SEKOLAH TINGGI ILMU FARMASI YAYASAN PHARMASI
SEMARANG, JAWA TENGAH

PRODI / UNIT : TEKNOLOGI INFORMASI

DOKUMEN : PROSEDUR OPERASIONAL BAKU	
JENIS KEGIATAN: SOP Keamanan Informasi, Perlindungan Data, dan Pencadangan	
Kode : STIFAR/SOP/L.007	Tanggal Dikeluarkan :
Area :	No. Revisi :

Tujuan

SOP ini bertujuan:

1. Menjamin keamanan informasi dan data yang dikelola oleh STIFAR Yayasan Pharmasi Semarang.
2. Melindungi informasi dan data dari akses, penggunaan, perubahan, pengungkapan, kehilangan, kerusakan, atau pemusnahan yang tidak sah.
3. Menjamin kerahasiaan, integritas, dan ketersediaan informasi dan data institusi.
4. Mengatur pelaksanaan pencadangan data dan sistem informasi secara teratur dan terdokumentasi.
5. Memastikan data dapat dipulihkan apabila terjadi kehilangan, kerusakan, gangguan sistem, atau insiden keamanan informasi.
6. Mengatur pengamanan perangkat, sistem, jaringan, akun, aplikasi, dan media penyimpanan yang digunakan untuk pengelolaan informasi.
7. Meningkatkan kesadaran dan tanggung jawab seluruh pengguna dalam menjaga keamanan informasi dan perlindungan data.

Definisi

Keamanan Informasi, Perlindungan Data, dan Pencadangan mencakup proses pengamanan informasi dan data institusi dari akses, penggunaan, perubahan, pengungkapan, kehilangan, kerusakan, atau pemusnahan yang tidak sah, serta proses pencadangan dan pemulihan data dan sistem informasi untuk menjamin keberlangsungan layanan. Keamanan informasi mencakup pengendalian terhadap aspek kerahasiaan, integritas, dan ketersediaan informasi. Perlindungan data mencakup pengelolaan data sesuai dengan kewenangan, kebutuhan, tujuan penggunaan, dan ketentuan yang berlaku. Pencadangan merupakan proses membuat dan menyimpan salinan data atau konfigurasi sistem pada media atau lokasi penyimpanan yang

ditentukan agar dapat digunakan dalam proses pemulihan apabila terjadi gangguan atau kehilangan data.

Ruang Lingkup

SOP ini mengatur proses:

1. Identifikasi dan klasifikasi informasi serta data institusi.
2. Pengamanan data dan informasi dalam sistem informasi.
3. Pengendalian akses terhadap data dan informasi.
4. Perlindungan data pengguna, dosen, tenaga kependidikan, mahasiswa, dan pihak terkait.
5. Pengamanan perangkat komputer, server, jaringan, aplikasi, dan media penyimpanan.
6. Penggunaan kata sandi dan kredensial secara aman.
7. Pengamanan data selama penyimpanan, pengolahan, dan pemindahan.
8. Pengelolaan media penyimpanan dan perangkat yang mengandung data institusi.
9. Pencadangan database, file, aplikasi, konfigurasi, dan data penting lainnya.
10. Penentuan jadwal dan media pencadangan.
11. Pengujian hasil pencadangan dan pemulihan data.
12. Penyimpanan dan pengamanan salinan cadangan.
13. Pemulihan data dan sistem akibat gangguan atau insiden.
14. Penanganan insiden keamanan informasi.
15. Monitoring dan evaluasi keamanan informasi.
16. Penghapusan data dan media penyimpanan secara aman sesuai ketentuan.
17. Dokumentasi kegiatan keamanan, pencadangan, dan pemulihan data.

Pengguna

SOP ini digunakan oleh:

1. UPT Teknologi Informasi (UPT TI).
2. Administrator Sistem.
3. Unit Kerja/Program Studi.
4. Pimpinan STIFAR.

5. Dosen dan Tenaga Kependidikan.
6. Mahasiswa.
7. Pengelola sistem informasi dan data.
8. Vendor/Pihak Ketiga yang memperoleh akses terhadap sistem atau data institusi.

Referensi

1. Statuta STIFAR Yayasan Pharmasi Semarang.
2. Rencana Strategis STIFAR Yayasan Pharmasi Semarang.
3. Kebijakan dan Standar SPMI STIFAR Yayasan Pharmasi Semarang.
4. Kebijakan Pengelolaan Sistem dan Teknologi Informasi STIFAR.
5. Kebijakan Keamanan Informasi STIFAR.
6. Kebijakan/ketentuan Perlindungan Data STIFAR.
7. SOP Pengelolaan Akun dan Hak Akses Sistem Informasi.
8. SOP Pengelolaan Jaringan dan Internet.
9. SOP Inventarisasi dan Pengelolaan Aset Teknologi Informasi.
10. Ketentuan peraturan perundang-undangan yang berkaitan dengan sistem elektronik, keamanan informasi, dan pelindungan data.
11. ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi.
12. ISO/IEC 27002 tentang pengendalian keamanan informasi.

Prosedur

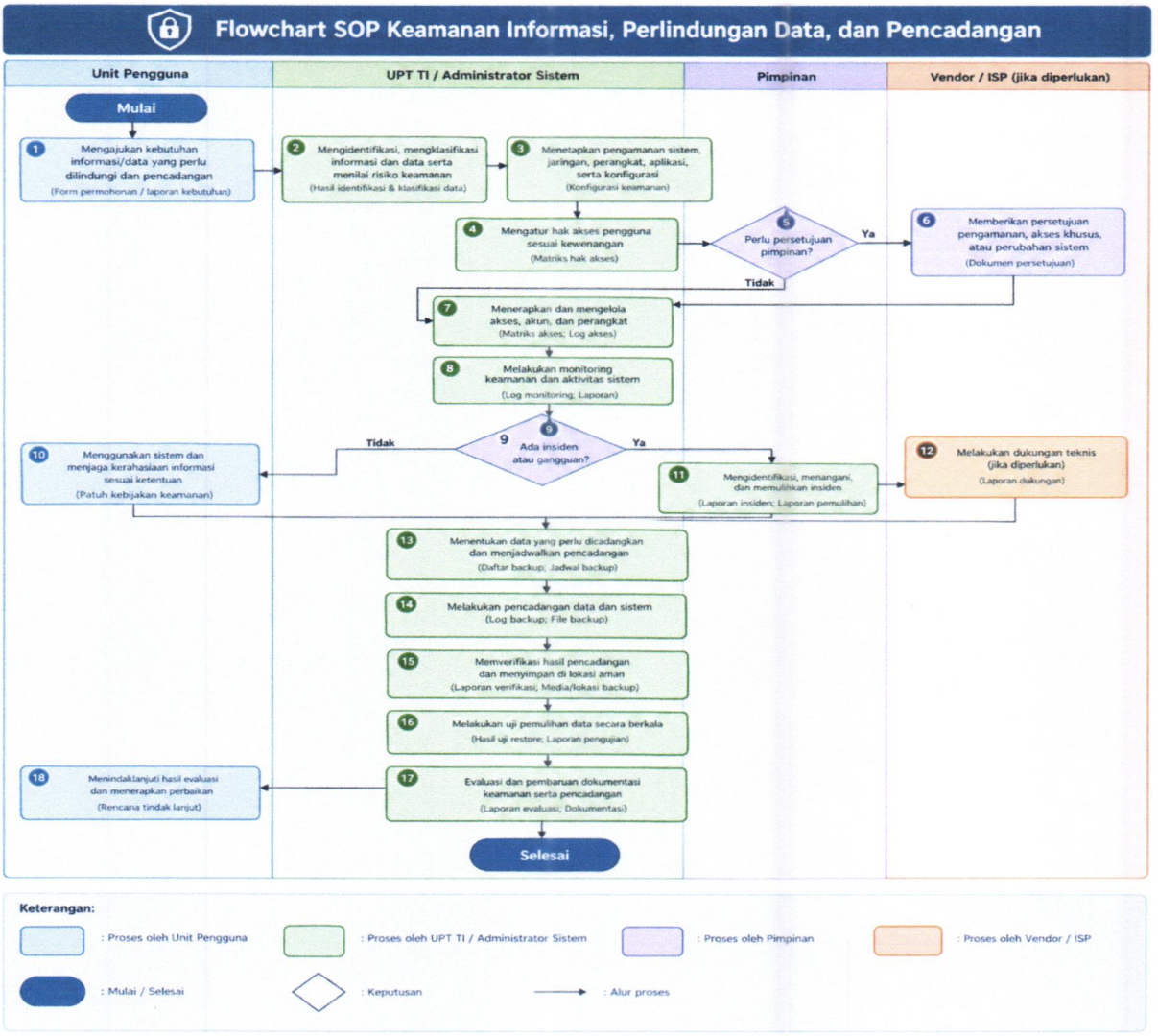
Tanggungjawab	Garis Besar Prosedur	Arsip/Dokumen Terkait
Unit Pengguna / UPT TI	Mengidentifikasi informasi dan data yang perlu dilindungi serta tingkat kepentingannya	Daftar informasi/data; Klasifikasi data
UPT TI	Mengidentifikasi risiko dan kebutuhan pengamanan informasi serta data	Hasil identifikasi risiko
UPT TI / Administrator Sistem	Menetapkan dan menerapkan pengamanan sistem, jaringan, perangkat, aplikasi, dan media penyimpanan	Konfigurasi keamanan; Pengendalian keamanan
UPT TI	Mengendalikan akses terhadap data berdasarkan kewenangan dan kebutuhan pengguna	Matriks hak akses; Log akses
Unit Pengguna / Pengguna	Menggunakan, menyimpan, dan membagikan informasi sesuai kewenangan dan ketentuan keamanan informasi	Data/informasi terkelola
UPT TI / Administrator Sistem	Melakukan monitoring terhadap keamanan sistem, jaringan, akun, dan aktivitas akses	Log monitoring; Laporan monitoring
UPT TI	Menentukan data, sistem, dan konfigurasi yang wajib dicadangkan serta jadwal pencadangan	Daftar backup; Jadwal backup
Administrator Sistem	Melaksanakan pencadangan database, file, konfigurasi, aplikasi, dan data penting sesuai jadwal	File backup; Log backup
Administrator Sistem / UPT TI	Memeriksa keberhasilan dan integritas hasil pencadangan	Laporan hasil backup
UPT TI	Menyimpan salinan cadangan pada media atau lokasi yang aman dan sesuai kebutuhan	Media/lokasi backup
UPT TI / Administrator Sistem	Melakukan pengujian pemulihan data secara berkala	Hasil uji restore; Laporan pengujian
Unit Pengguna / Pengguna	Melaporkan kehilangan data, dugaan kebocoran, akses tidak sah, atau insiden keamanan informasi	Laporan/tiket insiden
UPT TI / Administrator Sistem	Melakukan identifikasi, penanganan, pengamanan, dan pemulihan akibat insiden keamanan informasi	Laporan penanganan insiden

UPT TI / Administrator Sistem	Melakukan pemulihan data dan sistem menggunakan salinan cadangan apabila diperlukan	Data/sistem hasil pemulihan
UPT TI	Melakukan evaluasi keamanan informasi, efektivitas pencadangan, dan hasil pemulihan secara berkala	Laporan evaluasi; Rencana tindak lanjut
UPT TI / Administrator Sistem	Memperbarui dokumentasi keamanan, pencadangan, konfigurasi, dan prosedur berdasarkan hasil evaluasi	Dokumentasi keamanan; Dokumentasi backup

SEKOLAH TINGGI ILMU FARMASI YAYASAN PHARMASI
SEMARANG, JAWA TENGAH
PRODI / UNIT : TEKNOLOGI INFORMASI

DOKUMEN : PROSEDUR OPERASIONAL BAKU	
JENIS KEGIATAN: SOP Keamanan Informasi, Perlindungan Data, dan Pencadangan	
Kode : STIFAR/SOP/L.007	Tanggal Dikeluarkan :
Area :	No. Revisi :

Prosedur



Semarang,

Ketua Prodi / Unit

(Bayu Aditya, S. Kom)

PENGESAHAN			
Pembuat	Ketua UPT Teknologi Informasi	Bayu Aditya S. Kom.	
Mengetahui	Ketua LPMI	Dr. apt. M. Ryan Radix R. M.Sc	
Menyetujui	Ketua Stifar	Dr. apt. Endang Diyah Ikasari, M.Si.	