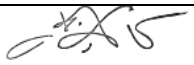
SOP BACK UP DAN KEAMANAN DATA SISTEM E-RISET UNIVERSITAS BAITURRAHMAH

Proses	Penanggungjawab			Tanggal
	Nama	Jabatan	Tanda tangan	
1. Perumusan	Dr.dr. Dita Hasni, M.Biomed	Ketua LPPM		14 Februari 2025
2. Pemeriksaan	dr. Rinita Amelia, M. Biomed, PhD	Wakil Rektor I		14 Februari 2025
3. Pertimbangan	Prof. Dr. Ir. Musliar Kasim, MS	Ketua Senat		14 Februari 2025
4. Persetujuan	Hj. Maizarnis	Yayasan		14 Februari 2025
5. Penetapan	Prof. Dr. Ir. Musliar Kasim, MS	Rektor		14 Februari 2025
6. Pengendalian	Dr. Drg. Utmi Arma, MDSC	Ka.LP3M		14 Februari 2025

1. TUJUAN

SOP ini bertujuan untuk:

1. Menjamin keamanan, integritas, dan ketersediaan data pada sistem e-Riset.
2. Mengatur mekanisme backup data secara berkala dan terdokumentasi.
3. Mencegah kehilangan, kerusakan, kebocoran, atau penyalahgunaan data institusi.
4. Menjamin pemulihan data (recovery) dapat dilakukan apabila terjadi gangguan sistem, kerusakan perangkat, atau insiden keamanan informasi.
5. Mendukung keberlangsungan layanan sistem e-Riset secara aman dan berkelanjutan.

2. RUANG LINGKUP

1. Backup data sistem e-Riset dan basis data institusi.
2. Pengamanan akses data dan server sistem e-Riset.
3. Pengelolaan penyimpanan backup lokal maupun cloud/server cadangan.
4. Monitoring keamanan sistem dan aktivitas pengguna.
5. Pemulihan data (restore/recovery) akibat gangguan atau kehilangan data.
6. Pengarsipan log keamanan dan audit trail sistem.

3. DEFINISI

1. Backup Data adalah proses penyalinan data dan dokumen sistem ke media penyimpanan lain sebagai cadangan keamanan.
2. Restore Data adalah proses pemulihan data dari hasil backup apabila terjadi kehilangan atau kerusakan data.
3. Keamanan Data adalah upaya perlindungan data dari akses tidak sah, kerusakan, perubahan, kehilangan, atau kebocoran.
4. Audit Trail adalah catatan aktivitas pengguna dan sistem yang tersimpan secara otomatis untuk kebutuhan pengawasan dan penelusuran aktivitas.
5. Hak Akses adalah kewenangan pengguna untuk mengakses fitur, data, dan fungsi tertentu dalam sistem e-Riset.
6. Disaster Recovery adalah proses pemulihan sistem dan data akibat gangguan besar, bencana, atau kegagalan sistem.

4. PENGGUNA

1. Admin Sistem e-Riset.
2. Unit Teknologi Informasi (TI).
3. LPPM sebagai pengelola data institusi.
4. Dosen/Peneliti/Pelaksana PkM sebagai pengguna sistem.
5. Pimpinan institusi sesuai kewenangan akses data.
6. Auditor internal atau pihak pengawas yang berwenang.

5. DASAR HUKUM

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).
2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
4. Permendikbud/Permendikbudristek terkait pengelolaan data pendidikan tinggi dan penelitian.

5. Kebijakan keamanan informasi dan tata kelola sistem informasi Universitas Baiturrahmah.
6. Ketentuan internal LPPM terkait pengelolaan data penelitian dan PkM.

6. PERSYARATAN

1. Tersedia server utama dan media penyimpanan backup.
2. Tersedia sistem e-Riset dan basis data institusi yang aktif.
3. Tersedia akun pengguna dan hak akses sistem yang tervalidasi.
4. Tersedia dokumen kebijakan keamanan data dan backup data.
5. Tersedia jadwal backup berkala dan mekanisme recovery data.
6. Tersedia log aktivitas sistem dan audit trail pengguna.
7. Tersedia perangkat keamanan sistem (firewall, autentikasi, antivirus, enkripsi, dll.).
8. Tersedia petugas/admin yang bertanggung jawab terhadap backup dan keamanan data.

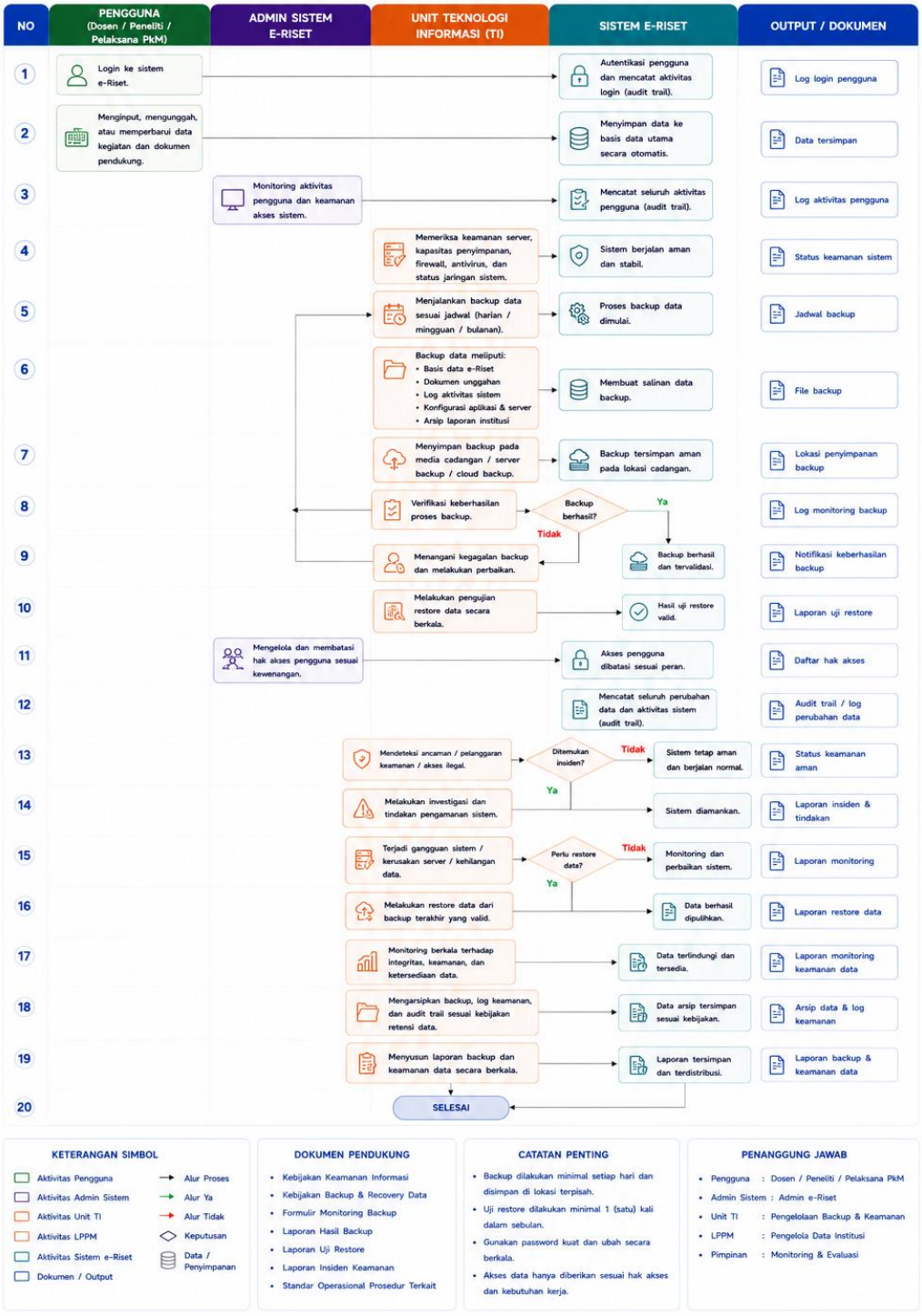
7. STANDAR OPERASIONAL PROSEDUR

1. Pengguna login ke sistem e-Riset sesuai hak akses masing-masing.
2. Sistem melakukan autentikasi pengguna dan mencatat aktivitas login pada audit trail.
3. Pengguna menginput, mengunggah, atau memperbarui data kegiatan penelitian, PkM, luaran, HKI, dan dokumen pendukung lainnya.
4. Sistem menyimpan data secara otomatis ke basis data utama institusi.
5. Admin sistem melakukan monitoring aktivitas sistem dan keamanan akses pengguna secara berkala.
6. Unit TI melakukan pemeriksaan keamanan server, kapasitas penyimpanan, firewall, antivirus, dan status jaringan sistem.
7. Sistem melakukan backup data otomatis sesuai jadwal yang telah ditetapkan (harian, mingguan, atau bulanan).
8. Backup data meliputi:
    a. Basis data e-Riset
    b. Dokumen unggahan pengguna
    c. Log aktivitas sistem
    d. Konfigurasi aplikasi dan server
    e. Arsip laporan institusi
9. Sistem menyimpan salinan backup pada media penyimpanan cadangan/server backup/cloud backup sesuai kebijakan institusi.
10. Unit TI melakukan verifikasi keberhasilan proses backup dan mencatat hasil backup dalam log monitoring.
11. Apabila proses backup gagal, sistem memberikan notifikasi kepada admin dan Unit TI untuk dilakukan tindakan perbaikan.
12. Unit TI melakukan pengujian restore/recovery data secara berkala untuk memastikan backup dapat digunakan apabila terjadi gangguan sistem.
13. Admin sistem melakukan pembatasan dan pengelolaan hak akses pengguna sesuai kewenangan dan kebutuhan kerja.
14. Sistem mencatat seluruh aktivitas pengguna dan perubahan data dalam audit trail.

15. Apabila ditemukan indikasi pelanggaran keamanan, akses ilegal, atau kebocoran data, admin dan Unit TI segera melakukan investigasi dan tindakan pengamanan sistem.
16. Dalam kondisi gangguan sistem, kerusakan server, atau kehilangan data, Unit TI melakukan proses restore data dari backup terakhir yang valid.
17. LPPM melakukan monitoring berkala terhadap integritas, keamanan, dan ketersediaan data institusi.
18. Data backup, log keamanan, dan audit trail diarsipkan sesuai kebijakan retensi data institusi.
19. Unit TI dan LPPM menyusun laporan backup dan keamanan data secara berkala untuk kebutuhan monitoring, evaluasi, dan audit institusi.
20. Proses backup dan keamanan data dinyatakan selesai setelah data tersimpan aman, terdokumentasi, dan sistem dapat beroperasi kembali secara normal apabila diperlukan proses recovery.

1. *FLOWCHART*

FLOWCHART SOP BACK UP DAN KEAMANAN DATA SISTEM E-RISET



Keterangan pembuatan flowchart SOP:

- Diagram alir SOP Back Up dan Keamanan Data menjelaskan mekanisme pengamanan, pencadangan (backup), monitoring, serta pemulihan data pada sistem e-Riset untuk menjamin integritas, ketersediaan, dan keamanan data institusi. Proses ini melibatkan pengguna sistem, admin sistem e-Riset, Unit Teknologi Informasi (TI), sistem e-Riset, serta unit pengelola institusi.
- Proses dimulai dari pengguna, yaitu dosen, peneliti, atau pelaksana PkM, yang login ke sistem e-Riset menggunakan akun yang telah diberikan hak akses. Sistem melakukan autentikasi pengguna dan secara otomatis mencatat aktivitas login ke dalam audit trail. Setelah login, pengguna dapat menginput, memperbarui, atau mengunggah data kegiatan dan dokumen pendukung ke sistem. Data yang diinput akan tersimpan secara otomatis ke basis data utama institusi.
- Selanjutnya admin sistem e-Riset melakukan monitoring aktivitas pengguna dan keamanan akses sistem. Seluruh aktivitas pengguna dicatat dalam audit trail untuk memastikan keterlacakan penggunaan sistem. Pada saat yang sama, Unit TI melakukan pemeriksaan terhadap keamanan server dan infrastruktur sistem, meliputi kapasitas penyimpanan, firewall, antivirus, serta stabilitas jaringan agar sistem tetap berjalan aman dan stabil.
- Tahap berikutnya adalah pelaksanaan backup data. Unit TI menjalankan backup data secara berkala sesuai jadwal yang telah ditetapkan, baik harian, mingguan, maupun bulanan. Data yang dibackup mencakup basis data e-Riset, dokumen unggahan pengguna, log aktivitas sistem, konfigurasi aplikasi dan server, serta arsip laporan institusi. Sistem kemudian membuat salinan backup dan menyimpannya pada media cadangan seperti server backup atau cloud backup.
- Setelah backup dilakukan, Unit TI memverifikasi keberhasilan proses backup. Apabila backup berhasil, sistem mencatat bahwa backup telah tervalidasi dan menghasilkan log monitoring backup serta notifikasi keberhasilan backup. Namun apabila backup gagal, Unit TI melakukan penanganan kegagalan dan tindakan perbaikan hingga proses backup berhasil dijalankan kembali.
- Untuk memastikan backup dapat digunakan saat diperlukan, Unit TI secara berkala melakukan pengujian restore data. Hasil uji restore dicatat sebagai laporan validasi pemulihan data. Selain itu, admin sistem mengelola dan membatasi hak akses pengguna sesuai kewenangan masing-masing. Sistem mencatat seluruh perubahan data dan aktivitas sistem dalam audit trail untuk menjaga akuntabilitas penggunaan sistem.
- Pada tahap keamanan sistem, Unit TI melakukan deteksi terhadap ancaman atau pelanggaran keamanan dan akses ilegal. Apabila tidak ditemukan insiden, sistem dinyatakan aman dan tetap berjalan normal. Namun jika ditemukan insiden keamanan, Unit TI melakukan investigasi dan tindakan pengamanan sistem untuk mencegah kerusakan atau kebocoran data lebih lanjut.

- Apabila terjadi gangguan sistem, kerusakan server, atau kehilangan data, dilakukan evaluasi apakah diperlukan proses restore data. Jika restore diperlukan, Unit TI melakukan pemulihan data menggunakan backup terakhir yang valid hingga data berhasil dipulihkan dan sistem kembali normal. Seluruh proses pemulihan dicatat dalam laporan restore data dan laporan monitoring sistem.
- LPPM melakukan monitoring berkala terhadap integritas, keamanan, dan ketersediaan data institusi. Backup data, log keamanan, dan audit trail kemudian diarsipkan sesuai kebijakan retensi data institusi. Pada tahap akhir, LPPM dan Unit TI menyusun laporan backup dan keamanan data secara berkala sebagai bagian dari monitoring, evaluasi, audit internal, dan pengendalian sistem institusi.
- Flowchart ini menegaskan bahwa keamanan data dan backup sistem e-Riset harus dilakukan secara terencana, berkala, terdokumentasi, dan terintegrasi agar data institusi tetap aman, tersedia, terlindungi dari kehilangan maupun akses ilegal, serta dapat dipulihkan apabila terjadi gangguan sistem.
-

2. PENUTUP

1) SOP ini mulai berlaku sejak tanggal ditetapkan dengan ketentuan apabila terdapat kekeliruan akan diadakan perubahan sebagaimana mestinya.
2) Hal-hal yang belum diatur dalam SOP ini akan ditetapkan kemudian, sesuai dengan peraturan perundang-undangan.