3. Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana							Mutu Baku			Keterangan
		Ka Unit IT	Sisfo ADAK	Bendahara	Sekretaris Jurusan	Admin Prodi	Mahasiswa	Pembimbing Akademik	Kelengkapan	Waktu	*Output/ Outcome*	
1	Setting awal semester yang akan berjalan								Laptop dengan aplikasi winbox dan form catatan	1 jam	Server selalu on dan terjaga koneksi dengan bank	
2	Integrasi data mahasiswa dari SIREG ke SIA								Lembar tagihan, aplikasi pembayaran	2 minggu	Tagihan masuk ke server	
3	Setting taggihan mahasiswa melalui aplikasi pembayaran								Slip pembayaran	Sesuai waktu pembayaran	Slip pembayaran yang telah terverifikasi bank	
4	Mempersiapkan data perkuliahan semester yang akan berjalan								Aplikasi pembayaran dan *host to host* dengan bank		Tergantung tingkat kendala yang muncul maksimal 1x24 jam	
5	Entry data perkiliahan ke back office SIA											
6	Mahasiswa melakukan KRS apabila tidak ada kendala dapat langsung mencetak KRS, apabila ada komplain dapat menghubungi admin prodi yang berkoordinasi dengan bendara dan Ka Unit IT											



Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana							Mutu Baku			Keterangan
		Ka Unit IT	Sisfo ADAK	Bendahara	Sekretaris Jurusan	Admin Prodi	Mahasiswa	Pembimbing Akademik	Kelengkapan	Waktu	*Output/ Outcome*	
7	Print out KRS Online ditandatangani oleh Pembimbing Akademik dan disimpan oleh mahasiswa											

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

<table>
<tr><td rowspan="4">KEMENTERIAN KESEHATAN REPUBLIK INDONESIA</td><td>Nomor SOP</td><td>IR.01.02/1/2742/2023</td></tr>
<tr><td>Tanggal Pembuatan</td><td>3 Januari 2017</td></tr>
<tr><td>Tanggal Revisi</td><td>26 Januari 2017</td></tr>
<tr><td>Tanggal Efektif</td><td>26 Januari 2017</td></tr>
<tr><td>DIREKTORAT JENDERAL TENAGA KESEHATAN</td><td>Disahkan oleh</td><td>Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta,
Sudiro, SKp, Ners, M.Pd
NIP 196801041989031002</td></tr>
<tr><td>POLTEKKES KEMENKES SURAKARTA</td><td>Nama SOP</td><td>Pemeliharaan Jaringan Internet</td></tr>
<tr><td>Dasar Hukum :</td><td colspan="2">Kualifikasi Pelaksanaan :</td></tr>
<tr><td>1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi;
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik</td><td colspan="2">1. Prosedur ini berlaku bagi pelaksanaan pemeliharaan jaringan internet wifi di lingkungan Poltekkes Kemenkes Surakarta</td></tr>
<tr><td>Keterkaitan dengan SOP lain :</td><td colspan="2">Peralatan yang digunakan :</td></tr>
<tr><td>1. SOP Layanan Pemeliharaan Hardware dan Software TI</td><td colspan="2">1. Komputer/Laptop
2. Jaringan internet</td></tr>
<tr><td>Peringatan :</td><td colspan="2">Pencatatan dan Pendataan :</td></tr>
<tr><td>Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada sistem aplikasi tidak dapat berjalan</td><td colspan="2">Disimpan dalam bentuk dokumen tercetak dan elektronik</td></tr>
</table>

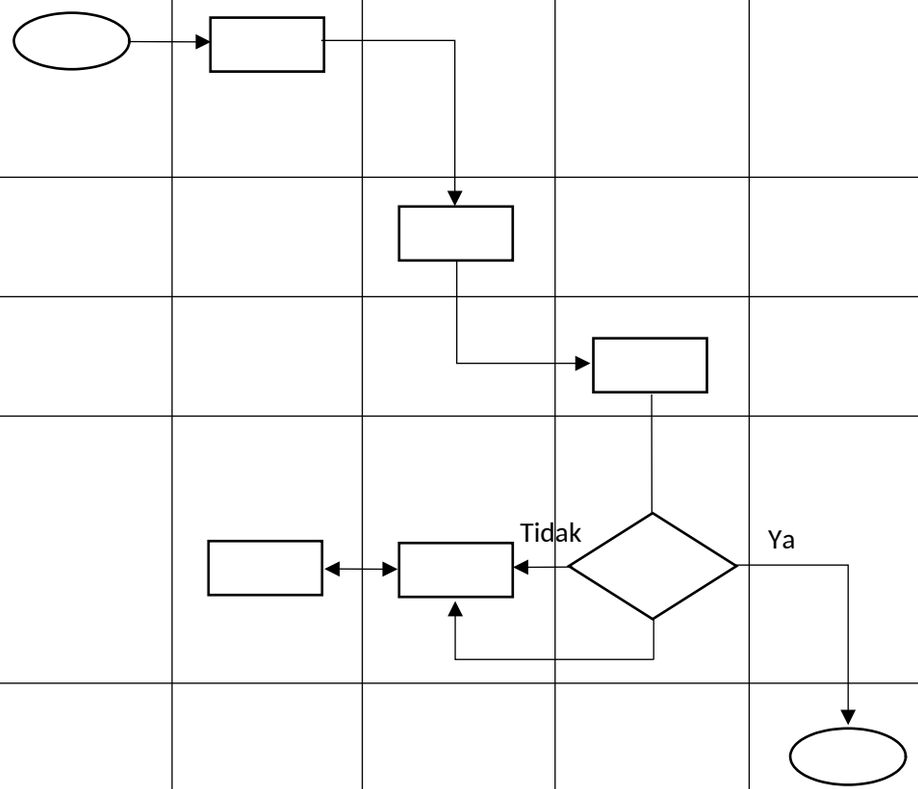
No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Ka Unit IT	Pengelola Sistem Jaringan/Rekanan	Ka Unit Pengadaan	Kelengkapan	Waktu	*Output/Outcome*	
1	Identifikasi dan pencatatan perangkat internet wifi sebulan sekali				Laptop dengan aplikasi winbox dan form catatan	1 jam	Identifikasi pencatatan perangkat	
2	Menerima laporan dari Ka Unit IT, menindaklanjuti dengan uji fungsi terhadap perangkat yang diidentifikasi tidak dapat bekerja dengan baik				Laporan uji fungsi perangkat	3 hari	Laporan uji fungsi perangkat	
3	Melakukan perbaikan perangkat dengan rekanan, apabila berhasil dilanjutkan dengan monitoring oleh Ka Unit IT, apabila tidak berhasil dilakukan penggantian perangkat baru berkoordinasi dengan Ka Unit Pengadaan	Tidak Ya			Laporan rekap spesifikasi dan rekomendasi penggantian perangkat	1 hari	Laporan rekap spesifikasi dan rekomendasi penggantian perangkat	
4	Memberikan persetujuan dan penggantian perangkat yang tidak dapat bekerja dengan baik				Laporan rekap penggantian perangkat, kwitansi	Estimasi waktu tergantung ketersediaan dan waktu pengiriman barang pada e-katalog	Laporan rekap penggantian perangkat, kwitansi	
5	Mengganti perangkat hingga perangkat dapat bekerja dengan normal kembali				Penggantian perangkat	1 jam	Perangkat telah diperbaiki	
6	Menerima laporan penggantian perangkat				Laporan penggantian perangkat dan perbaikan	1 jam	Laporan penggantian perangkat dan perbaikan	

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.01.02/1/2730/2023
	Tanggal Pembuatan	3 Januari 2017
	Tanggal Revisi	26 Juni 2023
	Tanggal Efektif	26 Juni 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Upload Materi Sistem Informasi Akademik (SIA)**

Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi; 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	1. Prosedur ini berlaku bagi pelaksanaan upload materi kuliah pada semester aktif di semua prodi yang ada
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi 2. SOP Layanan Pemeliharaan *Hardware* dan *Software* TI	1. Komputer/Laptop 2. Jaringan internet 3. Softcopy file materi kuliah 4. Aplikasi Sistem Informasi Akademik (SIA)
Peringatan :	**Pencatatan dan Pendataan :**
Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana					Mutu Baku			Keterangan
		Kasubag ADAK	Ka Unit IT	Admin Prodi	Dosen	Mahasiswa	Kelengkapan	Waktu	*Output/ Outcome*	
1	Kasubag ADAK menginstruksikan setting awal semester yang akan berjalan dan informasi ke Ka Unit IT untuk proses pembayaran, entry perkuliahan/jadwal kelas dan dosen pengampu MK serta KRS						Jadwal akademik semester	1 jam	Distribusi mata kuliah dan dosen	
2	Entry dosen MK dan jadwal kelas semua kelas yang ada di semester aktif						Jadwal akademik semester	1 hari	Distribusi mata kuliah dan dosen telah di entry	
3	Menyiapkan file upload materi MK maksimal 10 Mb dengan format .zip						File materi MK	1 hari	File materi MK dalam format zip	
4	Upload materi MK sesuai dengan kelas yang diampu, apabila berhasil file akan tersimpan dan terbaca di portal mahasiswa, apabila gagal koordinasi dengan admin prodi dan Ka Unit IT untuk membantu						File materi MK	1 hari	File materi MK telah terupload	
5	Mengakses materi kuliah melalui portal SIA mahasiswa dan mendownload file tersebut						Akses materi kuliah	1 jam	File materi MK telah terdownload	



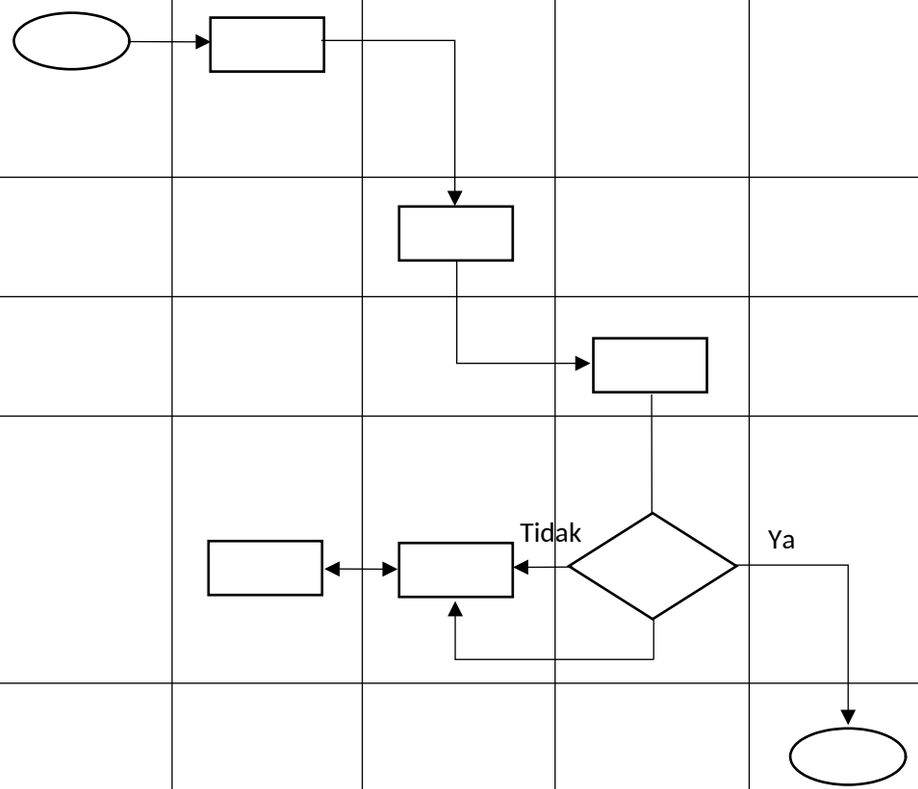
Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.01.02/1/2730/2023
	Tanggal Pembuatan	3 Januari 2017
	Tanggal Revisi	26 Juni 2023
	Tanggal Efektif	26 Juni 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Upload Materi Sistem Informasi Akademik (SIA)**

Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi; 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	1. Prosedur ini berlaku bagi pelaksanaan upload materi kuliah pada semester aktif di semua prodi yang ada
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi 2. SOP Layanan Pemeliharaan *Hardware* dan *Software* TI	1. Komputer/Laptop 2. Jaringan internet 3. Softcopy file materi kuliah 4. Aplikasi Sistem Informasi Akademik (SIA)
Peringatan :	**Pencatatan dan Pendataan :**
Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana					Mutu Baku			Keterangan
		Kasubag ADAK	Ka Unit IT	Admin Prodi	Dosen	Mahasiswa	Kelengkapan	Waktu	*Output/ Outcome*	
1	Kasubag ADAK menginstruksikan setting awal semester yang akan berjalan dan informasi ke Ka Unit IT untuk proses pembayaran, entry perkuliahan/jadwal kelas dan dosen pengampu MK serta KRS						Jadwal akademik semester	1 jam	Distribusi mata kuliah dan dosen	
2	Entry dosen MK dan jadwal kelas semua kelas yang ada di semester aktif						Jadwal akademik semester	1 hari	Distribusi mata kuliah dan dosen telah di entry	
3	Menyiapkan file upload materi MK maksimal 10 Mb dengan format .zip						File materi MK	1 hari	File materi MK dalam format zip	
4	Upload materi MK sesuai dengan kelas yang diampu, apabila berhasil file akan tersimpan dan terbaca di portal mahasiswa, apabila gagal koordinasi dengan admin prodi dan Ka Unit IT untuk membantu						File materi MK	1 hari	File materi MK telah terupload	
5	Mengakses materi kuliah melalui portal SIA mahasiswa dan mendownload file tersebut						Akses materi kuliah	1 jam	File materi MK telah terdownload	



Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.01.02/1/2760/2023
	Tanggal Pembuatan	8 Oktober 2019
	Tanggal Revisi	27 Juni 2023
	Tanggal Efektif	27 Juni 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Sistem Informasi Manajemen Aset**

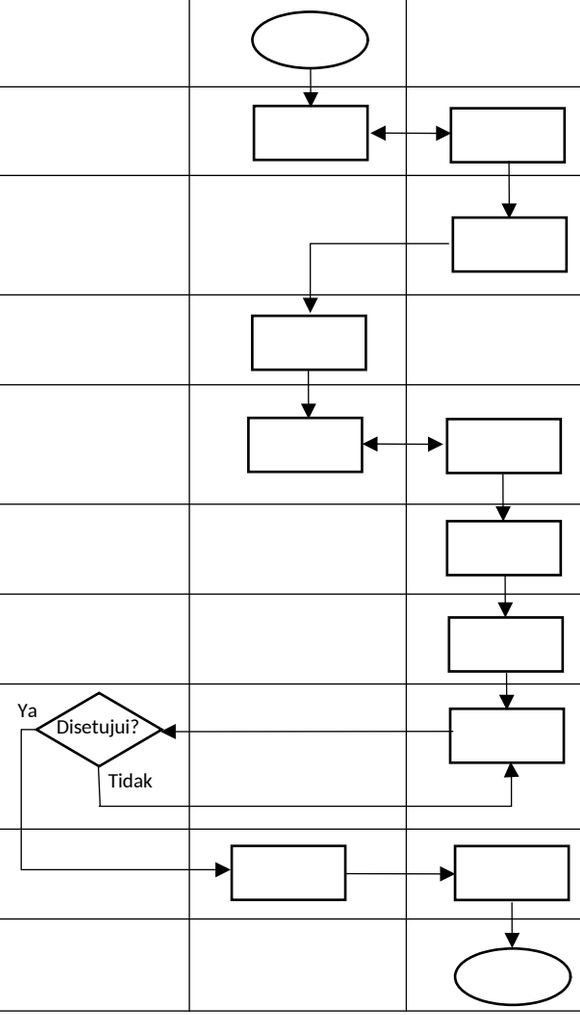
Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi; 2. Undang-Undang Nomor 17 Tahun 2003 tentang Keuangan Negara 3. Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara 4. Peraturan Presiden Nomor 27 Tahun 2014 tentang Pengelolaan Barang Milik Negara/Daerah 5. Peraturan Menteri Keuangan RI Nomor 120/PMK.06/2007 tentang Penatausahaan BMN 6. Surat Edaran Menteri Kesehatan Nomor KU/Menkes/471/VIII/2013 tentang Kebijakan Aktansi Penatausahaan Persediaan Kementerian Kesehatan	1. Memahami tentang penatausahaan barang persediaan 2. Memahami tentang jenis barang persediaan 3. Memahami cara penggunaan 4. aplikasi sistem informasi manajemen aset

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

Keterkaitan dengan SOP lain :	Peralatan yang digunakan :
1. SOP Penyusunan Laporan Persediaan 2. SOP Rekonsiliasi Internal Persediaan 3. SOP Stok Opname Fisik Persediaan 4. SOP Pemeriksaan Persediaan di Direktorat dan Jurusan	1. Komputer/Laptop 2. Jaringan internet 3. Laporan Persediaan 4. Laporan Stok Opname 5. Aplikasi Persediaan
Peringatan :	**Pencatatan dan Pendataan :**
1. Apabila tidak dilakukan stock opname persediaan, kesediaan barang persediaan secara fisik tidak diketahui 2. Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Ka Unit Pengadaan	Pengelola BMN Direktorat	Unit Pengelola BMN Jurusan	Kelengkapan	Waktu	*Output/ Outcome*	
1	Persiapan data master				Data master	1 jam	Data master	
2	Pendataan gedung dan ruang				Manajemen referensi	1 minggu	Data gedung dan ruang	
3	Pendataan barang exsisting inventaris dalam ruang				Manajemen gedung dan ruang	1 minggu	Data barang dan ruangan	
4	Mendata barang perolehan baru				Manajemen barang	1 jam	Data BMN	
5	Mengupdate status kondisi barang				Manajemen inventarisasi aset	1 jam	Kondisi barang	
6	Mengupdate lokasi barang dalam satu unit				Manajemen inventarisasi aset	1 jam	Data BMN	
7	Memutasi barang antar unit kerja				Manajemen barang	30 menit	Data BMN	
8	Mengusulkan BHP				Manajemen BHP	1 hari	Data master	
9	Menambah BHP ke dalam Gudang				Manajemen BHP	1 hari	Data BHP	
10	Melakukan register transaksi harian				Manajemen BHP	30 menit	Data BHP Harian	



Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.04/1.1/7487.1/2019
	TANGGAL PEMBUATAN	8 Oktober 2019
	TANGGAL REVISI	
	TANGGAL EFEKTIF	
	DISAHKAN OLEH	Direktur Satino, SKM, MScN NIP. 196101021989031001

PROSEDUR SISTEM MANAJEMEN KEAMANAN (SECURITY AWARENESS) SISTEM INFORMASI

PROSEDUR SISTEM MANAJEMEN KEAMANAN INFORMASI

1. Pendahuluan

Informasi merupakan aset yang sangat penting bagi Instansi 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

Melindungi aset informasi Instansi penyelenggara layanan publik dari segala bentuk ancaman, baik eksternal maupun internal, sengaja atau tidak.

3. Ruang lingkup

Kebijakan ini berlaku untuk seluruh aset informasi yang digunakan Instansi penyelenggara layanan publik yang meliputi:

3.1. Organisasi dan Lokasi

Seluruh unit kerja di Instansi penyelenggara layanan publik dan lokasi kerja yang digunakan untuk mengelola dan menyediakan layanan internal dan eksternal instansi penyelenggara layanan publik

3.2 Aset

Aset yang dicakup meliputi:

- Data dan Informasi
  Termasuk data dan informasi meliputi: dokumen pengadaan dan kontrak, data pelanggan, data gaji, data pegawai, sistem dokumentasi manajemen, dokumen teknis & konfigurasi jaringan, hasil penetration test, materi pelatihan, prosedur operasional, *business continuity plan*, dan hasil audit
- Software
  Yang termasuk dalam aset perangkat lunak atau software antara lain : software aplikasi, operating system, development tool, dan software tool (antivirus, audit tool)
- Hardware
  Yang termasuk dalam aset perangkat keras atau hardware misalnya :Server, PC, Laptop, media penyimpan data
- Perangkat Jaringan Komunikasi
  Yang termasuk dalam aset perangkat jaringan komunikasi antara lain Router, Modem, Switch, Kabel, Firewall
- Fasilitas Pendukung
  Yang termasuk dalam aset fasilitas pendukung antara lain Ruang Server / Ruang Data Center, Ruang Kerja, Ruang Disaster Recovery Center (DRC), UPS, Genset, A/C, CCTV, Fire Extinguisher, Access Door Electronic, dan sebagainya;
- Sumber Daya Manusia
  Yang termasuk dalam aset sumber daya manusia misalnya pegawai tetap, calon pegawai tetap, pegawai kontrak, mitra, vendor dan pihak ketiga lainnya yang menyediakan layanan, jasa, serta produk yang menunjang bisnis Instansi penyelenggara layanan publik.

4. Kebijakan

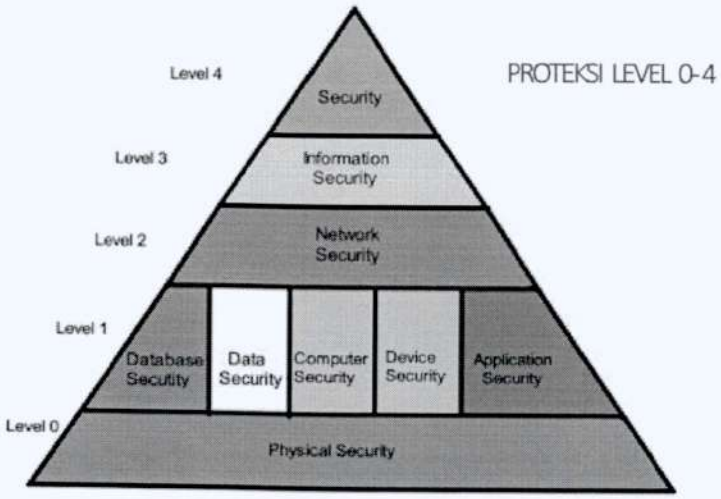
- Seluruh informasi yang disimpan dalam media simpan, ditulis, dicetak, dan dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi terhadap kemungkinan kerusakan, kesalahan penggunaan secara sengaja atau tidak, dicegah dari akses oleh user yang tidak berwenang dan dari ancaman terhadap kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability).
- Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
- Instansi penyelenggara layanan publik meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi pegawai. Sosialisasi juga perlu diberikan kepada vendor, konsultan, mitra, dan pihak ketiga lainnya sepanjang diperlukan.
- Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TI harus segera dilaporkan ke penanggung jawab TI terkait.
- Seluruh pimpinan di semua tingkatan bertanggungjawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya.
- Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan
- Setiap pelanggaran terhadap kebijakan ini yang relevan dapat dikenai sanksi atau tindakan disiplin sesuai peraturan yang berlaku.
- Kebijakan yang lebih teknis merujuk prinsip-prinsip yang ditetapkan dalam kebijakan ini.
- Setiap pengecualian terhadap kebijakan ini dan kebijakan turunnya harus mendapat persetujuan minimum dari pejabat yang berwenang

5. PROTEKSI

Skema Klasifikasi Informasi

RAHASIA	Aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran usaha instansi/lembaga secara temporer atau mengganggu citra dan reputasi perusahaan. Contoh: data wajib pajak, rencana mutasi, IP address, password komputer, laporan audit, data gaji dan penilaian kinerja karyawan, dan data kesehatan pribadi yang secara legal harus dilindungi instansi/lembaga.
INTERNAL	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan risiko penyebarannya secara tak berwenang tidak menimbulkan kerugian signifikan. Contoh: kebijakan instansi/lembaga, panduan kerja, prosedur kerja, instruksi kerja, memo / publikasi internal, bahan / materi training, informasi yang disediakan dalam intranet, dan data operasional TI lainnya.
PUBLIK	Informasi yang secara sengaja disediakan instansi/lembaga untuk dapat diketahui publik. Contoh: brosur marketing, situs publik dan siaran pers.

1. Tingkatan Level



- **Keamanan level 0**
  - Keamanan fisik, merupakan keamanan tahap awal dari komputer security. Jika keamanan fisik tidak terjaga dengan baik, maka data-data bahkan hardware komputer sendiri tidak dapat diamankan
- **Keamanan level 1**
  - keamanan database
  - keamanan data
  - keamanan dari PC itu sendiri
  - keamanan device
  - keamanan application

- **Keamanan level 2**
  - Keamanan jaringan
  - Komputer yang terhubung dengan jaringan sangat rawan dalam masalah keamanan, oleh karena itu keamanan level 2 harus dirancang supaya tidak terjadi kebocoran jaringan, akses ilegal yang dapat merusak keamanan data tersebut.
- **Keamanan level 3**
  - Keamanan informasi
  - Keamanan informasi kadang tidak dipedulikan oleh administrator, seperti memberikan *password* ke teman, atau menuliskannya dikertas.
- **Keamanan level 4**
  - merupakan keamanan secara keseluruhan dari komputer
  - Jika level 1-3 sudah dapat dikerjakan dengan baik maka otomatis keamanan untuk level 4 sudah tercapai

POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.04/1.1/8137.1/2019
	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

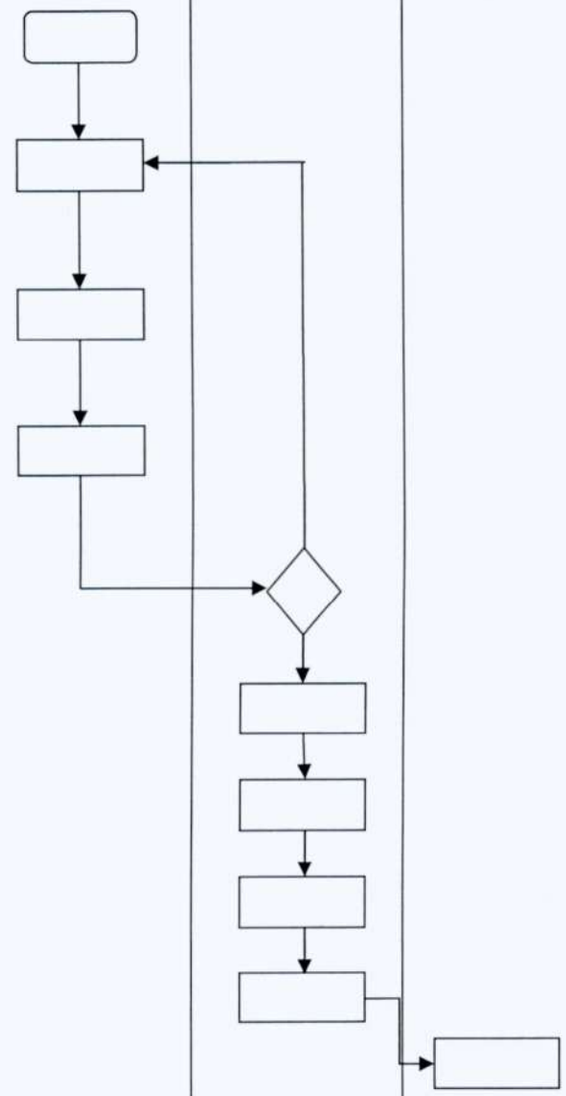
- **Akses Pihak Ketiga :**
  - Vendor, konsultan, mitra, atau pihak ketiga lainnya yang melakukan akses fisik atau lojik ke dalam aset harus menandatangani Ketentuan/Persyaratan Menjaga Kerahasiaan Informasi.
  - Hak akses pihak ketiga hanya diberikan berdasarkan kepentingan yang disahkan melalui kerjasama 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

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	DP.03.04/1.1/8137.2/2019
	Tanggal Pembuatan	13 November 2019
	Tanggal Revisi	
	Tanggal Efektif	
BADAN PENGEMBANGAN DAN PEMBERDAYAAN SUMBER DAYA MANUSIA KESEHATAN	Disahkan Oleh	Direktur Satino, SKM., MScN NIP. 196101021989031001
POLITEKNIK KESEHATAN KEMENKES SURAKARTA	Nama SOP	**Informasi Keterbukaan Publik Melalui Website dan Media Sosial**

Dasar Hukum	**Kualifikasi Pelaksanaan**
1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 2. Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik 3. Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia Nomor 75 Tahun 2016 tentang Layanan Informasi Publik di Lingkungan Kementerian Riset, Teknologi, dan Pendidikan Tinggi	1. Menghimpun dokumentasi informasi kegiatan di lingkungan Poltekkes Kemenkes Surakarta 2. Menyampaikan informasi publik yang diperoleh dari seluruh unit kerja di lingkungan Poltekkes Kemenkes Surakarta 3. Meningkatkan pengelolaan informasi publik melalui website 4. Menyediakan dan pemberian layanan informasi publik yang bersifat terbuka
Keterkaitan dengan SOP Lain	**Peralatan yang digunakan**
	1. Laptop / Personal Komputer 2. Kamera 3. Alat Tulis 4. Koneksi Internet 5. Dokumen
Peringatan	**Pencatatan dan Pendataan**
Apabila SOP ini tidak dijalankan maka dapat berakibat : 1. Keterlambatan dalam penyampaian informasi publik melalui website dan media sosial 2. Keterlambatan terselesaikannya suatu tanggung jawab yang informasinya belum tercantum di website dan media sosial 3. Tidak terdokumentasikannya kegiatan dan berkas kegiatan di website dan media sosial 4. Tidak tersampaikannya hak dan kewajiban yang bisa diakses oleh publik	Disimpan dalam bentuk dokumen softcopy dan laporan status keterbukaan publik

NO	AKTIFITAS	PELAKSANA			MUTU BAKU			KET
		PELAKSANA KEGIATAN	UNIT IT	WADIR I dan KAPUS JAMINTU	KELENGKAPAN	WAKTU	OUTPUT	
1	Melakukan identifikasi terkait informasi yang akan didokumentasikan pada unit di lingkungan Poltekkes Kemenkes Surakarta				Kamera, Alat Tulis, Berita Acara	45 Menit	Narasi/deskripsi kegiatan yang meliputi 5W 1 H atau SK atau Foto Kegiatan	
2	Melakukan koordinasi dengan pimpinan unit/panitia/pelaksana kegiatan dalam menghimpun serta mendokumentasikan data untuk informasi publik					15 Menit		
3	Mengumpulkan data dan informasi yang dibutuhkan dari berbagai sumber dalam mendokumentasikan informasi public				Kamera dan Alat Tulis	30 Menit		
4	Mengolah dan menyusun data hasil informasi yang telah didokumentasikan dalam bentuk softfile (narasi/deskripsi/konten kegiatan yang meliputi 5W 1 H atau SK atau Foto Kegiatan)				Laptop	60 Menit		
5	Menyerahkan hasil dokumen informasi dari Unit/ Panitia/ Pelaksana Kegiatan ke Unit IT untuk dipublikasikan melalui website dan medsos				Printout Narasi	10 Menit	Narasi dalam bentuk softcopy	
6	Melakukan koreksi terhadap dokumen publik				Softcopy Narasi dan Foto	15 Menit		
7	Melakukan dokumentasi serah terima dokumen publik				Printout Narasi	5 Menit		
8	Dokumen informasi diupload di website				Laptop	30 Menit		
9	Dokumen informasi disimpan sebagai arsip				Printout Log			
10	Membuat status keterbukaan publik						Log status keterbukaan publik	
11	Melaporkan kepada pimpinan							



Catatan

Website dan media sosial merupakan official website dan media sosial dari Politeknik Kesehatan Surakarta

Website

Beralamatkan di https://poltekkes-solo.ac.id

Media Sosial

Instagram : @polkesta.official

Twitter : @polkesta

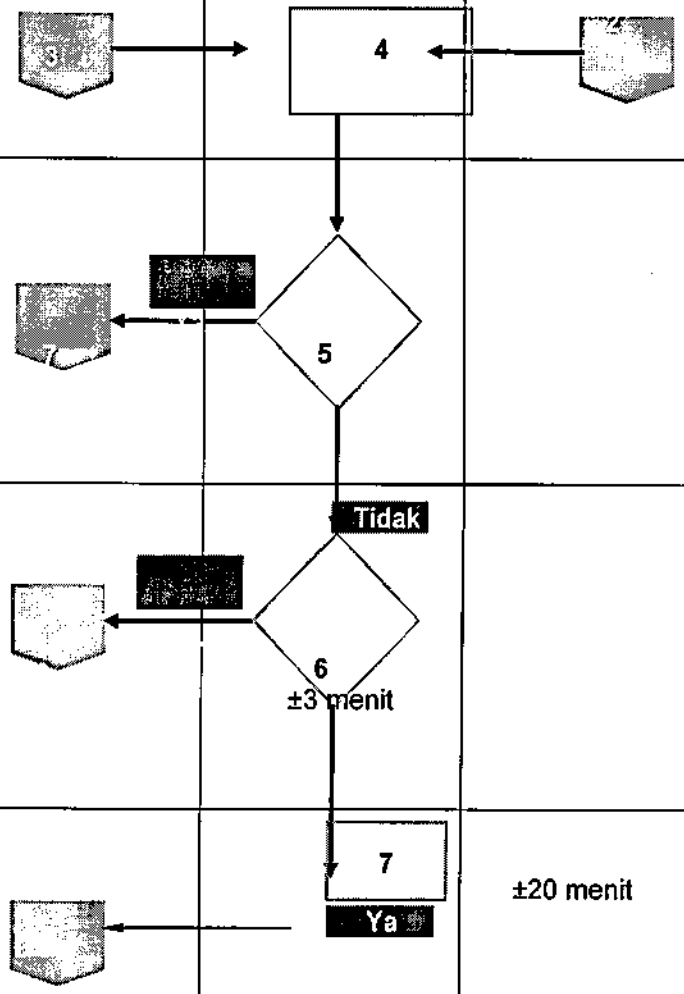
KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	DP.03.09/1.1/8911/2019
	Tanggal Pembuatan	9 Desember 2019
	Tanggal Revisi	
	Tanggal Efektif	
BADAN PENGEMBANGAN DAN PEMBERDAYAAN SUMBER DAYA MANUSIA KESEHATAN	Disahkan Oleh	Direktur Satino, SKM, MScN NIP. 196101021989031001
POLITEKNIK KESEHATAN KEMENKES SURAKARTA	Nama SOP	**Pemenuhan Permintaan Akses**

Dasar Hukum	**Kualifikasi Pelaksanaan**
1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 2. Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik 3. Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia Nomor 75 Tahun 2016 tentang Layanan Informasi Publik di Lingkungan Kementerian Riset, Teknologi, dan Pendidikan Tinggi	1. Menetapkan kebutuhan dan kepentingan pemohon hak akses 2. Menerbitkan hak akses
Keterkaitan dengan Aaturan Lain	**Peralatan yang digunakan**
1. Kebijakan Pengendalian Hak Akses 2. Pedoman Teknik Pengendalian dan Pengelolaan Sistem INformasi 3. Pedoman Security Awareness	1. Laptop / Personal Komputer 2. Alat Tulis 3. Koneksi Internet 4. Dokumen
Peringatan	**Pencatatan dan Pendataan**
Apabila SOP ini tidak dijalankan maka dapat berakibat : 1. Pemenuhan hak akses yang dilaporakan oleh klien akan tertunda dan mengakibatkan waktu pemenuhan permintaan semakin lama	Disimpan dalam bentuk hardcopy

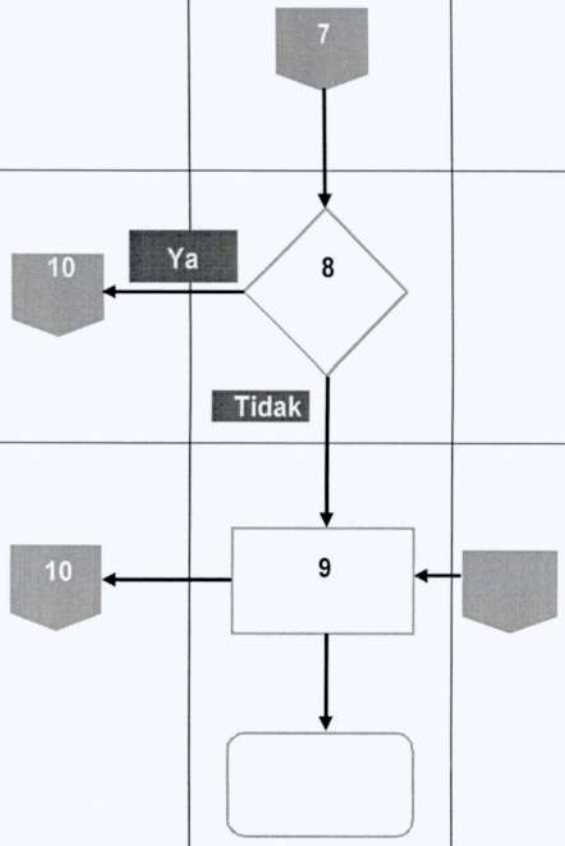
ALUR TAHAPAN PROSEDUR PEMENUHAN PERMINTAAN AKSES

No	Aktivitas	Pelaksana		Mutu Baku	
		Klien	Service Desk Operator	Syarat	Waktu
1	Menghubungi service desk operator untuk melaporkan permintaan akses	1			
2	Memeriksa apakah pelaporan permintaan akses tercatat melalui aplikasi service desk - Jika ya, maka lanjutkan ke aktivitas no 4 - Jika tidak, maka lanjutkan ke aktivitas no 3	4	2 Tidak	±2 menit	
3	Mengisikan formulir buat pada aplikasi service desk	4	3	±2 menit	

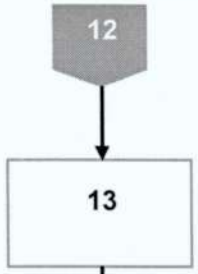
4	Mengidentifikasi perubahan hak akses klien berdasarkan status pengguna saat ini				±3 menit
5	Apakah perlu dilakukan pengurangan atau pencabutan hak akses? - Jika ya, maka lanjutkan pada aktivitas no 7 - Jika tidak, maka lanjutkan pada aktivitas no 6				±3 menit
6	Apakah diperlukan dilakukan penambahan hak akses? - Jika ya, maka lanjutkan pada aktivitas no 7 - Jika tidak, maka lanjutkan pada aktivitas no 9				
7	Melakukan verifikasi terhadap identitas klien, memastikan status klien dan haknya terhadap layanan yang diminta				±20 menit



8	Berdasarkan hasil verifikasi, apakah pengguna berhak mendapatkan hak akses tersebut? - Jika ya, maka lanjutkan pada aktivitas no 10 - Jika tidak, maka lanjutkan pada aktivitas no 9				±2 menit
9	Menginformasikan pada pengguna bahwa permintaan akses terhadap layanan yang diajukan tidak dapat dipenuhi dan mengubah status tiket selesai				±3 menit



10	Menyediakan hak akses untuk pengguna pada layanan TI yang diminta		9 10		±15 menit
11	Mendokumentasikan pemberian hak akses layanan TI		11		±5 menit
Penutupan Permintaan Akses					
12	Menginformasikan kepada klien bahwa pemenuhan permintaan akses telah diselesaikan dan mengirimkan link penanganan akses		12 13		±2 menit

13	Melakukan pengecekan kategorisasi dan kelengkapan pencatatan permintaan akses				±1 menit
14	Melakukan penutupan permintaan akses dan merubah status pemenuhan permintaan akses				±1 menit

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	DP.03.04 / 1.1 / 8912 / 2019
	Tanggal Pembuatan	9 Desember 2019
	Tanggal Revisi	
	Tanggal Efektif	
BADAN PENGEMBANGAN DAN PEMBERDAYAAN SUMBER DAYA MANUSIA KESEHATAN	Disahkan Oleh	Direktur Satino, SKM., MScN NIP. 196101021989031001
POLITEKNIK KESEHATAN KEMENKES SURAKARTA	Nama SOP	**Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi**

Dasar Hukum	**Kualifikasi Pelaksanaan**
1. Peraturan menteri kesehatan RI, Nomor 86 Tahun 2014 tentang Standart Pedoman Pengusulan Pengadaan, Serta Pemeliharaan dan Operasional kendaraan dinas lingkungan Kementerian Kesehatan 2. Peraturan Menteri Keuangan Nomor 78/PMK.06/2014 Tata Cara Pemanfaatan BMN	1. Melayani laporan gangguan perangkat komputer dan jaringan internet 2. Melayani laporan gangguan aplikasi (*software*) 3. Memelihara sarana dan prasarana teknologi informasi
Keterkaitan dengan SOP Lain	**Peralatan yang digunakan**
1. SOP Pengerjaan Perbaikan BMN 2. SOP Pengadaan Barang dan Jasa 3. SOP Pemeliharaan Sarana dan Prasarana	1. Laptop / Personal Komputer 2. Software Tools 3. Google Form 4. Hardware Tools 5. Koneksi Internet
Peringatan	**Pencatatan dan Pendataan**
Apabila SOP ini tidak dijalankan maka dapat berakibat : 1. Keterlambatan dalam perbaikan sarana dan prasarana pembelajaran dan perkantoran 2. Terganggunya proses belajar mengajar dan kegiatan perkantoran 3. Ketidaknyamanan dalam pekerjaan	Disimpan dalam bentuk dokumen softcopy dan dokumen cetak

		PELAKSANA				MUTU BAKU			KET
NO	AKTIFITAS	PELAPOR	PJ IT KAMPUS	SEKJUR	DIREKTORAT	KELENGKAPAN	WAKTU	OUTPUT	
1	Pelapor melaporkan kerusakan atau masalah yang dialami			YA		Mengisi form pengaduan di bit.ly/SIYANTI	5 Menit	Form Pelaporan	
2	Unit IT Kampus menerima laporan dari form pelaporan. Menindak lanjuti dengan memeriksa perangkat yang dilaporkan					Tools perbaikan sesuai laporan	15 Menit	Analisis Kerusakan. Hasil Analisis	
3	Jika kerusakan bisa ditangani. Langsung dikerjakan di lokasi.						1 Jam	Laporan Di form bit.ly/INFOYANTI	
4	Jika memerlukan pergantian hardware, dilaporkan ke Sekretaris Jurusan					Rekomendasi Unit IT	5 Menit		
5	Pelapor menerima proses							Proses pengerjaan di form bit.ly/INFOYANTI	

	pengerjaan								
6	Dikirim ke Unit IT Direktorat dilanjutkan ke bagian ULP					Piranti yang rusak	1 – 7 Hari Kerja	Perkembangan proses di form bit.ly/INFOYANTI	
7	Unit dikembalikan ke Pelapor melalui Jurusan								

POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.04/1.1/8913 /2019
	TANGGAL PEMBUATAN	9 Desember 2019
	TANGGAL REVISI	
	TANGGAL EFEKTIF	
	DISAHKAN OLEH	Direktur Satino, SKM., MScN NIP. 196101021989031001

PROSEDUR
PENGELOLAAN AKSES LAYANAN TEKNOLOGI INFORMASI

PROSEDUR
PENGELOLAAN AKSES LAYANAN TEKNOLOGI INFORMASI

OPERATING LEVEL AUTHORITY (OLA) AND SERVICE LEVEL AUTHORITY(SLA)

RUANG LINGKUP KONTEN SOP

Tabel 1 Ruang Lingkup Konten SOP

RUANG LINGKUP	PROSEDUR	DEFINISI	KEY PERFORMANCE INDICATOR	FORMULIR
PENGELOLAAN INSIDEN	**PENANGANAN INSIDEN**	• Pendefinisian insiden layanan • Tujuan utama SOP • Pendefinisian kategori insiden • Pendefinisian prioritas • Status penanganan	KPI *Incident Management*	▪ Formulir Pelaporan (FRM- Service Desk-001) ▪ Formulir Pencatatan (FRM- Service Desk-002) ▪ Formulir Survey Kepuasaan Masalah (FRM--004) ▪ Formulir Eskalasi (FRM-006)
PEMENUHAN PERMINTAAN	**PEMENUHAN PERMINTAAN LAYANAN**	• Pendefinisian permintaan layanan • Tujuan utama SOP • Pendefinisian kategori permintaan layanan • Pendefinisian prioritas • Status penanganan	KPI *Request Fulfillment*	▪ Formulir Pelaporan (FRM- Service Desk-001) ▪ Formulir Pencatatan (FRM- Service Desk-002) ▪ Formulir Survey Kepuasaan Permintaan (FRM- -005) ▪ Formulir Eskalasi (FRM--006) ▪ Surat Permohonan Permintaan Layanan (FRM-

				- 007)
PENGELOLAAN PERMASALAHAN	**PENANGANAN PERMASALAHAN** **(SOP-- 003)**	• Pendefinisian masalah • Tujuan utama SOP • Pendefinisian kategori permasalahan	KPI *Problem Management*	▪ Formulir Tambah Artikel (FRM- - 003)
PENGELOLAAN AKSES	**PEMENUHAN PERMINTAAN AKSES** **(SOP-- 004)**	• Pendefinisian permintaan akses • Tujuan utama SOP • Pendefinisian kategori permintaan akses • Pendefinisian prioritas • Status penanganan	KPI *Access Management*	▪ Formulir Pelaporan (FRM- Service Desk -001) ▪ Formulir Pencatatan (FRM- Service Desk -002) ▪ Formulir Survey Kepuasaan Permintaan (FRM- - 005) ▪ Formulir Eskalasi (FRM- -006) ▪ Surat Permohonan Permintaan Akses (FRM- - 008)

PROSEDUR PEMENUHAN PERMINTAAN AKSES (SOP--004)

Prosedur pengelolaan akses ini merupakan panduan yang berisi alur dan langkah-langkah untuk melakukan aktivitas pemenuhan akses layanan teknologi informasi yang diajukan oleh klien kepada pihak pengelola layanan TI. Dalam memenuhi kebutuhan aktivitas pengelolaan akses, telah disusun *standard operating prosedur* pada bab ini

DEFINISI

Permintaan Akses

Permintaan akses merupakan suatu permintaan yang diajukan oleh klien. Permintaan yang diajukan oleh klien dapat berupa permintaan atas disediakannya suatu layanan, permintaan akses atau permintaan panduan operasional. Permintaan akses yang diajukan harus sesuai dengan ruang lingkup layanan teknologi informasi yang disediakan .

Tujuan utama

Tujuan utama penyusunan prosedur terkait proses pemenuhan permintaan akses adalah untuk memastikan bahwa permintaan klien terkait hak akses yang diajukan dapat dipenuhi sesuai dengan kebutuhan permintaan dan kriteria pemenuhan permintaan yang diajukan klien, termasuk kebutuhan persetujuan pemenuhan permintaan akses. Dengan demikian dapat diketahui bagaimana alur pemenuhan permintaan akses yang dapat dilakukan oleh pihak pengelola layanan TI dalam melakukan pemenuhan permintaan layanan yang diajukan oleh klien.

Pendefinisian Kategori Permintaan akses

Berikut merupakan kategori pemenuhan permintaan akses terkait yang dimiliki.

Kategori	Rincian Layanan	Layanan
Aplikasi	Aplikasi	Permintaan pembuatan hak akses baru untuk aplikasi
		Permintaan perubahan hak akses lama untuk aplikasi
Status Identitas	Status Identitas	Permintaan perubahan mengundurkan diri
		Permintaan perubahan diberhentikan
		Permintaan perubahan pensiun
		Permintaan perubahan meninggal dunia
		Permintaan perubahan cuti
		Permintaan perubahan penurunan jabatan
		Permintaan perubahan mutasi

Pendefinisian Prioritas

Berikut merupakan pendefinisian prioritas penanganan layanan yang dibedakan berdasarkan urgensi dan dampak permintaan akses.

Level Urgensi

Level Urgensi	Deskripsi
Tinggi	Layanan tidak tersedia jika permintaan akses tidak segera dipenuhi
	Merupakan kebutuhan banyak pengguna
Menenggah	Layanan tersedia dalam waktu yang kritis jika permintaan akses tidak dipenuhi
	Merupakan kebutuhan beberapa pengguna
Rendah	Layanan tersedia secara terbatas dan membuat pengguna tidak dapat mengerjakan sebagian aktivitas mereka
	Merupakan kebutuhan pengguna yang bersifat personal

Level Dampak

Level Dampak	Deskripsi
Tinggi	Mengganggu proses bisnis utama jika permintaan akses tidak segera dipenuhi
	Banyak user yang tidak dapat meneruskan pekerjaan
Menenggah	Mengganggu satu atau beberapa proses bisnis jika permintaan akses tidak segera dipenuhi
	Hanya satu atau beberapa user yang terhambat pekerjaannya jika permintaan akses tidak segera dipenuhi
Rendah	Menghambat pekerjaan user secara personal jika permintaan akses tidak segera dipenuhi

Berdasarkan dampak dan urgensi tersebut, dapat diperoleh level prioritas yang disesuaikan dengan kebutuhan organisasi (Standard Level Agreement) atau SLA. Level prioritas penanganan dibagi menjadi level prioritas yaitu tinggi, menenggah, dan rendah seperti berikut:

		DAMPAK		
		Tinggi	Menenggah	Rendah
URGENSI	Tinggi	1-Tinggi	1-Tinggi	2-Menenggah
	Menenggah	1-Tinggi	2-Menenggah	3-Rendah
	Rendah	2-Menenggah	3-Rendah	3-Rendah

Masing-masing kategori prioritas tersebut kemudian ditentukan *target response time* dan *target resolution time* nya agar penanganan dari masing-masing kategori prioritas dapat dilaksanakan tepat waktu. Berikut ini *target response time* dan *resolution time*.

Target Response Time dan Resolution Time untuk Pemenuhan Permintaan Akses

Priority Code	Description	Target Response Time	Target Resolution Time
1	Tinggi	10 menit	8 jam
2	Menengah	1 jam	24 jam
3	Rendah	4 jam	48 jam

Keterangan:

- Target Response Time
  Merupakan total waktu yang dibutuhkan dari permintaan akses dilaporkan dan dicatat sampai direspon, serta diberi status **"Baru"**.
- Resolution Time
  Merupakan total waktu yang dibutuhkan dari pencatatan permintaan lakses sampai permintaan tersebut terpenuhi

Berikut merupakan deskripsi target waktu penyelesaian untuk setiap level prioritas sesuai dengan:

No	Level	Nama Layanan	Waktu Respon	Waktu Penyelesaian
1	**Rendah**	Pembuatan hak akses baru	10 menit	1 x 8 jam
	Menengah		1 jam	3 x 8 jam
	Tinggi		4 jam	6 x 8 jam
2	**Rendah**	Perubahan hak akses lama	10 menit	1 x 8 jam
	Menengah		1 jam	3 x 8 jam
	Tinggi		4 jam	6 x 8 jam
3	**Rendah**	Mengundurkan diri atas user ID	10 menit	1 x 8 jam
	Menengah		1 jam	3 x 8 jam
	Tinggi		4 jam	6 x 8 jam
4	**Rendah**	Diberhentikan User ID	10 menit	1 x 8 jam
	Menengah		1 jam	3 x 8 jam
	Tinggi		4 jam	6 x 8 jam

Berdasarkan pendefinisian urgensi, dampak, serta *response time* dan *resolution time*, didapatkan tiga prioritas pemenuhan permintaan layanan. Kriteria masing-masing level prioritas pemenuhan permintaan akses dijelaskan pada tabel dibawah ini sebagai berikut:

Tabel Pendefinisian Prioritas Permintaan Akses

Prioritas	Keterangan
Tinggi	Waktu yang tersedia untuk menyelesaikan masalah adalah ≤ 8 jam
	Layanan tidak tersedia jika permintaan akses tidak segera dipenuhi
	Merupakan kebutuhan banyak pengguna
	Mengganggu proses bisnis utama jika permintaan akses tidak segera dipenuhi
	Banyak user yang tidak dapat meneruskan pekerjaan
Menenggah	Waktu yang tersedia untuk menyelesaikan masalah adalah ≤ 24 jam
	Layanan tersedia dalam waktu yang kritis jika permintaan akses tidak dipenuhi
	Merupakan kebutuhan beberapa pengguna
	Mengganggu satu atau beberapa proses bisnis jika permintaan akses tidak segera dipenuhi
	Hanya satu atau beberapa user yang terhambat pekerjaannya jika permintaan akses tidak segera dipenuhi
Rendah	Waktu yang tersedia untuk menyelesaikan masalah adalah ≤ 48 jam
	Layanan tersedia secara terbatas dan membuat pengguna tidak dapat mengerjakan sebagian aktivitas mereka
	Merupakan kebutuhan pengguna yang bersifat personal
	Menghambat pekerjaan user secara personal jika permintaan akses tidak segera dipenuhi

Status penanganan

Dalam melakukan penanganan akses, service desk sebagai pihak yang melakukan penerimaan dan pengelolaan penanganan layanan, memiliki tugas untuk memberikan status penanganan layanan dan melakukan update terkait status penanganan tersebut. Berikut merupakan status penanganan layanan service desk:

Status Penanganan	Deskripsi
Baru	Status yang menunjukkan bahwa layanan yang dilaporkan telah tercatat dan segera membutuhkan penanganan lebih lanjut
Dalam Penanganan	Status yang menunjukkan bahwa layanan yang dilaporkan sedang dalam proses penanganan
Selesai	Status yang menunjukkan bahwa layanan yang dilaporkan telah ditutup dan dinyatakan selesai penanganannya
Ditinjau	Status yang menunjukkan bahwa permintaan layanan yang diajukan pengguna sedang ditinjau untuk dilakukan pemenuhan atau tidak
Ditolak	Status yang menunjukkan bahwa permintaan layanan yang diajukan pengguna tidak dapat dipenuhi ditolak
Dipenuhi	Status yang menunjukkan bahwa permintaan layanan yang diajukan pengguna telah selesai dilakukan penanganan

STRUKTUR ORGANISASI SERVICE DESK

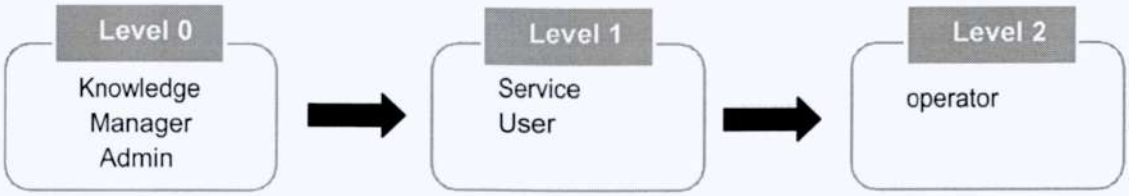
struktur organisasi service desk tersebut, masing-masing pelaksana memiliki peran dan tanggung jawab yang ditunjukkan pada tabel berikut:

Tabel 2 Peran dan Tanggung Jawab Staff Service Desk

JABATAN	PERAN DAN TANGGUNG JAWAB
Super admin	Penanggungjawab layanan pengelolaan data elektronik
Admin	Sebagai level 1 yang membantu dalammelakukan urusan pengendalian tata usaha pengadaan, penyimpanan, pendistribusian, pengadministrasian dan perawatan
User	Sebagai level 1 yang membantu dalam melakukan kegiatan sistem informasi berbasis komputer.
Operator	Sebagai level 2 yang membantu melaksanakanlayanan pengembangan *Business Process Reengineering* pelayanan untuk mendukung layanan

Peran dan Tanggung Jawab Pelaksana

Penanganan layanan yang dikelola untukmendefinisikan level *support* yang dibagi menjadi dua tingkat dan setiap tingkat memiliki deskripsi pekerjaan yang berbeda dalam melakukan penanganan layanan teknologi informasi.



Gambar 2 Eskalasi Service Desk

Tabel 3 Deskripsi Peran Level Pelaksana

Level	PELAKSANA	DESKRIPSI
Level 0	Knowledge Manager	Melakukan pencatatan terkait masalah yang sudah diketahui penyelesaian masalahnya untuk dimasukkan kedalam pusat bantuan
Level 1	Service Desk Operator	Sebagai titik komunikasi utama dengan klien
		Berupaya melakukan penyelesaian masalah klien
		Melakukan eskalasi kepada pihak teknisi ketika tidak dapat melakukan penyelesaian masalah
		Melakukan pencatatan seluruh aktivitas yang berkaitan dan berhubungan dengan klien

Level 2	Teknisi	Membantu melakukan penyelesaian masalah klien yang tidak dapat diselesaikan oleh service desk operator
		Mempertanggung jawabkan aktivitas penyelesaian masalah klien kepada service desk
		Berperan menyelesaikan masalah klien sesuai dengan keahlian masing-masing teknisi

Aplikasi Desk Service berupa aplikasi desktop: Aplikasi SAS, SILABI, SAIBA, SIMAK BMN dan Persediaan

POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.04/1.1/8914/2019
	TANGGAL PEMBUATAN	9 Desember 2019
	TANGGAL REVISI	
	TANGGAL EFEKTIF	
	DISAHKAN OLEH	Direktur Satino, SKM., MScN NIP. 196101021989031001

PEDOMAN TEKNIK
PENGENDALIAN DAN PENGELOLAAN SISTEM INFORMASI DI LINGKUNGAN POLITEKNIK KESEHATAN SURAKARTA

Pedoman Teknis
Pengendalian dan
Pengelolaan Sistem informasi
di Lingkungan Poltekkes Surakarta

KATA PENGANTAR

Pembinaan penyelenggaraan Sistem Pengendalian Intern Pemerintah (SPIP) merupakan tanggung jawab semua institusi sesuai dengan pasal 59 Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah. Pembinaan ini merupakan salah satu cara untuk memperkuat dan menunjang efektivitas sistem pengendalian intern, di lingkungan masing-masing.

Pembinaan penyelenggaraan SPIP yang menjadi tugas dan tanggung jawab tersebut meliputi: diarahkan dalam rangka penerapan unsur-unsur SPIP, yaitu:

1. lingkungan pengendalian;
2. penilaian risiko;
3. kegiatan pengendalian;
4. informasi dan komunikasi; dan
5. pemantauan pengendalian intern.

Untuk memenuhi kebutuhan pedoman penyelenggaraan SPIP, telah menyusun Pedoman Teknis Umum Penyelenggaraan SPIP. Pedoman tersebut merupakan pedoman tentang hal-hal apa saja yang perlu dibangun dan dilaksanakan dalam rangka penyelenggaraan SPIP. Selanjutnya, pedoman tersebut dijabarkan ke dalam pedoman teknis penyelenggaraan masing-masing subunsur pengendalian. Pedoman teknis subunsur ini merupakan acuan langkah-langkah yang perlu dilaksanakan dalam penyelenggaraan subunsur SPIP.

Pedoman Teknis Penyelenggaraan SPIP sub unsur Pengendalian atas Pengelolaan Sistem Informasi pada unsur Kegiatan Pengendalian merupakan acuan yang memberikan arah bagi instansi pemerintah pusat dan daerah dalam menyelenggarakan subunsur tersebut, dan dapat disesuaikan dengan karakteristik masing-masing instansi, yang meliputi fungsi, sifat, tujuan, dan kompleksitas instansi tersebut.

Pedoman ini masih jauh dari sempurna. Oleh karena itu, masukan dan saran perbaikan dari pengguna pedoman ini, sangat diharapkan sebagai bahan penyempurnaan.

Surakarta , Oktober 2019

DAFTAR ISI

Halaman

KATA PENGANTAR i

DAFTAR ISI iii

BAB I PENDAHULUAN

A. Latar Belakang 1

B. Sistematika Pedoman 2

BAB II GAMBARAN UMUM

A. Pengertian 3

B. Tujuan dan Manfaat 15

C. Peraturan Perundang-undangan Terkait 16

D. Parameter Penerapan 17

BAB III LANGKAH-LANGKAH PENYELENGGARAAN

A. Tahap Persiapan 25

B. Tahap Pelaksanaan 29

C. Tahap Pelaporan 32

BAB IV PENUTUP

BAB I
PENDAHULUAN

A. Latar Belakang

Kegiatan pengendalian dalam sistem pengendalian intern pemerintah (SPIP), salah satunya adalah subunsur pengendalian atas pengelolaan sistem informasi. Pimpinan instansi pemerintah wajib memiliki kegiatan pengendalian atas pengelolaan sistem informasi dilakukan untuk memastikan akurasi dan kelengkapan informasi, yang sangat menunjang penyajian laporan keuangan yang andal.

Kegiatan pengendalian atas pengelolaan sistem informasi meliputi pengendalian umum dan pengendalian aplikasi. Pengendalian umum terkait dengan lingkungan pengelolaan sistem informasi, sedangkan pengendalian aplikasi memastikan bahwa *input* telah lengkap dan diperoleh dari sumber yang valid, sistem yang memproses *input* dapat diandalkan, dan *output* yang dihasilkan dapat diuji kebenarannya.

Pedoman ini dimaksudkan untuk memberikan panduan maupun acuan dalam memahami dan melakukan kegiatan pengendalian pengelolaan atas sistem informasi. Pedoman ini merupakan penjabaran lebih lanjut dari pedoman teknis penyelenggaraan SPIP.

B. Sistematika Pedoman

Sistematika penyajian pedoman ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi uraian mengenai alasan perlunya disusun pedoman, hubungan dengan pedoman sebelumnya, dan sistematika isi pedoman.

BAB II Gambaran Umum

Bab ini berisi uraian mengenai pengertian, tujuan dan manfaat pengendalian atas pengelolaan sistem informasi, peraturan per-undang-undangan terkait, serta parameter penerapan dilakukannya pengendalian atas pengelolaan sistem informasi.

BAB III Langkah-Langkah Penyelenggaraan

Bab ini menguraikan mengenai langkah-langkah yang perlu dilaksanakan dalam menerapkan subunsur Pengendalian atas Pengelolaan Sistem Informasi, yang terdiri dari langkah persiapan, pelaksanaan, dan pelaporan.

BAB IV Penutup

Penutup berisikan hal-hal penting yang perlu diperhatikan kembali dan penjelasan atas penggunaan pedoman ini.

BAB II
GAMBARAN UMUM

A. Pengertian

Kegiatan pengendalian merupakan suatu tindakan yang diperlukan untuk mengatasi risiko, penetapan, serta pelaksanaan kebijakan dan prosedur untuk memastikan bahwa tindakan mengatasi risiko telah dilaksanakan secara efektif. Kegiatan pengendalian dirancang dan dikembangkan berdasarkan hasil penilaian risiko yang telah dilakukan.

Sistem informasi diperlukan untuk mendukung pelaksanaan kegiatan tugas dan fungsi instansi pemerintah, serta untuk pemrosesan data akuntansi dan kinerja. Akurasi dan ketepatan waktu pengambilan keputusan pimpinan instansi pemerintah dapat ditingkatkan dengan bantuan teknologi komputer. Oleh karena itu, sistem informasi yang dikembangkan instansi pemerintah idealnya berbasis teknologi komputer.

Jenis dan kompleksitas sistem informasi yang dijalankan di instansi pemerintah berbeda-beda dan dapat dikelompokkan menjadi sistem informasi yang sederhana dan sistem informasi yang canggih. Dalam kelompok pertama, termasuk penggunaan sistem informasi yang bersifat manual dan penggunaan komputer yang berdiri sendiri, dengan aplikasi yang sederhana. Dalam kelompok kedua, termasuk sistem informasi berbasis komputer, menggunakan jaringan *Local Area Network* (LAN) dan/atau *Wide Area Network* (WAN), dengan penggunaan aplikasi-aplikasi dalam jumlah yang relatif besar dan kompleks.

Penerapan sistem informasi di suatu instansi pemerintah, dipengaruhi pula oleh sifat khusus instansi pemerintah. Instansi pemerintah yang kegiatan utamanya sangat bergantung pada informasi yang cepat dan akurat akan menjadikan sistem informasi sebagai bagian dari kegiatan penting, sedangkan instansi pemerintah yang kegiatan utamanya tidak bergantung pada sistem informasi akan menjadikan sistem informasi sebagai kegiatan pendukung.

Pengelolaan sistem informasi berbasis teknologi komputer memiliki risiko, antara lain:

1. *Garbage in Garbage out* (GIGO)

   Akurasi *output* yang dihasilkan sangat bergantung pada akurasi *input* dan ketepatan aplikasi yang memroses *input* tersebut. Hal ini merupakan konsekuensi dari prinsip *garbage in garbage out* (GIGO). Kesalahan *input* secara otomatis akan menghasilkan *output* yang salah pula.

2. Jejak transaksi

   Beberapa sistem komputer dirancang sedemikian rupa sehingga jejak transaksi yang lengkap hanya ada dalam jangka waktu yang pendek, atau dalam bentuk yang hanya dapat dibaca dengan komputer.

3. Pemrosesan transaksi secara seragam

   Dengan instruksi pemrosesan yang sama, maka komputer akan meminimalisasi kesalahan klerikal. Namun, apabila aplikasi program komputer ataupun perangkat keras yang digunakan tidak tepat, maka akan menghasilkan *output* yang salah, yang kemungkinan akan terjadi dalam cakupan *(magnitude)* yang besar.

4. Inisiasi atau pengerjaan selanjutnya oleh komputer

   Transaksi tertentu secara otomatis akan diinisiasi oleh sistem komputer atau prosedur tertentu yang diperlukan untuk melaksanakan transaksi secara otomatis dapat dilakukan oleh sistem komputer. Otorisasi manajemen atas transaksi tersebut mungkin dilakukan secara implisit melekat dalam desain sistem komputer.

5. Potensi kesalahan dan penyimpangan

   Pegawai memiliki potensi untuk dapat mengakses data atau mengubah data, tanpa meninggalkan bukti fisik yang kasat mata. Berkurangnya keterlibatan manusia dalam menangani transaksi dapat mengurangi pengamatan atas kesalahan dan penyimpangan. Kesalahan dan penyimpangan yang terjadi selama perancangan atau perubahan program aplikasi, bisa jadi tidak dapat terdeteksi dalam jangka waktu yang lama.

Pimpinan instansi pemerintah harus mengembangkan rencana pengamanan sistem informasi dan membangun kesadaran seluruh pegawai bahwa pengamanan sistem informasi adalah tanggung jawab bersama, bukan hanya tanggung jawab unit kerja atau pejabat yang bertugas mengembangkan program dan pengamanan sistem informasi saja.

Kegiatan pengendalian atas pengelolaan sistem informasi, dilakukan untuk memastikan akurasi dan kelengkapan informasi, yang meliputi pengendalian umum dan pengendalian aplikasi.

1. Pengendalian Umum

Pengendalian umum meliputi struktur, kebijakan, dan prosedur yang berlaku terhadap seluruh operasional sistem komputer instansi pemerintah. Pengendalian umum berkaitan dengan seluruh aktivitas komputer, seperti yang terkait dengan rencana instansi pemerintah atas aktivitas pemrosesan data dan pemisahan fungsi.

Kegiatan pengendalian umum meliputi:

a. Pengamanan sistem informasi;

b. Pengendalian atas akses;

c. Pengendalian atas pengembangan dan perubahan perangkat lunak aplikasi;

d. Pengendalian atas perangkat lunak sistem;

e. Pemisahan tugas;

f. Kontinuitas pelayanan;

a. Pengamanan Sistem Informasi

Pengendalian intern yang baik atas sistem informasi mensyaratkan adanya upaya yang dilakukan untuk memproteksi *file* dan program dari pengungkapan yang tidak diotorisasi, dan dari kerusakan/kehancuran yang diakibatkan oleh kecelakaan. Instansi pemerintah harus mengidentifikasi semua kemungkinan ancaman atau bahaya terhadap peralatan dan operasi pemrosesan data.

Pengamanan sistem informasi sekurang-kurangnya mencakup kegiatan:

1) Pelaksanaan penilaian risiko secara periodik yang komprehensif.
2) Pengembangan rencana yang secara jelas menggambarkan program pengamanan, serta kebijakan dan prosedur yang mendukungnya.
3) Penetapan organisasi untuk mengimplementasikan dan mengelola program pengamanan.
4) Penguraian tanggung jawab pengamanan secara jelas.
5) Implementasi kebijakan yang efektif atas sumber daya manusia terkait dengan program pengamanan.
6) Pemantauan efektivitas program pengamanan dan melakukan perubahan program pengamanan jika diperlukan.
7) Lokasi penyimpanan yang aman.
8) Rencana pemulihan setelah bencana (*disaster recovery plan*).

b. Pengendalian atas Akses

Instansi pemerintah harus melakukan pengendalian atas akses terhadap sistem komputer untuk mencegah penyalahgunaan sistem informasi dan menjaga keamanan *hardware, software,* maupun perangkat terkait lainnya dari penggunaan yang tidak sah. Hanya orang- orang tertentu yang diotorisasi, yang dapat masuk ke dalam lingkungan sistem informasi dan melakukan akses terhadap sistem.

Pengendalian atas akses, sekurang-kurangnya mencakup kegiatan:

1) Mengklasifikasikan sumber daya sistem informasi berdasarkan kepentingan dan sensitivitasnya.

2) Mengidentifikasi pengguna yang berhak dan otorisasi akses ke informasi dengan pengendalian logis, untuk mencegah dan mendeteksi akses yang tidak diotorisasi.

3) Pemantauan atas akses ke sistem informasi, investigasi atas pelanggaran, serta tindakan perbaikan dan penegakan disiplin.

Pengendalian keamanan fisik *(physical security control)* adalah pembatasan akses terhadap sumber daya informasi secara fisik, misalnya dengan memakai kartu akses ruangan untuk memasuki suatu ruangan penyimpanan komputer.

Pengendalian kemanan logis *(logical security control)* adalah pembatasan akses terhadap sumber daya informasi dengan menggunakan logika komputer, misalnya melalui penggunaan kode akses (*password*) untuk memasuki suatu sistem jaringan komunikasi.

C. Pengendalian atas Pengembangan dan Perubahan Perangkat Lunak Aplikasi

Instansi pemerintah harus mengendalikan pengembangan dan perubahan perangkat lunak aplikasi, sekurang- kurangnya mencakup kegiatan:

1) Otorisasi atas fitur pemrosesan sistem informasi dan modifikasi program.
2) Pengujian dan persetujuan atas seluruh perangkat lunak yang baru dan yang dimutakhirkan.
3) Penetapan prosedur untuk memastikan terselenggaranya pengendalian atas kepustakaan perangkat lunak.

Prosedur untuk memastikan terselenggaranya pengendalian atas kepustakaan perangkat lunak (*software libraries*), termasuk di dalamnya adalah pemberian label, pembatasan akses, dan penggunaan kepustakaan perangkat lunak yang terpisah.

d. **Pengendalian atas Perangkat Lunak Sistem** Pengendalian atas perangkat lunak sistem, sekurang- kurangnya mencakup kegiatan:

1) Pembatasan akses ke perangkat lunak sistem berdasarkan tanggung jawab pekerjaan dan dokumentasi atas otorisasi akses.
2) Pengendalian dan pemantauan atas akses dan penggunaan perangkat lunak sistem.
3) Pengendalian atas perubahan yang dilakukan terhadap perangkat lunak sistem.

e. **Pemisahan Tugas**

Dalam sistem informasi berbasis komputer, prosedur yang dilakukan oleh pegawai yang berbeda dalam sistem informasi manual mungkin akan digabung ke dalam fungsi pemrosesan yang ada di komputer. Oleh karena itu, pegawai yang memiliki akses ke komputer akan mempunyai kesempatan yang besar untuk melakukan kecurangan.

Pemisahan tugas, mensyaratkan bahwa kewenangan dan tanggung jawab dalam pengelolaan sistem informasi harus secara jelas dibagi ke dalam beberapa fungsi berikut: (1) sistem analis aplikasi dan programer, (2) operator komputer, (3) programer sistem, (4) otorisasi transaksi, (5) pemelihara *file* perpustakaan sistem, dan

(6) pengendali data.

Pengendalian pemisahan tugas sekurang-kurangnya mencakup kegiatan:

1) Identifikasi tugas yang tidak dapat digabungkan dan penetapan kebijakan untuk memisahkan tugas tersebut.
2) Penetapan pengendalian akses untuk pelaksanaan pemisahan tugas.
3) Pengendalian atas kegiatan pegawai, melalui penggunaan prosedur, supervisi, dan reviu.

f. Kontinuitas Pelayanan

Instansi pemerintah harus memiliki rencana untuk kejadian tidak terduga *(contingency plan),* seperti langkah pengamanan apabila terjadi kebakaran, sabotase, bencana alam (seperti gempa bumi dan banjir), dan terorisme, untuk menjaga agar kegiatan pelayanan instansi tidak terganggu.

Rencana tersebut sebaiknya memuat hal-hal seperti:

- struktur organisasi;
- tugas dan tanggung jawab semua pihak yang terkait dengan sistem informasi;
- struktur dokumentasi;
- uji coba dan pelaksanaan rencana;

- identifikasi sumber daya penting;
- pemantauan dan pelaporan atas ketersediaan sumber daya penting tersebut;
- prosedur alternatif dan prinsip *back-up* dan pemulihan data.

Kegiatan untuk menjaga kontinuitas pelayanan, sekurang- kurangnya mencakup:

1) Penilaian, pemberian prioritas, dan pengidentifikasian sumber daya pendukung atas kegiatan komputerisasi yang kritis dan sensitif.
2) Pencegahan dan peminimalisasian potensi kerusakan dan terhentinya operasi komputer.
3) Pengembangan dan pendokumentasian rencana komprehensif untuk mengatasi kejadian tidak terduga.
4) Pengujian secara berkala atas rencana untuk mengatasi kejadian tidak terduga dan melakukan penyesuaian, jika diperlukan.

Contoh langkah pencegahan dan peminimalisasian potensi kerusakan dan terhentinya operasi komputer, antara lain melalui penggunaan prosedur *back-up* data dan program, penyimpanan *back-up* data di tempat lain, pengendalian atas lingkungan, pelatihan staf, serta pengelolaan dan pemeliharaan perangkat keras.

2. Pengendalian Aplikasi

Pengendalian aplikasi, meliputi struktur, kebijakan, dan prosedur yang dirancang untuk membantu memastikan kelengkapan, keakuratan, otorisasi, serta keabsahan semua transaksi selama pemrosesan aplikasi.

Pengendalian aplikasi berkaitan dengan pekerjaan pemrosesan tertentu yang dilakukan pada fasilitas komputer, yang berhubungan dengan *input* data, *file*, program, dan *output* aplikasi komputer tertentu, bukan sistem komputer secara umum. Tujuan utama pengendalian aplikasi adalah untuk menjaga keakuratan *output* sistem, *file* data, dan catatan-catatan transaksi/kejadian.

Pengendalian aplikasi terdiri atas:

a. Pengendalian otorisasi;

b. Pengendalian kelengkapan;

c. Pengendalian akurasi; serta

d. Pengendalian terhadap keandalan pemrosesan dan *file* data.

a. Pengendalian otorisasi

Pengendalian otorisasi sekurang-kurangnya mencakup:

1) Pengendalian terhadap dokumen sumber;

2) Pengesahan atas dokumen sumber;

3) Pembatasan akses ke terminal entri data; dan

4) Penggunaan *file* induk dan laporan khusus untuk memastikan bahwa seluruh data yang diproses telah diotorisasi.

Laporan khusus sebagaimana dinyatakan dalam butir 4) di atas adalah laporan yang mengungkapkan hal- hal yang tidak normal, seperti rekening piutang karyawan yang bersaldo kredit dan tanggal surat keputusan suatu permohonan yang mendahului tanggal surat permohonannya.

b. Pengendalian kelengkapan

Pengendalian kelengkapan, dirancang untuk mengatasi risiko tidak lengkapnya laporan yang dihasilkan oleh sistem informasi, karena tidak semua data telah dientri ke dalam sistem informasi.

Pengendalian kelengkapan, sekurang-kurangnya mencakup:

1) Pengentrian dan pemrosesan seluruh transaksi yang telah diotorisasi ke dalam komputer; dan
2) Pelaksanaan rekonsiliasi data untuk memverifikasi kelengkapan data.

c. Pengendalian akurasi

Pengendalian akurasi dirancang untuk mengatasi risiko kesalahan pada *output* (laporan) yang dihasilkan sistem informasi (tidak akurat), karena kesalahan (ketidakakuratan) data yang dientri.

Pengendalian akurasi, sekurang-kurangnya mencakup:

1) Penggunaan desain entri data untuk mendukung akurasi data.
2) Pelaksanaan validasi data untuk mengidentifikasi data yang salah.
3) Pencatatan, pelaporan, investigasi, dan perbaikan data yang salah dengan segera.
4) Reviu atas laporan keluaran untuk mempertahankan akurasi dan validitas data.

Dalam merancang entri data agar diperhatikan fitur yang mendukung akurasi data. Misalnya, untuk tipe/jenis *field* (kolom) yang sudah terstandarisasi, seperti unit organisasi, pengentrian dilakukan dengan memasukkan nomor kode organisasi dan komputer secara otomatis akan menampilkan nama unit organisasi.

Pelaksanaan validasi data dapat dilakukan melalui suatu program (disebut *program edit*), yang menggunakan komputer untuk mengecek validitas dan akurasi entri data sebelum data diproses.

Pengendalian (berupa reviu) atas laporan keluaran, dilakukan oleh pegawai yang mengendalikan data dan oleh pemakai laporan keluaran. Pegawai dimaksud harus mereviu kewajaran dan kelayakan seluruh keluaran dan harus melakukan rekonsiliasi terhadap total keluaran dengan total *input* yang berkaitan.

d. Pengendalian terhadap keandalan pemrosesan dan *file* data

Pengendalian terhadap keandalan pemrosesan dan *file* data, sekurang-kurangnya mencakup:

1) Penggunaan prosedur yang memastikan bahwa hanya program dan *file* data versi terkini yang digunakan selama pemrosesan.
2) Penggunaan program yang memiliki prosedur untuk memverifikasi kesesuaian versi *file* komputer yang digunakan selama pemrosesan.

3) Penggunaan program yang memiliki prosedur untuk mengecek *internal file header labels* sebelum pemrosesan.

4) Penggunaan aplikasi yang mencegah perubahan *file* secara bersamaan.

Kebijakan dan prosedur pengendalian terhadap pengelolaan sistem informasi harus dibuat secara tertulis dan diinformasikan kepada seluruh pegawai. Dalam mengembangkan aktivitas pengendalian atas pengelolaan sistem informasi, instansi pemerintah harus tetap memertimbangkan prinsip biaya manfaat *(cost and benefit)*. Dengan prinsip ini, aktivitas pengendalian yang dibangun seharusnya memberikan manfaat yang lebih besar dibandingkan dengan biaya yang dikeluarkan.

Bagi instansi pemerintah yang belum memiliki sistem informasi berbasis teknologi komputer, aktivitas pengendalian atas pengelolaan sistem informasi, setidak-tidaknya meliputi:

1. Pengecekan ulang atas data masukan (dokumen sumber);
2. Pencatatan dilaksanakan dalam nomor yang berurutan;
3. Penyimpangan (pengecualian dan pelanggaran) yang diindikasikan dari kegiatan pengendalian lainnya (seperti hasil audit intern atau ekstern) harus diuji dan ditindaklanjuti dengan segera;
4. Akses ke data dan *file* dikendalikan dengan cara tertentu, seperti penggunaan *password*.

B. Tujuan dan Manfaat

Pedoman teknis ini bertujuan untuk memberikan arahan bagi pimpinan instansi pemerintah yang akan mengembangkan kegiatan pengendalian atas pengelolaan sistem informasi. Dengan mendasarkan pada pedoman teknis ini, maka kegiatan pengendalian yang disusun diharapkan sesuai dengan yang digariskan dalam PP Nomor 60 Tahun 2008, sehingga sistem informasi yang diimplementasikan dapat mendukung pencapaian tujuan organisasi.

Tujuan pengendalian atas pengelolaan sistem informasi adalah:

1. Meningkatkan akurasi *input*, proses, dan *output* dari pengelolaan sistem informasi;
2. Meningkatkan pengamanan data;
3. Menekan risiko kesalahan pengelolaan sistem informasi.

Jika pengendalian atas sistem informasi dilakukan secara memadai, maka instansi pemerintah akan memeroleh manfaat sebagai berikut:

1. peningkatan kualitas pengambilan keputusan;
2. produktivitas kinerja operasional dan keuangan; dan
3. tercapainya tujuan pengendalian.

C. Peraturan Perundang-undangan Terkait

Peraturan tentang pengendalian atas pengelolaan sistem informasi yang dapat dijadikan acuan antara lain:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

3. Peraturan Presiden Nomor 42 Tahun 2005 tentang Komite Kebijakan Percepatan Penyediaan Infrastruktur.
4. Keputusan Presiden Nomor 9 Tahun 2003 tentang Tim Koordinasi Telematika Indonesia.
5. Instruksi Presiden Nomor 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-government*.
6. Instruksi Presiden Nomor 6 Tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia.
7. Peraturan dari Departemen Komunikasi dan Informasi:
   a. Panduan Pembangunan Infrastruktur Portal Pemerintah.
   b. Panduan Manajemen Sistem Dokumen Elektronik.
   c. Panduan Penyusunan Rencana Induk Pengembangan *E-government* Lembaga.
   d. Panduan Penyelenggaraan Situs Web Pemerintah Daerah.

D. Parameter Penerapan

Pengendalian atas pengelolaan sistem informasi dilakukan untuk memastikan akurasi dan kelengkapan informasi. Pengendalian dilakukan melalui pengendalian umum dan pengendalian aplikasi. Parameter penerapan pengendalian atas pengelolaan sistem informasi adalah sebagai berikut:

1. Pengendalian Umum

a. Pengamanan Sistem Informasi

1) Instansi pemerintah secara berkala melaksanakan penilaian risiko secara periodik yang komprehensif. Hal- hal yang perlu dipertimbangkan adalah sebagai berikut:

a) Penilaian risiko dilaksanakan dan didokumentasikan secara teratur dan pada saat sistem, fasilitas, atau kondisi lainnya berubah;

b) Penilaian risiko tersebut sudah mempertimbangkan sensitivitas dan keandalan data;

c) Penetapan risiko akhir dan persetujuan pimpinan instansi pemerintah didokumentasikan.

2) Pimpinan instansi pemerintah mengembangkan rencana yang secara jelas menggambarkan program pengamanan serta kebijakan dan prosedur yang mendukungnya.

3) Pimpinan instansi pemerintah menetapkan organisasi untuk mengimplementasikan dan mengelola program pengamanan.

4) Pimpinan instansi pemerintah menetapkan uraian tanggung jawab pengamanan secara jelas.

5) Instansi pemerintah mengimplementasikan kebijakan yang efektif atas pegawai yang terkait dengan program pengamanan.

6) Instansi pemerintah memantau efektivitas program pengamanan dan melakukan perubahan program pengamanan jika diperlukan. Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

a) Pimpinan instansi pemerintah secara berkala menilai kelayakan kebijakan pengamanan dan kepatuhan terhadap kebijakan tersebut;

b) Tindakan korektif diterapkan dan diuji dengan segera dan efektif serta dipantau secara terus-menerus.

b. Pengendalian atas Akses

1) Instansi pemerintah mengklasifikasikan sumber daya sistem informasi berdasarkan kepentingan dan sensitivitasnya.

   Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

   a) Klasifikasi sumber daya dan kriteria terkait sudah ditetapkan dan dikomunikasikan kepada pemilik sumber daya;

   b) Pemilik sumber daya memilah-milah sumber daya informasi berdasarkan klasifikasi dan kriteria yang sudah ditetapkan dengan memperhatikan penetapan dan penilaian risiko serta mendokumentasikannya.

2) Pemilik sumber daya mengidentifikasi pengguna yang berhak dan otorisasi akses ke informasi secara formal.

3) Instansi pemerintah menetapkan pengendalian fisik dan pengendalian logik untuk mencegah dan mendeteksi akses yang tidak diotorisasi.

4) Instansi pemerintah memantau akses ke sistem informasi, melakukan investigasi atas pelanggaran, dan mengambil tindakan perbaikan dan penegakan disiplin.

c. Pengendalian atas Pengembangan dan Perubahan Perangkat Lunak Aplikasi

1) Fitur pemrosesan sistem informasi dan modifikasi program diotorisasi.

2) Seluruh perangkat lunak yang baru dan yang dimutakhirkan sudah diuji dan disetujui.

3) Instansi pemerintah telah menetapkan prosedur untuk memastikan terselenggaranya pengendalian atas kepustakaan perangkat lunak (*software libraries*), termasuk pemberian label, pembatasan akses, dan penggunaan kepustakaan perangkat lunak yang terpisah.

d. Pengendalian atas Perangkat Lunak Sistem

1) Instansi pemerintah membatasi akses ke perangkat lunak sistem berdasarkan tanggung jawab pekerjaan dan otorisasi akses tersebut didokumentasikan.
2) Akses ke dan penggunaan perangkat lunak sistem dikendalikan dan dipantau.
3) Instansi pemerintah mengendalikan perubahan yang dilakukan terhadap perangkat lunak sistem.

e. Pemisahan Tugas

1) Tugas yang tidak dapat digabungkan sudah diidentifikasi dan kebijakan untuk memisahkan tugas tersebut sudah ditetapkan.
2) Pengendalian atas akses sudah ditetapkan untuk pelaksanaan pemisahan tugas.
3) Instansi pemerintah melakukan pengendalian atas kegiatan pegawai melalui penggunaan prosedur, supervisi, dan reviu.

f. Kontinuitas Pelayanan

1) Instansi pemerintah melakukan penilaian, pemberian prioritas, dan pengidentifikasian sumber daya pendukung atas kegiatan komputerisasi yang kritis dan sensitif.

2) Instansi pemerintah sudah mengambil langkah-langkah pencegahan dan minimalisasi potensi kerusakan dan terhentinya operasi komputer, antara lain melalui penggunaan prosedur *backup* data dan program, penyimpanan *back-up* data di tempat lain, pengendalian atas lingkungan, pelatihan staf, serta pengelolaan dan pemeliharaan perangkat keras.

3) Pimpinan instansi pemerintah sudah mengembangkan dan mendokumentasikan rencana komprehensif untuk mengatasi kejadian tidak terduga (*contingency plan*), misalnya langkah pengamanan apabila terjadi bencana alam, sabotase, dan terorisme.

4) Instansi pemerintah secara berkala menguji rencana untuk mengatasi kejadian tidak terduga dan melakukan penyesuaian jika diperlukan.

2. Pengendalian Aplikasi

a. Pengendalian Otorisasi

1) Instansi pemerintah mengendalikan dokumen sumber. Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

   a) Akses ke dokumen sumber yang masih kosong dibatasi;

   b) Dokumen sumber diberikan nomor urut tercetak (*prenumbered*).

2) Atas dokumen sumber dilakukan pengesahan. Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

   a) Dokumen sumber yang penting memerlukan tanda tangan otorisasi;

b) Untuk sistem aplikasi *batch*, harus digunakan lembar kendali *batch* yang menyediakan informasi seperti tanggal, nomor kendali, jumlah dokumen, dan jumlah kendali (*control totals*) dari *field* kunci;

c) Reviu independen terhadap data dilakukan sebelum data dientri ke dalam sistem aplikasi.

3) Akses ke terminal entri data dibatasi.

4) *File* induk dan laporan khusus digunakan untuk memastikan bahwa seluruh data yang diproses telah diotorisasi.

b. Pengendalian Kelengkapan

1) Transaksi yang dientri dan diproses ke dalam komputer adalah seluruh transaksi yang telah diotorisasi.

2) Rekonsiliasi data dilaksanakan untuk memverifikasi kelengkapan data.

c. Pengendalian Akurasi

1) Desain entri data digunakan untuk mendukung akurasi data.

2) Validasi data dan *editing* dilaksanakan untuk mengidentifikasi data yang salah.

3) Data yang salah dengan segera dicatat, dilaporkan, diinvestigasi, dan diperbaiki.

4) Laporan keluaran direviu untuk mempertahankan akurasi dan validitas data.

d. **Pengendalian terhadap Keandalan Pemrosesan dan *File* Data**

1) Terdapat prosedur untuk memastikan bahwa hanya program dan *file* data versi terkini yang digunakan selama pemrosesan.
2) Terdapat program yang memiliki prosedur untuk memverifikasi bahwa versi *file* komputer yang sesuai yang digunakan selama pemrosesan.
3) Terdapat program yang memiliki prosedur untuk mengecek *internal file header labels* sebelum pemrosesan.
4) Terdapat aplikasi yang mencegah perubahan *file* secara bersamaan.

Indikator keberhasilan penerapan pengendalian atas pengelolaan sistem informasi, yang meliputi indikator *output* dan *outcome,* adalah sebagai berikut:

1. Indikator *output*

a. Pelaksanaan penilaian risiko atas pengelolaan sistem informasi;

b. Dokumen pengamanan, berisi aturan mengenai:

1) Rencana program pengamanan dan kebijakan serta prosedur yang mendukungnya;
2) Organisasi yang mengimplementasikan dan mengelola program pengamanan;
3) Uraian tanggung jawab pengamanan;
4) Kebijakan efektif atas pegawai yang terkait program pengamanan;

c. Pelaksanaan pemantauan efektivitas program pengamanan;

d. Pelaksanaan penilaian kelayakan kebijakan pengamanan;

e. Pelaksanaan tindakan korektif;

f. Dokumen berisi kebijakan, prosedur, dan tingkatan akses terhadap sistem informasi;

g. Pelaksanaan pemantauan atas penerapan kebijakan dan prosedur akses;

h. Pelaksanaan otorisasi dan akses atas:

   a. Pengembangan dan perubahan perangkat lunak aplikasi;

   b. dokumen sumber;

   c. entri data;

   d. desain data entri;

i. Program *contingency plan* telah disusun.

2. Indikator *outcome*

a. Kebijakan dan prosedur pengendalian yang diatur dalam suatu pedoman telah diterapkan dengan tepat.

b. Seluruh pegawai memahami tujuan dari kegiatan pengendalian atas pengelolaan sistem informasi.

c. Sistem informasi berfungsi secara optimal.

d. Pelaporan yang handal.

e. Tidak terdapat gangguan dalam pelayanan instansi pemerintah yang disebabkan oleh tidak berfungsinya sistem informasi.

BAB III

LANGKAH-LANGKAH PENYELENGGARAAN

Penyelenggaraan SPIP berupa kegiatan pengendalian atas pengelolaan sistem informasi dilakukan melalui tiga tahap utama, yaitu:

1. **Tahap Persiapan**, merupakan tahap awal implementasi, yang ditujukan untuk memberikan pemahaman atau kesadaran yang lebih baik tentang pengelolaan sistem informasi dan pengendaliannya, serta pemetaan atas kondisi pengendalian atas pengelolaan sistem informasi yang ada di instansi pemerintah, dan kebutuhan penerapannya.
2. **Tahap Pelaksanaan**, merupakan langkah tindak lanjut atas pemetaan, yang meliputi kegiatan pembangunan infrastruktur dan internalisasi.
3. **Tahap Pelaporan**, merupakan tahap melaporkan kegiatan dan upaya pengembangan berkelanjutan.

Setiap tahapan implementasi dan beberapa contoh akan diuraikan di bab ini.

A. Tahap Persiapan

Langkah-langkah yang perlu dilakukan oleh instansi pemerintah dalam persiapan penerapan sistem pengendalian atas pengelolaan sistem informasi, terdiri dari proses pemahaman dan persamaan persepsi, serta pemetaan, yaitu:

1) Pemahaman dan Persamaan Persepsi (*Knowing*)

Tahap pemahaman merupakan langkah awal dalam membangun kesadaran (*building awareness*) terhadap arti penting pengendalian atas pengelolaan sistem informasi, memperkuat komitmen, serta dukungan seluruh pejabat dan pegawai instansi pemerintah.

Seluruh pegawai harus diinformasikan mengenai sistem informasi yang ada di instansi pemerintah tersebut yang meliputi seluruh rangkaian sistem informasi, berupa *input*, proses, dan *output* sistem. Mereka juga harus memahami seluruh perangkat sistem yang digunakan, baik perangkat keras maupun perangkat lunak. Pimpinan harus memberikan pemahaman kepada seluruh pegawai akan arti penting dan tujuan dari sistem informasi, serta kaitannya dengan pencapaian tujuan organisasi. Pimpinan agar memberikan pemahaman kepada pegawai mengenai risiko-risiko terkait dengan pengelolaan sistem informasi, yang meliputi risiko atas *input*, proses, dan *output* sistem informasi, serta perlunya kegiatan pengendalian untuk mengatasi risiko tersebut.

Dengan adanya kesepahaman dan kesamaan persepsi tersebut, diharapkan implementasi dari pengendalian atas pengelolaan sistem informasi akan lebih efektif dan dapat mengurangi resistensi dari seluruh lapisan pegawai, serta mereka akan berpartisipasi aktif dalam mendukung pengendalian atas pengelolaan sistem informasi.

Tahap pemahaman diawali dengan mengomunikasikan pentingnya pengendalian atas pengelolaan sistem informasi dalam rangka menyediakan informasi, memastikan akurasi, dan kelengkapan informasi untuk pembuatan laporan kinerja maupun laporan keuangan yang lengkap dan akurat, serta untuk mendukung pengambilan keputusan.

Untuk memberikan penyamaan pemahaman tersebut, beberapa langkah yang dapat dilakukan adalah sebagai berikut:

a. Sosialisasi

- Sosialisasi mengenai kegiatan pengendalian atas pengelolaan sistem informasi disampaikan kepada seluruh pegawai. Sosialisasi tersebut merupakan bagian dari sosialisasi SPIP secara umum (keseluruhan).
- Kegiatan sosialisasi dilakukan oleh Satgas SPIP, yang dibentuk oleh pimpinan instansi pemerintah, beranggotakan perwakilan dari seluruh unit (bidang/bagian) di instansi tersebut, dan ada anggota Satgas yang memiliki pemahaman yang baik atas pengelolaan sistem informasi. Jika diperlukan, pimpinan instansi pemerintah dapat meminta bantuan narasumber dari untuk memberikan sosialisasi.
- Dalam kegiatan sosialisasi tersebut, satgas menyampaikan pula rencana tindak *(action plan)* pengembangan kegiatan pengendalian atas pengelolaan sistem informasi.
- Sosialisasi dilakukan melalui kegiatan ceramah, tanya jawab, diskusi, dan/atau seminar.

Dengan sosialisasi ini, diharapkan seluruh pegawai memahami pentingnya pengendalian atas pengelolaan sistem informasi yang ada di instansi, dan *road map,* serta rencana tindak pengembangan kegiatan pengendaliannya.

b. Penyebaran Informasi

Informasi mengenai sistem informasi yang dimiliki organisasi dan kegiatan pengendalian yang terkait disampaikan kepada pegawai melalui berbagai cara, antara lain melalui jaringan informasi internal (*Intranet*) dan tulisan dalam bulletin kantor, yang menganalisis dan mengkaji tentang kegiatan pengendalian atas pengelolaan sistem informasi.

2) Pemetaan (*Mapping*)

Setelah dilakukan sosialisasi pemahaman kegiatan pengendalian atas pengelolaan sistem informasi, maka perlu dilakukan suatu pemetaan terhadap kegiatan pengendalian atas pengelolaan sistem informasi yang dijalankan di instansi pemerintah. Pemetaan terhadap kegiatan pengendalian atas pengelolaan sistem informasi, dilakukan bersamaan dengan pemetaan yang dilakukan di subunsur kegiatan pengendalian dan unsur-unsur SPIP lainnya (pemetaan dilakukan serentak terhadap semua unsur dan subunsur SPIP, dengan mendasarkan pada Pedoman *Diagnostic Assessment*)

Pemetaan dilakukan untuk melihat kondisi kegiatan pengendalian yang sudah diimplementasikan dan berjalan pada instansi pemerintah, serta keberadaan infrastruktur dalam bentuk kebijakan dan prosedur pengelolaan sistem informasi.

Pemetaan juga untuk mengetahui apakah instansi telah mendokumentasikan penyelenggaraan pengendalian sistem informasi dan telah melakukan monitoring dan evaluasi atas kegiatan tersebut.

Dengan pemetaan, akan diketahui kondisi yang memerlukan perbaikan (*area of improvement*) agar kegiatan pengendalian atas pengelolaan sistem informasi dapat terbangun secara utuh.

B. Tahap Pelaksanaan

Setelah tahap persiapan, langkah berikutnya adalah tahap pelaksanaan penyelenggaraan pengendalian atas pengelolaan sistem informasi. Dalam tahap pelaksanaan ini, termasuk di dalamnya adalah tahap membangun infrastruktur (*norming*), tahap internalisasi (*forming*), dan tahap pengembangan berkelanjutan (*performing*).

Dalam tahap pelaksanaan ini, apabila dari hasil pemetaan diperoleh informasi bahwa instansi pemerintah telah melaksanakan pengendalian atas pengelolaan sistem informasi dan sudah berjalan efektif, maka langkah pelaksanaan tersebut tinggal dilanjutkan. Apabila suatu langkah pelaksanaan pengendalian belum ada/belum efektif, maka langkah tersebut perlu ditetapkan dan dilaksanakan.

1) Pembangunan Infrastruktur (*Norming*)

Instansi pemerintah menyusun kebijakan dan prosedur, serta pedoman lainnya terkait dengan pengendalian atas pengelolaan sistem informasi, dengan hasil pemetaan yang dilakukan dan hasil penilaian risiko.

Hasil pemetaan menggambarkan *area of improvement* secara umum di instansi. Hasilnya kemudian disesuaikan dengan hasil penilaian risiko atas pengelolaan sistem informasi, sehingga didapatkan *area of improvement* yang secara khusus ada di instansi.

Kebijakan, prosedur, dan pedoman lainnya yang perlu dibangun antara lain meliputi:

a. Kebijakan dan prosedur otorisasi atas:
   1) akses ke sistem informasi;
   2) akses perangkat lunak sistem;
   3) akses ke terminal entri;
   4) perubahan fitur dan modifikasi program;
   5) dokumen sumber;
   6) transaksi yang dientri dan diproses dalam komputer.
b. Penetapan aset teknologi informasi yang perlu dikelola dan rencana penyusunan kebijakan dan prosedur teknologi informasi.
c. Penetapan struktur organisasi untuk mengelola sistem informasi (termasuk program pengamanan).
d. Kebijakan dan prosedur pemisahan fungsi dalam pengelolaan sistem informasi.
e. Pedoman rencana kontinjensi (*contingency plan*).

2. Internalisasi (*Forming*)

Kebijakan, prosedur, dan pedoman lain yang terkait dengan pengendalian atas pengelolaan sistem informasi diinternalisasikan kepada seluruh pegawai.

Internalisasi adalah suatu proses untuk mewujudkan infrastruktur menjadi bagian dari kegiatan operasional sehari- hari. Perwujudannya, dapat tercermin dalam konteks seberapa jauh proses internalisasi memengaruhi pimpinan instansi pemerintah dalam mengambil keputusan, dan memengaruhi perilaku para pegawai dalam melaksanakan kegiatan.

Langkah-langkah yang perlu dilakukan sehubungan dengan internalisasi pengendalian atas pengelolaan sistem informasi, meliputi:

a. Melakukan pelatihan dan/atau *workshop* mengenai infrastruktur pengendalian yang telah dibangun kepada seluruh pegawai yang terkait dengan pengelolaan sistem informasi.

b. Mendistribusikan manual pedoman kegiatan pengendalian atas pengelolaan sistem informasi keseluruh unit yang ada di instansi pemerintah.

c. Memuat pedoman kegiatan pengendalian atas pengelolaan sistem informasi ke media informasi yang dimiliki instansi untuk dapat diakses oleh seluruh pegawai.

d. Pimpinan memberikan pengarahan secara rutin tentang pentingnya pengendalian umum dan pengendalian aplikasi atas pengelolaan sistem informasi.

e. Melaksanakan pedoman pengendalian atas pengelolaan sistem informasi.

3. Pengembangan Berkelanjutan (*Performing*)

Pengembangan berkelanjutan, dilakukan untuk memantau penerapan kebijakan dan prosedur yang terkait dengan pengelolaan sistem informasi, serta melakukan penyempurnaan kebijakan dan prosedur terkait apabila diperlukan.

Pengembangan berkelanjutan atas penyelenggaraan aktivitas pengendalian atas pengelolaan sistem informasi dilakukan dengan langkah-langkah berikut:

a. Pemantauan atas pelaksanaan pengendalian pengelolaan sistem informasi.

b. Evaluasi secara berkala atas hasil yang diperoleh dari kegiatan pemantauan.

c. Identifikasi perubahan lingkungan organisasi yang memengaruhi sistem informasi.

d. Identifikasi *gap* antara sistem informasi yang sedang berjalan dengan kebutuhan baru sehubungan dengan perubahan lingkungan organisasi.

e. Lakukan upaya penyempurnaan atas pengendalian sistem informasi yang ada.

Pada tahap awal pembangunan SPIP, pemantauan penerapan kegiatan pengendalian dilakukan oleh Tim Satgas, sedangkan pada periode-periode berikutnya merupakan bagian tidak terpisahkan dari unsur Pemantauan.

C. Tahap Pelaporan

Setelah tahap pelaksanaan selesai, seluruh kegiatan penyelenggaraan sub unsur perlu didokumentasikan. Pendokumentasian ini merupakan satu kesatuan (bagian yang tidak terpisahkan) dari kegiatan pelaporan berkala dan tahunan penyelenggaraan SPIP. Pendokumentasian dimaksud meliputi:

1. Pelaksanaan kegiatan, yang terdiri dari:

   a. Kegiatan pemahaman, antara lain kegiatan sosialisasi (ceramah, diskusi, seminar, rapat kerja, dan *focus group*) mengenai pengendalian sistem informasi.

b. Kegiatan pemetaan keberadaan dan penerapan infrastruktur, yang antara lain berisi: 1) pemetaan penerapan pengendalian atas pengelolaan sistem informasi, 2) masukan atas rencana tindak yang tepat untuk menyempurnakan kebijakan dan prosedur pengendalian yang sudah ada, baik pengendalian umum maupun pengendalian aplikasi.

c. Kegiatan pembangunan infrastruktur, yang antara lain berisi: 1) kebijakan dan prosedur pengelolaan sistem informasi, 2) penyusunan kebijakan dan prosedur pengendalian umum dan pengendalian aplikasi.

d. Kegiatan internalisasi, yang antara lain berisi: 1) kegiatan sosialisasi kebijakan dan prosedur pengelolaan sistem informasi, 2) kegiatan yang memastikan seluruh pegawai telah menerima informasi, serta memahami kebijakan dan prosedur pengelolaan sistem informasi.

e. Kegiatan pengembangan berkelanjutan, yang antara lain berisi: 1) kegiatan pemantauan penerapan kebijakan dan prosedur pengelolaan sistem informasi, 2) masukan bagi pimpinan instansi pemerintah untuk menyatakan asersi di Teknologi Informasi (TI) bahwa TI telah dikelola dengan baik.

2. Hambatan kegiatan

Apabila ditemukan hambatan-hambatan dalam pelaksanaan kegiatan yang menyebabkan tidak tercapainya target/tujuan kegiatan tersebut, agar dijelaskan penyebab terjadinya hambatan.

3. Saran

Saran diberikan berkaitan dengan adanya hambatan pelaksanaan kegiatan dan dicarikan saran pemecahan masalah agar kejadian serupa tidak terulang, dan guna peningkatan pencapaian tujuan. Saran yang diberikan agar realistis dan benar-benar dapat dilaksanakan.

4. Tindak lanjut atas saran periode sebelumnya

Bagian ini mengungkapkan tindak lanjut yang telah dilakukan atas saran yang telah diberikan pada kegiatan periode sebelumnya.

Dokumentasi ini merupakan bahan dukungan bagi penyusunan laporan berkala dan tahunan (penjelasan penyusunan laporan dapat dilihat pada Pedoman Teknis Umum Penyelenggaraan SPIP). Kegiatan pendokumentasian menjadi tanggung jawab pelaksana kegiatan, yang hasilnya disampaikan kepada pimpinan instansi pemerintah sebagai bentuk akuntabilitas, melalui Satuan Tugas Penyelenggaraan SPIP di instansi pemerintah terkait.

BAB IV
PENUTUP

Pedoman ini disusun dengan tujuan agar tersedia acuan bagi instansi pemerintah pusat dan satuan kerja dalam membangun aktivitas pengendalian, khususnya pada sub unsur Pengendalian atas Pengelolaan Sistem Informasi. Lebih lanjut, dengan terwujudnya pengendalian yang baik ini, maka kegiatan pengendalian yang dibangun dapat menjamin akurasi dan kelengkapan informasi untuk pengambilan keputusan, serta untuk mendukung penyusunan laporan yang dapat diandalkan.

Di dalam pedoman ini disajikan bahwa kegiatan pengendalian atas pengelolaan sistem informasi dikembangkan dengan mendasarkan pada hasil penilaian risiko terhadap sistem informasi organisasi. Kegiatan pengendalian terdiri atas pengendalian umum dan pengendalian aplikasi. Pengendalian umum berhubungan dengan pengendalian atas pengelolaan sistem informasi secara umum, sedangkan pengendalian aplikasi berkaitan dengan entri data, *file*, program, dan keluaran dari aplikasi tertentu

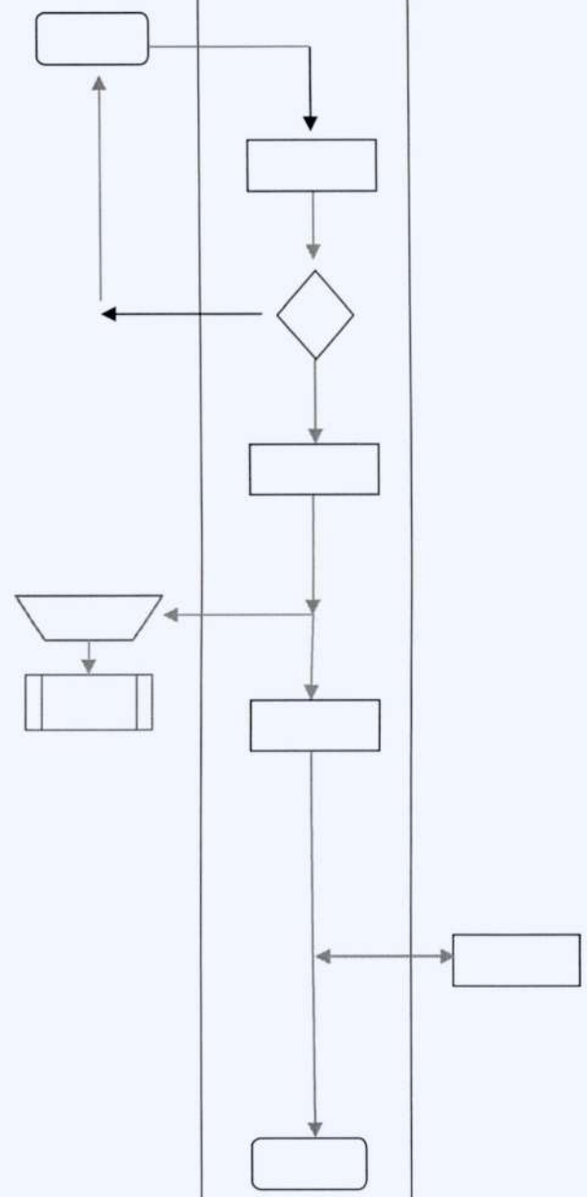
Langkah-langkah yang tertuang dalam pedoman ini merupakan langkah pelaksanaan minimal yang sebaiknya dibangun. Instansi pemerintah hendaknya dapat mengembangkan lebih jauh langkah-langkah yang perlu diambil sesuai dengan kebutuhan, dengan tetap mengacu pada (dan tidak boleh bertentangan dengan) peraturan perundang-undangan yang berlaku.

Kami sadar bahwa pedoman ini belum sempurna, dan kami pun mengerti bahwa perkembangan teori dan praktik-praktik sistem pengendalian intern tidak mungkin terhentikan. Oleh karenanya, pedoman ini akan terus diperbarui dan perlu masukan-masukan dari pihak mana pun demi lebih baiknya pedoman ini.

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	DP.03.04/1.1/ 119 /2020
	Tanggal Pembuatan	02 Januari 2020
	Tanggal Revisi	
	Tanggal Efektif	02 Januari 2020
BADAN PENGEMBANGAN DAN PEMBERDAYAAN SUMBER DAYA MANUSIA KESEHATAN	Disahkan Oleh	Direktur Satino, SKM, MScN NIP. 196101021989031001
POLITEKNIK KESEHATAN KEMENKES SURAKARTA	Nama SOP	**HAK AKSES RUANG SERVER dan MESIN SERVER**

Dasar Hukum	**Kualifikasi Pelaksanaan**
1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 2. Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik 3. Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia Nomor 75 Tahun 2016 tentang Layanan Informasi Publik di Lingkungan Kementerian Riset, Teknologi, dan Pendidikan Tinggi 4. Peraturan Menteri Komunikasi dan Informatika RI No. 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sisten Elektronik	1. Menghimpun Informasi tentang kebutuhan akses ruang server dan mesin server 2. Menentukan tingkat kepentingan akses 3. Memberikan hak akses dengan pendampingan
Keterkaitan dengan SOP Lain	**Peralatan yang digunakan**
1. Sistem Informasi Sistem Manajemen Keamanan Informasi (Security Awarennes) 2. SOP Hak Akses 3. Prosedur Pengelolaan Akses Pelayanan TI	1. Kunci Ruang Server 2. Buku Daftar Akses 3. Alat Tulis 4. Koneksi Internet 5. Dokumen yang dibutuhkan
Peringatan	**Pencatatan dan Pendataan**
Apabila SOP ini tidak dijalankan maka dapat berakibat : 1. Hilangnya data 2. Hilang atau rusaknya mesin server 3. Tidak berfungsinya aplikasi dengan baik	Disimpan dalam bentuk dokumen Softcopy dan Hardcopy

NO	AKTIFITAS	PELAKSANA			MUTU BAKU			KET
		PEMOHON HAK AKSES	KA. UNIT IT / TIM IT	WADIR I	KELENGKAPAN	WAKTU	OUTPUT	
1	Pemohon hak akses ruang server mengajukan peminjaman terhadapa kunci ruang server dan atau akses mesin server					5 Menit	Narasi/deskripsi kegiatan	
2	Ka. Unit IT melakukan identifikasi terkait informasi atau kegiatan yang akan dilakukan oleh pemohon hak akses					2 Menit		
3	Ka Unit IT memberikan hak akses dan atau menolaknya				Kunci Ruang Server/ Dokumen Server	3 Menit		
4	Jika memberikan hak akses, Ka Unit IT mendampingi dan atau mewakilkan kepada Tim IT untuk melakukan pendampingan terhadap pemohon selama berada di ruang server atau selama akses ke mesin server					60 Menit		
5	Pemohon mengisi buku daftar akses yang berada di ruang server,				Buku Hak Akses	3 Menit	Narasi dalam bentuk hardcopy	
6	Melakukan aktifitas di ruang server				Buku Daftar Akses dan Alat Tulis, Internet dan Dokumen			
7	Memeriksa kembali kondisi ruang server dan mesin server sebelum meninggalkan ruang server dan memastikan server dalam kondisi baik dan normal					60 Menit		
8	Apabila terdapat kerusakan pada ruang server atau mesin server atau data server selama pengerjaan akses, maka dilakukan pencatatan di dalam buku hak akses dan dilaporkan kepada pimpinan setingkat lebih tinggi (Ka. Unit IT dan atau Wadir I					5 Menit	Daftar Kerusakan	
9	Mengunci kembali ruang server dan atau keluar dari hak akses mesin server					1 Menit		



TUJUAN	SOP ini ditetapkan untuk melindungi ruang server, mesin server secara fisik dan data yang merupakan asset dari Politeknik Kesehatan Surakarta. Mencegah atau menanggulangi dan menjaga orang, hardware, program, jaringan dan data dari bahaya fisik dan kejadian yang dapat menyebabkan kehilangan yang besar atau kehancuran, termasuk perlindungan terhadap kebakaran, bencana alam, pencurian, vandalism dan teroris
RUANG LINGKUP	Pengelolaan ruang server, kunci ruangan dan mesin server serta data yang tersimpan di dalam mesin server di kantor Direktorat POliteknik Kesehatan Surakarta
KOORDINATOR	Kepala Unit Teknologi Informasi
PENGERTIAN	1. **Ruang Server** adalah sebuah ruangan yang digunakan untuk menyimpan aplikasi, data, perangkat jaringan (router, hub dll) dan perangkat lainnya yang terkait dengan operasional sistem sehari-hari seperti Uninterruptible Power Supply (UPS) dan lain-lain 2. **Server** adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Dilihat dari fungsinya, server bisa di kategorikan dalam beberapa jenis, seperti: server aplikasi (application server), server data (data server) maupun server proxy (proxy server) **3. Data** adalah catatan atas kumpulan fakta
PEMOHON	Pemohon adalah orang atau pribadi yang membutuhkan akses terhadap server, ruang server dan data aplikasi. Bisa berasal dari lingkup pegawai Politeknik Kesehatan Surakarta atau rekanan/pihak ke 2 dari institusi Politeknik Kesehatan Surakarta

<table>
<tr><td rowspan="4">KEMENTERIAN KESEHATAN REPUBLIK INDONESIA</td><td>Nomor SOP</td><td>IR.02/1/2376/2023</td></tr>
<tr><td>Tanggal Pembuatan</td><td>26 Mei 2023</td></tr>
<tr><td>Tanggal Revisi</td><td>-</td></tr>
<tr><td>Tanggal Efektif</td><td>26 Mei 2023</td></tr>
<tr><td>DIREKTORAT JENDERAL TENAGA KESEHATAN</td><td>Disahkan oleh</td><td>Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta,

Sudiro, SKp, Ners, M.Pd
NIP 196801041989031002</td></tr>
<tr><td>POLTEKKES KEMENKES SURAKARTA</td><td>Nama SOP</td><td>Layanan Troubleshooting Server</td></tr>
<tr><td>Dasar Hukum :</td><td colspan="2">Kualifikasi Pelaksanaan :</td></tr>
<tr><td>1. Peraturan Menteri Kesehatan Republik Indonesia Nomor 71 Tahun 2020 Tentang Organisasi dan Tata Kerja Politeknik Kesehatan di Lingkungan Badan Pengembangan dan Pemberdayaan Sumber Daya Manusia Kesehatan Kementerian Kesehatan;
2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi;</td><td colspan="2">1. Menguasai OS Linux
2. Menguasai firewall
3. Menguasai instalasi, konfigurasi dan troubleshooting server
4. Menguasai jaringan</td></tr>
<tr><td>Keterkaitan dengan SOP lain :</td><td colspan="2">Peralatan yang digunakan :</td></tr>
<tr><td>1. SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi
2. SOP Pengembangan Sistem Informasi</td><td colspan="2">1. Komputer/Laptop
2. Jaringan internet
3. Server
4. Data server</td></tr>
<tr><td>Peringatan :</td><td colspan="2">Pencatatan dan Pendataan :</td></tr>
<tr><td>Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada semua sistem aplikasi tidak dapat berjalan</td><td colspan="2">Disimpan dalam bentuk dokumen tercetak dan elektronik</td></tr>
</table>

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Unit IT	Pengelola Sistem Jaringan/Rekanan	Pengelola Aplikasi/Rekanan	Kelengkapan	Waktu	*Output/Outcome*	
1	Melakukan monitoring aplikasi				Komputer/laptop, koneksi internet, server		Data log server	Waktu monitoring dilakukan selama 24 jam setiap hari
2	Melakukan identifikasi masalah				Komputer/laptop, koneksi internet, server	2 x 24 jam	Laporan permasalahan server	
3	Melakukan pemeriksaan aplikasi dan database server				Komputer/laptop, koneksi internet, server	2 x 24 jam	Laporan permasalahan server	
4	Melaporkan permasalahan server				Komputer/laptop, koneksi internet, server	1 jam	Laporan permasalahan server	
5	Melakukan monitoring dan pemeriksaan server		Bermasalah? Ya		Komputer/laptop, koneksi internet, server		Laporan permasalahan server	Waktu monitoring dilakukan selama 24 jam setiap hari
6	Melakukan koordinasi jaringan		Tidak		Laporan permasalahan server	2 jam	Laporan permasalahan server	
7	Melakukan pemeriksaan dan perbaikan jaringan				Komputer/laptop, koneksi internet	1 hari	Laporan permasalahan jaringan dan waktu penyelesaian pekerjaan ini tergantung tingkat kerusakan dan ketersediaan hardware jaringan	
8	Melakukan uji coba koneksi jaringan				Komputer/laptop, koneksi internet	1 jam	Jaringan lancar	
9	Melakukan perbaikan server				Komputer/laptop, koneksi internet, server	2 x 24 jam	Laporan permasalahan server	
10	Melakukan uji coba aplikasi hingga aplikasi berjalan lancar				Komputer/laptop, koneksi internet, server	1 jam	Aplikasi berjalan lancar	

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

<table>
<tr><td rowspan="4">KEMENTERIAN KESEHATAN REPUBLIK INDONESIA</td><td>Nomor SOP</td><td>IR.02/1/2375/2023</td></tr>
<tr><td>Tanggal Pembuatan</td><td>26 Mei 2023</td></tr>
<tr><td>Tanggal Revisi</td><td>-</td></tr>
<tr><td>Tanggal Efektif</td><td>26 Mei 2023</td></tr>
<tr><td>DIREKTORAT JENDERAL TENAGA KESEHATAN</td><td>Disahkan oleh</td><td>Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta,

Sudiro, SKp, Ners, M.Pd
NIP 196801041989031002</td></tr>
<tr><td>POLTEKKES KEMENKES SURAKARTA</td><td>Nama SOP</td><td>Layanan Pemeliharaan Hardware dan Software TI</td></tr>
<tr><td colspan="2">Dasar Hukum :</td><td>Kualifikasi Pelaksanaan :</td></tr>
<tr><td colspan="2">1. Peraturan Menteri Kesehatan Republik Indonesia Nomor 71 Tahun 2020 Tentang Organisasi dan Tata Kerja Politeknik Kesehatan di Lingkungan Badan Pengembangan dan Pemberdayaan Sumber Daya Manusia Kesehatan Kementerian Kesehatan;
2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi;</td><td>1. Memahami tentang tugas dan fungsi unit IT
2. Memahami tentang rencana strategis Poltekkes Kemenkes Surakarta
3. Mengetahui prosedur pengadaan hardware dan software TI</td></tr>
<tr><td colspan="2">Keterkaitan dengan SOP lain :</td><td>Peralatan yang digunakan :</td></tr>
<tr><td colspan="2">1. SOP Pemeliharaan Jaringan Internet
2. SOP Layanan Troubleshooting Server
3. SOP Pengembangan Sistem Informasi</td><td>1. Komputer/Laptop
2. Jaringan internet
3. Printer
4. Kertas</td></tr>
<tr><td colspan="2">Peringatan :</td><td>Pencatatan dan Pendataan :</td></tr>
<tr><td colspan="2">Apabila SOP ini tidak dijalankan dengan baik, mengakibatkan terlambatnya pelayanan pada bagian TI</td><td>Disimpan dalam bentuk dokumen tercetak dan elektronik</td></tr>
</table>

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Unit IT	Pengelola Sistem Jaringan/Rekanan	Unit Layanan Pengadaan	Kelengkapan	Waktu	*Output/Outcome*	
1	Melakukan pemeriksaan *hardware /software* TI				*Hardware/software* TI	1 hari	Laporan kerusakan *hardware/software* TI	
2	Membuat laporan kerusakan *hardware/software* TI				Laporan kerusakan *hardware/software* TI	1 jam	Laporan kerusakan *hardware/software* TI	
3	Membuat rekapitulasi spesifikasi dan memberikan rekomendasi penggantian *hardware* TI				Laporan rekap spesifikasi dan rekomendasi penggantian *hardware* TI	1 hari	Laporan rekap spesifikasi dan rekomendasi penggantian *hardware* TI	
4	Memberikan persetujuan penggantian *hardware* TI				Laporan rekap penggantian *hardware* TI	1 hari	Laporan rekap penggantian *hardware* TI	
5	Melakukan pembelian *hardware* TI				*Hardware* TI, kwitansi		*Hardware* TI, kwitansi	Estimasi waktu tergantung ketersediaan dan waktu pengiriman barang pada e-katalog
6	Melakukan penggantian *hardware* TI				*Hardware* TI	1 hari	*Hardware* TI	
7	Melakukan perbaikan *software* TI				*Software* TI	1 hari	*Software* TI telah diperbaiki	
8	Menerima laporan penggantian *hardware* dan perbaikan *software* TI				Laporan penggantian *hardware* dan perbaikan *software* TI	1 jam	Laporan penggantian *hardware* dan perbaikan *software* TI	

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.02/1/2374/2023
	Tanggal Pembuatan	26 Mei 2023
	Tanggal Revisi	-
	Tanggal Efektif	26 Mei 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Permintaan Penambahan *Bandwidth***

Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Kesehatan Republik Indonesia Nomor 71 Tahun 2020 Tentang Organisasi dan Tata Kerja Politeknik Kesehatan di Lingkungan Badan Pengembangan dan Pemberdayaan Sumber Daya Manusia Kesehatan Kementerian Kesehatan; 2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi;	1. Menguasai website 2. Menguasai domain 3. Menguasai jaringan 4. Menguasai penambahan *bandwidth*
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi 2. SOP Pemeliharaan Jaringan Internet 3. SOP Layanan *Troubleshooting* Server	1. Komputer/Laptop 2. Jaringan internet 3. Website dan domain
Peringatan :	**Pencatatan dan Pendataan :**
Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada semua sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Unit Kerja Pemohon	Unit IT	Pengelola Sistem Jaringan/Rekanan	Kelengkapan	Waktu	*Output/Outcome*	
1	Pimpinan Unit kerja/Jurusan/Prodi pemohon berkordinasi kepada Unit IT terkait permohonan perubahan *bandwidth*				Permohonan perubahan *bandwidth*	30 menit	Permohonan perubahan *bandwidth*	
2	Melakukan cek ketersediaan *bandwidth* berdasarkan data daftar *bandwidth* apabila pengubahan *bandwidth* berupa penambahan *bandwidth*				Pengecekan ketersediaan *bandwidth*	30 menit	Data daftar *bandwidth*	
3	Apabila *bandwidth* tidak mencukupi dicarikan solusi mengenai masalah tersebut, jika ternyata permohonan tersebut tidak dapat dipenuhi, maka pengelola sistem jaringan/rekanan melaporkan hal tersebut kepada Unit IT dengan rekomendasi menunda implementasi permohonan itu menunggu penambahan alokasi *bandwidth*				Pengecekan ketersediaan *bandwidth*	1 jam	Rekomendasi Unit IT terkait penambahan *bandwidth*	
4	Apabila permohonan tersebut dapat dilaksanakan maka pengelola sistem jaringan/rekanan akan melaksanakan pengubahan dan melakukan pembaharuan data daftar ketersediaan *bandwidth*				Pembaharuan data daftar ketersediaan *bandwidth*	1 jam	Penambahan alokasi *bandwidth*	
5	Unit IT akan menginformasikan status penyelesaikan layanan *bandwidth* kepada pimpinan unit pemohon				Informasi penyelesaian penambahan *bandwidth*	30 menit	Informasi penyelesaian penambahan *bandwidth*	

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.02/1/2373/2023
	Tanggal Pembuatan	26 Mei 2023
	Tanggal Revisi	-
	Tanggal Efektif	26 Mei 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Pengembangan Sistem Informasi**

Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Kesehatan Republik Indonesia Nomor 71 Tahun 2020 Tentang Organisasi dan Tata Kerja Politeknik Kesehatan di Lingkungan Badan Pengembangan dan Pemberdayaan Sumber Daya Manusia Kesehatan Kementerian Kesehatan; 2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi;	1. Menguasai website 2. Menguasai domain 3. Menguasai jaringan
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi	1. Komputer/Laptop 2. Jaringan internet 3. Website dan domain
Peringatan :	**Pencatatan dan Pendataan :**
Apabila SOP ini tidak dijalankan dengan baik, maka layanan pada semua sistem aplikasi tidak dapat berjalan	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Unit Kerja Pemohon	Unit IT	Pengelola Aplikasi/Rekanan	Kelengkapan	Waktu	*Output/Outcome*	
1	Pimpinan Unit kerja/Jurusan/Prodi pemohon berkordinasi dengan Unit IT terkait permohonan pengembangan sistem informasi				Permohonan pengembangan sistem informasi	1 jam	Permohonan pengembangan sistem informasi	
2	Unit IT membuat rencana pengembangan sistem informasi				Rencana pengembangan sistem informasi	1 hari	Rencana pengembangan sistem informasi	
3	Unit IT menentukan sistem informasi yang akan dikembangkan, selanjutnya menunjuk pengelola aplikasi/rekanan untuk membuat kerangka acuan kerja				Kerangka acuan kerja	1 jam	Kerangka acuan kerja	
4	Pengelola aplikasi/rekanan membuat kerangka acuan kerja melalui aplikasi sistem informasi berdasarkan aturan yang berlaku				Kerangka acuan kerja	1 hari	Kerangka acuan kerja berdasarkan aturan yang berlaku	
5	Unit IT bersama pimpinan Unit kerja/Jurusan/Prodi pemohon melakukan evaluasi terhadap kerangka acuan kerja yang telah dibuat pengelola aplikasi/rekanan				Kerangka acuan kerja	1 hari	Evaluasi terhadap kerangka acuan kerja	
6	Unit IT memberitahukan hasil evaluasi kerangka acuan kerja kepada pengelola aplikasi/rekanan				Kerangka acuan kerja	1 jam	Hasil evaluasi kerangka acuan kerja	
7	Pengelola aplikasi/rekanan melaksanakan kegiatan pengembangan sistem informasi				Hasil evaluasi kerangka acuan kerja		Pengembangan sistem informasi	Estimasi waktu tergantung pada fitur pengembangan sistem informasi yang dibuat
8	Pengelola aplikasi/rekanan memberitahukan ke Unit IT jika sistem informasi telah selesai dibuat dan diinstalasi				Pemberitahuan sistem informasi telah selesai dibuat	1 jam	Sistem informasi telah selesai dibuat dan diinstalasi	
9	Pengelola aplikasi/rekanan membuat laporan dan *user manual* sistem informasi yang telah dibuat				Pembuatan laporan dan *user manual* sistem informasi	1 hari	Laporan dan *user manual* sistem informasi	
10	Pengelola aplikasi/rekanan melakukan presentasi pengembangan sistem informasi yang telah dibuat kepada Unit IT dan pimpinan Unit kerja/Jurusan/Prodi				Presentasi pengembangan sistem informasi	1 hari	Presentasi pengembangan sistem informasi kepada Unit IT dan Unit kerja pemohon	

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA	Nomor SOP	IR.01.02/1/2704/2023
	Tanggal Pembuatan	22 Juni 2023
	Tanggal Revisi	-
	Tanggal Efektif	22 Juni 2023
DIREKTORAT JENDERAL TENAGA KESEHATAN	Disahkan oleh	Direktur Politeknik Kesehatan Kementerian Kesehatan Surakarta, **Sudiro, SKp, Ners, M.Pd** NIP 196801041989031002
POLTEKKES KEMENKES SURAKARTA	Nama SOP	**Manajemen Keamanan Sistem Informasi (SI)**

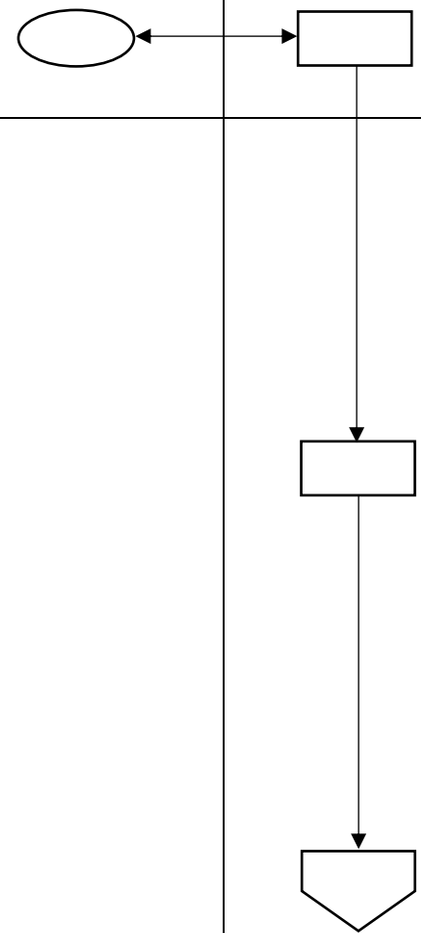
Dasar Hukum :	**Kualifikasi Pelaksanaan :**
1. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi; 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik	1. Memiliki kemampuan membangun aplikasi web yang sesuai dengan standar keamanan 2. Memiliki kemampuan anlisis terhadap spesifikasi perangkat lunak yang digunakan pada aplikasi web 3. Memiliki kemampuan untuk melakukan asesmen keamanan informasi pada aplikasi web
Keterkaitan dengan SOP lain :	**Peralatan yang digunakan :**
1. SOP Hak Akses Ruang Server dan Mesin Server 2. SOP Informasi Keterbukaan Publik Melalui Website dan Media Sosial 3. SOP Pemenuhan Permintaan Akses 4. SOP Pelayanan Pelaporan Gangguan Sistem Teknologi Informasi 5. SOP Pengembangan Sistem Informasi	1. Komputer / Laptop 2. Peralatan (*tools*) asesmen keamanan informasi 3. Aplikasi web yang akan diasesmen

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

Peringatan :	Pencatatan dan Pendataan :
1. Apabila prosedur ini dilaksanakan, spesifikasi perangkat lunak pada aplikasi web dapat terpantau dan dapat ditindaklanjuti secara cepat dan tepat untuk menghindari adanya celah keamanan pada aplikasi web 2. Apabila prosedur ini tidak dilaksanakan, aplikasi web berpotensi menjadi sasaran serangan siber sekaligus berpotensi menjadi pintu masuk serangan siber yang mengancam aplikasi-aplikasi lain yang berada dalam satu data center 3. Apabila prosedur ini dilaksanakan oleh pihak-pihak atau individu yang tidak memiliki kompetensi yang disebutkan, proses asesmen keamanan informasi pada aplikasi web tidak akan berjalan dengan baik. Sebab seluruh aspek yang mungkin harus dianalisis, dilaporkan, dan diperbaiki tidak akan terindentifikasi secara lengkap.	Disimpan dalam bentuk dokumen tercetak dan elektronik

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

No	Kegiatan	Pelaksana		Mutu Baku			Keterangan
		Ka Unit IT	Pengelola Aplikasi/ Rekanan	Kelengkapan	Waktu	*Output/Outcome*	
1	Pengumpulan informasi, monitoring dan berkoordinasi dengan pengelola aplikasi/rekanan pada aplikasi web yang akan diasesmen			Komputer/Laptop, Laporan rekap data aplikasi web yang akan diasesmen	3 hari	Laporan rekap data aplikasi web yang akan diasesmen	
2	Pelaksanaan asesmen keamanan informasi pada aplikasi web meliputi kegiatan sebagai berikut : a. Pemeriksaan perangkat lunak yang dipergunakan. b. Pemeriksaan pengaturan hak akses file dan folder pada direktori server (directory listing). c. Pemeriksaan standar keamanan yang digunakan pada fitur pembuatan password. d. Pemeriksaan kerentanan SQL, nosql, OS, dan LDAP Injection pada database. e. Pemeriksaan fitur Captcha. f. Pemeriksaan kerentanan terhadap serangan Cross-Site Scripting (XSS) g. Pemeriksaan implementasi Cross-Site Request Forgery (CSRF) token. h. Pemeriksaan kerentanan fungsi file upload. i. Pemeriksaan implementasi password storage. j. Pemeriksaan penggunaan XML untuk web service. k. Pemeriksaan konfigurasi pada cookie. l. Pemeriksaan access control. m. Pemeriksaan halaman back end. n. Pemeriksaan error handling. o. Pemeriksaan mode debug.			Komputer/Laptop, peralatan (*tools*) asesmen keamanan informasi	1 minggu	a. Perangkat lunak yang digunakan pada aplikasi web merupakan versi terbaru, ter-update, dan masih didukung secara penuh dan resmi oleh upstream provider. b. Memastikan file dan folder sensitif tidak bisa diakses oleh publik. c. Standar keamanan untuk password antara lain: • Berjumlah 8 karakter atau lebih. • Terdiri dari kombinasi huruf besar, huruf kecil, dan angka. • Menggunakan karakter tanda baca Contoh: !@#$%^&*()-=_+<>?”’{} dan sejenisnya. (Apabila tidak menggunakan karakter tanda baca maka jumlah karakter pada password minimal berjumlah 10 karakter.) d. Penyebab kerentanan SQL Injection adalah penulisan coding yang tidak memperhatikan best practice secure coding. e. Direkomendasikan menggunakan Captcha dari Google. f. Kerentanan Cross-Site Scripting (XSS) disebabkan oleh library yang tidak update dan/atau tidak	



Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

	p. Pemeriksaan fungsionalitas menu aplikasi web					dilakukan sanitasi dan validasi pada input pengguna. g. Cross-Site Request Forgery (CSRF) merupakan bentuk eksploitasi website yang dieksekusi atas wewenang korban, tanpa dikehendakinya h. Pada fungsi file upload tidak terdapat file upload yang executable, mengandung XML atau script yang berpotensi problem. i. Password storage menggunakan strong adaptive dan salted hashing functions / algoritma dengan delay factor, seperti Argon2, scrypt, bcrypt, atau PBKDF2). j. Menghindari penggunaan XML untuk webservice. k. Cookie menggunakan flag HttpOnly l. Pada access control, pengguna hanya dapat mengakses menu, fitur, dan data sesuai dengan kewenangannya. m. Halaman back end menggunakan alamat custom, yaitu tidak menggunakan alamat /admin, /login, dan sejenisnya. n. Pada error handling, apabila aplikasi mengalami error, maka aplikasi memberikan respon terhadap error tersebut, melalui notifikasi pop-up atau redirect ke halaman awal. o. Mode debug harus off atau tidak aktif. p. Seluruh menu pada aplikasi berfungsi sebagaimana mestinya	

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN

3	Analisis dan penyusunan laporan hasil asesmen keamanan informasi. Keterangan: a. Aplikasi web dinyatakan LULUS ASESMEN dengan syarat tidak ditemukan adanya celah keamanan pada aplikasi web atau celah keamanan yang ditemukan merupakan celah keamanan dengan resiko keamanan tingkat rendah dan/atau informasi yang harus segera diperbaiki oleh penanggung jawab aplikasi. b. Aplikasi web dinyatakan TIDAK LULUS ASESMEN apabila ditemukan adanya celah keamanan pada aplikasi web dengan resiko keamanan tingkat sedang dan/atau tinggi sedang dan/atau kritis yang harus segera diperbaiki oleh penanggung jawab aplikasi			Hasil analisis asesmen keamanan informasi	1 minggu	Laporan hasil analisis asesmen keamanan informasi	
4	Aplikasi yang dinyatakan lulus asesmen keamanan informasi dapat dilanjutkan rekomendasi pemasangan aplikasi web dan dilaporkan kepada Ka Unit IT			Laporan hasil analisis asesmen keamanan informasi	1 hari	Asesmen keamanan informasi dilanjutkan pemasangan aplikasi web	

Dokumen ini telah ditandatangani secara elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), BSSN