KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS LAMPUNG
Jalan Prof. Dr. Soemantri Brojonegoro No. 1 Bandar Lampung 35145
Telepon (0721) 701609, Fax. (0721) 702767
laman http://unila.ac.id

SALINAN
Reg. 4/2026

PERATURAN REKTOR UNIVERSITAS LAMPUNG
NOMOR 4 TAHUN 2026

TENTANG

SISTEM INFORMASI TERINTEGRASI, INFRASTRUKTUR JARINGAN, DAN KEAMANAN DATA

DENGAN RAHMAT TUHAN YANG MAHA ESA

REKTOR UNIVERSITAS LAMPUNG,

Menimbang:
a. bahwa berdasarkan Statuta Unila, Rektor Universitas Lampung memiliki tugas dan wewenang menyelenggarakan sistem informasi manajemen berbasis teknologi informasi dan komunikasi yang mendukung pengelolaan Tridharma Perguruan Tinggi, akuntasi dan keuangan, kepersonaliaan, kemahasiswaan, dan kealumnian;
b. bahwa dalam menjalankan tugas dan wewenang sebagaimana dimaksud pada huruf a, perlu diatur pengelolaan sistem teknologi informasi dan infrastruktur jaringan yang mendukung layanan akademik dan non-akademik secara efisien serta aman dari ancaman serangan siber yang semakin meningkat;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan huruf b, perlu menetapkan Peraturan Rektor Universitas Lampung tentang Sistem Informasi Terintegrasi, Infrastruktur Jaringan, dan Keamanan Data;

Mengingat:
1. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 158, Tambahan Lembaran Negara Republik Indonesia Nomor 5336);
2. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 16, Tambahan Lembaran Negara Nomor 5500);
3. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);

4. Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Nomor 6 Tahun 2015 tentang Statuta Universitas Lampung (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 518);
5. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia Nomor 31 Tahun 2022 tentang Satu Data Pendidikan, Kebudayaan, Riset, dan Teknologi (Berita Negara Republik Indonesia Tahun 2024 Nomor 633);
6. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia Nomor 49 Tahun 2024 tentang Organisasi dan Tata Kerja Universitas Lampung (Berita Negara Republik Indonesia Tahun 2022 Nomor 666);

MEMUTUSKAN:

Menetapkan: PERATURAN REKTOR TENTANG SISTEM INFORMASI TERINTEGRASI, INFRASTRUKTUR JARINGAN, DAN KEAMANAN DATA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Rektor ini, yang dimaksud dengan:

1. Universitas Lampung yang selanjutnya disebut Unila merupakan perguruan tinggi yang diselenggarakan oleh Kementerian Pendidikan Tinggi, Sains dan Teknologi.
2. Rektor adalah Organ Unila yang memimpin penyelenggaraan dan pengelolaan Unila.
3. Wakil Rektor adalah Wakil Rektor Bidang Perencanaan, Kerja Sama, dan Teknologi Informasi dan Komunikasi.
4. Sistem Informasi adalah teknologi yang digunakan untuk mendukung operasi dan manajemen data.
5. Unit Kerja adalah seluruh unit kerja yang berfungsi mendukung implementasi sistem informasi dan infrastruktur jaringan di lingkungan Unila, meliputi Fakultas, Pascasarjana, Lembaga, Unit Penunjang Akademik, dan Badan di lingkungan Unila.
6. Unit Penunjang Akademik Teknologi Informasi dan Komunikasi yang selanjutnya disebut UPA TIK merupakan unit penunjang akademik yang mempunyai tugas melaksanakan pengembangan, pengelolaan, dan pemberian layanan teknologi informasi dan komunikasi serta pengelolaan sistem informasi dan jaringan di lingkungan Unila.
7. Sistem Informasi Terintegrasi adalah sistem informasi yang dirancang untuk memungkinkan pertukaran data dan informasi secara efisien antara berbagai unit kerja di lingkungan Unila guna mendukung layanan akademik, non akademik, administratif, dan operasional.
8. Sistem Informasi Terpusat atau disebut myUnila, adalah platform utama layanan digital Unila yang berfungsi sebagai pusat pengelolaan, integrasi, pemrosesan, penyimpanan, dan penyajian data serta informasi secara terpadu yang dikelola oleh UPA TIK.

9. Infrastruktur Jaringan adalah perangkat keras, perangkat lunak, dan layanan yang digunakan untuk mendukung komunikasi dan pengelolaan data di lingkungan Unila.
10. Mitigasi Serangan Siber adalah langkah-langkah pencegahan, pendeteksian, dan penanganan serangan terhadap sistem informasi, data, dan infrastruktur jaringan guna melindungi kerahasiaan, integritas, dan ketersediaan informasi.

BAB II
TUJUAN DAN RUANG LINGKUP

Pasal 2

Peraturan Rektor ini bertujuan untuk:
a. Mengintegrasikan seluruh sistem informasi akademik, non-akademik, dan administratif;
b. Menjamin pengelolaan infrastruktur jaringan yang handal, efisien, dan aman;
c. Memberikan pedoman mitigasi serangan siber dan langkah-langkah pemulihan bencana (*disaster recovery plan*);
d. Mendukung pelaksanaan layanan berbasis teknologi informasi untuk mewujudkan *One Data* Unila.

Pasal 3

Ruang Lingkup Peraturan Rektor ini mengatur:
a. Pengelolaan sistem informasi terintegrasi untuk layanan akademik, non akademik, dan administratif;
b. Penyediaan dan pengelolaan infrastruktur jaringan internal dan eksternal;
c. Kebijakan keamanan data dan mitigasi serangan siber;
d. Koordinasi antara UPA TIK dengan seluruh unit kerja di lingkungan Unila.

BAB III
PENGELOLAAN DAN KEBIJAKAN

Bagian Kesatu
Pengelolaan Sistem Informasi Terintegrasi

Pasal 4

Pengelolaan sistem informasi terintegrasi diatur dengan ketentuan:
a. Sistem informasi yang mencakup pengelolaan data dan informasi untuk:
   1) Layanan akademik, termasuk pendaftaran mahasiswa, penilaian, dan pengelolaan jadwal;
   2) Layanan non-akademik, seperti kegiatan kemahasiswaan, penelitian, dan pengabdian masyarakat;
   3) Layanan administratif, termasuk keuangan, kepegawaian, dan manajemen aset.
b. Sistem informasi terintegrasi mendukung interoperabilitas antarunit kerja untuk memastikan kelancaran operasional.
c. Sistem informasi terintegrasi wajib menggunakan protokol keamanan data yang sesuai dengan standar nasional dan internasional.

Pasal 5

Standar operasional sistem informasi terintegrasi mencakup:

a. Sistem informasi terintegrasi harus dirancang dan dikelola sesuai dengan standar operasional yang mencakup:
   1) Keandalan: Sistem harus mampu menangani beban kerja yang tinggi tanpa gangguan;
   2) Keamanan: Sistem wajib dilengkapi dengan protokol keamanan data untuk melindungi informasi sensitif;
   3) Interoperabilitas: Sistem harus kompatibel dengan aplikasi dan perangkat lain yang digunakan oleh Unila;
   4) Kemudahan Penggunaan: Sistem harus memiliki antarmuka pengguna yang sederhana dan mudah diakses oleh semua pemangku kepentingan.
b. Setiap unit kerja wajib mematuhi standar operasional sistem informasi terintegrasi yang ditetapkan oleh Rektor.

Pasal 6

(1) Seluruh data dan informasi yang dihasilkan oleh unit kerja di Unila wajib diintegrasikan ke dalam myUnila, yang dikelola oleh UPA TIK.
(2) Ketentuan lebih lanjut mengenai tata cara pengembangan, integrasi, pengelolaan, dan pemanfaatan sistem untuk mendukung implementasi myUnila diatur dan ditetapkan dengan Keputusan Rektor.
(3) Setiap unit kerja bertanggung jawab atas keakuratan dan keandalan data yang disediakan.
(4) Proses integrasi data harus menggunakan format standar yang ditetapkan oleh UPA TIK untuk memastikan konsistensi dan kompatibilitas.

Pasal 7

(1) Akses terhadap sistem informasi terintegrasi diatur berdasarkan hierarki jabatan dan kebutuhan operasional, meliputi:
   a. Hak Akses Administrator, diberikan kepada UPA TIK untuk mengelola dan memantau sistem;
   b. Hak Akses Unit Kerja, diberikan kepada staf di unit kerja untuk menjalankan fungsi terkait;
   c. Hak Akses Pengguna Akhir, diberikan kepada mahasiswa, dosen, dan pemangku kepentingan lain untuk layanan tertentu.
(2) Pengguna wajib menjaga kerahasiaan kredensial akses sistem dan dilarang membagikannya kepada pihak yang tidak berwenang.
(3) Pelanggaran hak akses akan dikenakan sanksi sesuai ketentuan peraturan perundang-undangan.

Pasal 8

(1) Dalam hal pengembangan dan Pemeliharaan Sistem, UPA TIK bertanggung jawab untuk:
   a. Mengembangkan fitur baru dalam sistem terintegrasi sesuai kebutuhan operasional;
   b. Melakukan pemeliharaan berkala untuk memastikan sistem berjalan dengan baik;
   c. Menyediakan pelatihan kepada pengguna sistem di unit kerja terkait.
(2) Setiap pengembangan dan pemeliharaan sistem wajib melalui evaluasi dan persetujuan oleh Rektor.

Pasal 9

(1) Monitoring sistem terintegrasi dilakukan oleh UPA TIK melalui:
   a. Pemantauan real-time terhadap performa sistem;
   b. Pelaporan insiden dan masalah teknis oleh unit kerja;
   c. Analisis data untuk mengidentifikasi kebutuhan peningkatan sistem.
(2) Evaluasi sistem dilakukan secara berkala setiap enam bulan dengan melibatkan seluruh unit kerja.
(3) Hasil evaluasi digunakan untuk:
   a. Menyusun rekomendasi peningkatan sistem;
   b. Menyusun laporan kinerja sistem kepada Rektor.

Bagian Kedua
Penyediaan dan Pengelolaan Infrastruktur Jaringan

Pasal 10

Infrastruktur jaringan Unila dirancang untuk:
a. Mendukung komunikasi data yang cepat, stabil, dan aman di lingkungan Unila;
b. Menyediakan akses yang terintegrasi bagi seluruh sivitas akademika dan tenaga kependidikan untuk layanan akademik dan non-akademik;
c. Menjamin keberlangsungan operasional sistem informasi Unila, baik dalam skala internal maupun eksternal.

Pasal 11

Penyediaan dan pengelolaan infrastruktur jaringan diatur dengan ketentuan:
a. Infrastruktur jaringan di Unila mencakup:
   1) Jaringan lokal (LAN) dan nirkabel (*Wi-Fi*) untuk mendukung akses data di lingkungan kampus;
   2) Perangkat keras, seperti *server, router, dan switch*, yang diperlukan untuk pengelolaan jaringan;
   3) Pusat data utama dan pusat data cadangan untuk memastikan kontinuitas layanan.
b. Infrastruktur jaringan wajib dikelola secara profesional oleh UPA TIK, dengan pemeliharaan berkala untuk memastikan ketersediaan dan keandalan.
c. Jaringan internal dan eksternal harus memiliki perlindungan terhadap ancaman keamanan, termasuk penggunaan *firewall*, enkripsi data, dan sistem pemantauan *real-time*.

Pasal 12

(1) Pengelolaan infrastruktur jaringan menjadi tanggung jawab UPA TIK.
(2) Tanggung jawab pengelolaan meliputi antara lain:
   a. Perencanaan dan pengembangan jaringan sesuai kebutuhan Unila;
   b. Pemeliharaan perangkat keras dan perangkat lunak jaringan secara berkala;
   c. Pemantauan *real-time* terhadap performa jaringan menggunakan alat pemantauan khusus (*network monitoring tools*).
(3) Setiap perangkat keras yang akan digunakan dalam jaringan Unila wajib disetujui oleh UPA TIK untuk memastikan kompatibilitas dan keamanan.

Pasal 13

(1) Upaya penjagaan keamanan jaringan mencakup:
   a. Proteksi terhadap ancaman eksternal, seperti serangan *malware*, *ransomware*, atau *phishing*;
   b. Proteksi terhadap ancaman internal, seperti akses tidak sah atau penyalahgunaan jaringan oleh pengguna internal;
   c. Implementasi sistem autentikasi ganda (*Two-Factor Authentication*) untuk akses jaringan tertentu.
(2) Pemantauan keamanan jaringan dilakukan secara *real-time* oleh UPA TIK dengan menggunakan sistem deteksi dan pencegahan intrusi (*Intrusion Detection and Prevention Systems*).
(3) Setiap insiden keamanan jaringan pada Unit Kerja wajib dilaporkan kepada UPA TIK dalam waktu paling lambat 24 jam sejak diketahuinya insiden untuk ditindaklanjuti.

Pasal 14

(1) Penggunaan jaringan internal dan eksternal Unila hanya diperbolehkan untuk:
   a. Aktivitas Tri Dharma Perguruan Tinggi dan administrasi Unila;
   b. Kegiatan pendukung seperti seminar, konferensi, dan pelatihan.
(2) Dilarang menggunakan jaringan Unila untuk:
   a. Aktivitas yang melanggar hukum, seperti pembajakan perangkat lunak atau konten;
   b. Penyebaran konten tidak etis, termasuk hoaks dan ujaran kebencian;
   c. Aktivitas komersial tanpa izin resmi dari Unila.
(3) Dilarang menggunakan jaringan internal dan eksternal Unila untuk mengunduh, menginstal, maupun mengoperasikan perangkat lunak (software) yang tidak memiliki lisensi resmi serta melakukan aktivitas ilegal lainnya yang dapat merugikan universitas maupun melanggar ketentuan hukum yang berlaku.
(4) Setiap pelanggaran dalam penggunaan jaringan akan dikenakan sanksi sesuai dengan ketentuan yang berlaku di Unila.

Pasal 15

(1) Pemeliharaan infrastruktur jaringan dilakukan secara berkala oleh UPA TIK, mencakup antara lain:
   a. Pemeriksaan kondisi perangkat keras, seperti router dan server;
   b. Pembaruan perangkat lunak untuk menjaga kompatibilitas dan keamanan;
   c. Penggantian perangkat yang telah usang atau tidak berfungsi dengan baik.
(2) Dalam hal terjadi gangguan jaringan, UPA TIK wajib:
   a. Memberikan tanggapan awal dalam waktu maksimal 2 jam setelah laporan diterima;
   b. Menyelesaikan perbaikan dalam waktu 24 jam untuk gangguan yang ringan, atau paling lambat 72 jam untuk gangguan yang berat.
(3) Pemeliharaan dan perbaikan wajib dilaporkan dalam log jaringan dan disertakan dalam evaluasi kinerja tahunan.

Pasal 16

(1) Evaluasi infrastruktur jaringan dilakukan setiap enam bulan oleh UPA TIK untuk menilai:
   a. Kinerja jaringan berdasarkan tingkat kecepatan, stabilitas, dan keamanan;
   b. Kebutuhan peningkatan kapasitas jaringan sesuai dengan jumlah pengguna;
   c. Efektivitas perangkat keamanan dalam melindungi jaringan.
(2) Hasil evaluasi digunakan untuk menyusun rencana kerja tahunan yang mencakup pengembangan dan peningkatan infrastruktur jaringan.
(3) Rencana kerja tahunan ini wajib disetujui oleh Rektor sebelum diimplementasikan.

Bagian Ketiga
Kebijakan Keamanan Data dan Mitigasi Serangan Siber

Pasal 17

Keamanan siber bertujuan untuk:
   a. Melindungi kerahasiaan, integritas, dan ketersediaan data serta sistem informasi Unila;
   b. Mencegah dan meminimalkan risiko serangan siber;
   c. Meningkatkan kesadaran dan kepatuhan terhadap protokol keamanan siber di lingkungan Unila.

Pasal 18

Kebijakan keamanan data dan mitigasi serangan siber di lingkungan Unila dilakukan dengan ketentuan:
   a. Seluruh unit kerja di lingkungan UNILA wajib melaporkan insiden keamanan data paling lambat 2 x 24 jam sejak diketahuinya insiden keamanan kepada UPA TIK untuk ditindaklanjuti.
   b. Mitigasi serangan siber meliputi:
      1) Pendeteksian dini terhadap ancaman siber, termasuk *malware*, *ransomware*, dan serangan *phishing*;
      2) Penerapan kebijakan autentikasi ganda (*two-factor authentication*) untuk akses ke sistem informasi;
      3) Penyusunan rencana tanggap darurat untuk mengatasi insiden siber;
      4) Pemulihan data dan layanan melalui implementasi *disaster recovery plan*.
   c. UPA TIK menerapkan langkah-langkah mitigasi serangan siber berikut:
      1) Pencegahan:
         a) Penggunaan *firewall*, antivirus, dan enkripsi data;
         b) Penerapan autentikasi ganda (*Two-Factor Authentication*) untuk akses sistem.
      2) Pendeteksian:
         a) Sistem deteksi ancaman secara real-time menggunakan *Intrusion Detection System* (IDS);
         b) Pemantauan log aktivitas pengguna untuk mendeteksi aktivitas mencurigakan.
      3) Penanganan:
         a) Tim Tanggap Insiden Siber (*Computer Security Incident Response Team/ CSIRT*) yang siap 24/7 untuk menangani ancaman;
         b) Prosedur darurat untuk memblokir akses jika terjadi serangan.

4) Pemulihan:
   a) Implementasi *Disaster Recovery Plan* (DRP) untuk memastikan pemulihan data dan sistem setelah serangan;
   b) Penyediaan pusat data cadangan untuk kontinuitas layanan.

Pasal 19

(1) Dalam hal terjadi serangan siber, UPA TIK wajib:
   a. Melakukan analisis awal terhadap serangan dalam waktu maksimal 2 jam setelah deteksi;
   b. Memberikan notifikasi darurat kepada unit kerja terkait untuk menghentikan aktivitas yang berisiko;
   c. Melakukan isolasi sistem yang terkena serangan untuk mencegah penyebaran lebih lanjut.
(2) Prosedur pemulihan mencakup:
   a. Pemulihan data melalui backup yang tersedia di pusat data cadangan;
   b. Evaluasi menyeluruh untuk menentukan penyebab dan mencegah serangan serupa di masa depan.

Pasal 20

(1) Evaluasi keamanan siber dilakukan oleh UPA TIK setiap enam bulan sekali untuk menilai efektivitas sistem keamanan.
(2) Audit eksternal terhadap sistem keamanan dapat dilakukan untuk memastikan kepatuhan terhadap standar nasional dan internasional.
(3) Hasil evaluasi dan audit wajib dilaporkan kepada Rektor untuk dijadikan dasar pengambilan keputusan strategis.

BAB IV
TANGGUNG JAWAB DAN KOORDINASI

Pasal 21

(1) UPA TIK bertanggung jawab dalam:
   a. Penyusunan kebijakan teknis terkait pengelolaan sistem informasi, dengan cara:
      1) Merancang, mengembangkan, dan mengelola sistem informasi akademik dan non-akademik.
      2) Menyusun standar operasional sistem informasi yang berlaku untuk semua unit kerja.
   b. Penyusunan kebijakan teknis terkait infrastruktur jaringan, dengan cara:
      1) Menyediakan jaringan yang stabil dan aman di seluruh lingkungan UNILA.
      2) Melakukan pemeliharaan rutin perangkat keras dan perangkat lunak jaringan.
   c. Penyusunan kebijakan teknis terkait mitigasi serangan Siber, dengan cara:
      1) Menyusun kebijakan keamanan data dan mitigasi ancaman siber.
      2) Melakukan pemantauan real-time terhadap ancaman keamanan siber.
      3) Melatih staf unit kerja dan mahasiswa mengenai kesadaran keamanan siber (*cybersecurity awareness*).
   d. Monitoring dan evaluasi pelaksanaan sistem terintegrasi di semua unit kerja;
   e. Melaporkan hasil kinerja kepada Rektor UNILA setiap semester.

(2) Unit Kerja bertanggung jawab dalam:
   a. Melaksanakan protokol keamanan data yang telah ditetapkan oleh UPA TIK di unit kerja masing-masing;
   b. Melaporkan kebutuhan teknis dan kendala terkait sistem informasi kepada UPA TIK;
   c. Melakukan koordinasi dengan UPA TIK terkait pengelolaan data dan infrastruktur jaringan;
   d. Memastikan data dan informasi yang diberikan kepada UPA TIK sesuai dengan standar yang ditetapkan;
   e. Menunjuk koordinator teknis untuk berkomunikasi dengan UPA TIK.

Pasal 22

(1) Koordinasi dan monitoring bertujuan untuk:
   a. Memastikan pelaksanaan sistem terintegrasi, infrastruktur jaringan, dan keamanan siber berjalan sesuai dengan kebijakan UNILA;
   b. Meningkatkan efektivitas kerja sama antara UPA TIK dengan seluruh unit kerja;
   c. Menjamin keterpaduan pengelolaan sistem informasi dan data antarunit kerja.
(2) Koordinasi antara UPA TIK dan Unit Kerja dilakukan melalui pertemuan koordinasi rutin antara UPA TIK dan unit kerja, dan/atau sistem pelaporan digital yang memungkinkan komunikasi dua arah secara *real-time*;
(3) Koordinasi sebagaimana dimaksud pada ayat (1) dilakukan dengan rincian mekanisme berikut:
   a. Rapat Koordinasi Berkala, dengan ketentuan:
      1) Diadakan setiap tiga bulan sekali oleh UPA TIK dengan perwakilan unit kerja;
      2) Membahas evaluasi kinerja sistem, infrastruktur jaringan, dan keamanan siber.
   b. Sistem Pelaporan Digital:
      1) Menggunakan platform digital untuk pelaporan masalah teknis, kebutuhan pengembangan, dan insiden keamanan;
      2) Setiap laporan wajib ditanggapi oleh UPA TIK dalam waktu paling lambat 48 jam.
   c. Komunikasi Darurat: Saluran komunikasi khusus untuk menangani insiden yang membutuhkan respons segera.
(4) Dalam hal terjadi insiden keamanan siber, UPA TIK berwenang untuk mengambil tindakan darurat dengan melibatkan unit kerja terkait.

Pasal 23

(1) Rektor UNILA bertanggung jawab atas pengawasan umum terhadap pelaksanaan sistem informasi dan infrastruktur jaringan.
(2) UPA TIK bertanggung jawab melakukan evaluasi rutin terhadap:
   a. Kinerja sistem informasi terintegrasi;
   b. Keandalan dan keamanan infrastruktur jaringan;
   c. Efektivitas kebijakan mitigasi serangan siber.
(3) Unit kerja wajib menerima dan melaksanakan rekomendasi hasil evaluasi yang diberikan oleh UPA TIK.

BAB V

MONITORING DAN EVALUASI BERKALA

Pasal 24

(1) Monitoring pelaksanaan sistem informasi dan infrastruktur jaringan dilakukan oleh UPA TIK melalui:
   a. Pemantauan *real-time* menggunakan perangkat lunak khusus untuk mendeteksi kendala teknis dan ancaman keamanan;
   b. Analisis data performa jaringan dan penggunaan sistem secara berkala.
(2) Monitoring wajib mencakup:
   a. Tingkat keandalan jaringan (*uptime*);
   b. Keamanan data dan sistem informasi;
   c. Kepatuhan unit kerja terhadap kebijakan yang telah ditetapkan.
(3) Hasil monitoring digunakan sebagai dasar untuk evaluasi dan penyusunan rencana pengembangan sistem.

Pasal 25

(1) Evaluasi kinerja sistem dan jaringan dilakukan secara berkala setiap enam bulan oleh UPA TIK.
(2) Evaluasi meliputi:
   a. Kinerja sistem terintegrasi dalam mendukung layanan akademik dan non-akademik;
   b. Keandalan infrastruktur jaringan berdasarkan indikator kecepatan, stabilitas, dan keamanan;
   c. Efektivitas protokol mitigasi serangan siber yang diterapkan.
(3) UPA TIK wajib menyusun laporan evaluasi setiap enam bulan yang mencakup rekomendasi perbaikan dan pengembangan sistem.

BAB VI

SANKSI

Pasal 26

Sanksi diberikan untuk:
   a. Menjamin kepatuhan terhadap kebijakan pengelolaan sistem terintegrasi, infrastruktur jaringan, dan keamanan siber di Unila;
   b. Mencegah terjadinya pelanggaran yang dapat merugikan operasional Unila;
   c. Memberikan efek jera kepada pelaku pelanggaran.

Pasal 27

Pelanggaran terhadap Peraturan Rektor ini dibagi menjadi tiga kategori:
   a. Pelanggaran Ringan, meliputi:
      1) kelalaian dalam menjaga kredensial akses sistem;
      2) penggunaan jaringan untuk aktivitas pribadi yang tidak terkait dengan tugas akademik atau administratif.
   b. Pelanggaran Sedang, meliputi:
      1) Penyalahgunaan data Unila untuk kepentingan pribadi;
      2) Akses tanpa izin ke sistem atau data sensitif.
   c. Pelanggaran Berat, meliputi:
      1) Penyebaran data rahasia Unila tanpa otorisasi;
      2) Peretasan atau upaya sabotase terhadap sistem informasi Unila;
      3) Penggunaan jaringan untuk aktivitas ilegal, seperti penyebaran konten terlarang atau pembajakan perangkat lunak.

Pasal 28

Sanksi bagi sivitas akademika dan tenaga kependidikan terhadap pelanggaran peraturan rektor ini dikenakan sesuai peraturan yang berlaku di Unila.

Pasal 29

(1) Penegakan sanksi dilakukan melalui tahapan berikut:
   a. Identifikasi Pelanggaran: UPA TIK melakukan investigasi awal untuk mengidentifikasi jenis pelanggaran dan pelaku yang terlibat.
   b. Pemberitahuan: Pelaku pelanggaran diberitahukan secara resmi tertulis mengenai dugaan pelanggaran dan diberi kesempatan untuk memberikan klarifikasi dalam waktu 3 (tiga) hari kerja sejak pemberitahuan diterima.
   c. Evaluasi dan Keputusan: Tim Evaluasi yang terdiri dari perwakilan UPA TIK, unit kerja terkait, dan pimpinan Unila menentukan sanksi yang sesuai berdasarkan tingkat pelanggaran.
   d. Pelaksanaan Sanksi: Sanksi dijalankan oleh unit kerja yang bertanggung jawab sesuai keputusan.
(2) Semua proses penegakan sanksi wajib terdokumentasi secara resmi untuk memastikan akuntabilitas.

Pasal 30

(1) Pelaku pelanggaran dapat mengajukan permohonan keringanan sanksi kepada Rektor Unila jika:
   a. Pelanggaran terjadi karena faktor di luar kendali pelaku;
   b. Pelaku telah menunjukkan upaya nyata untuk memperbaiki kesalahan.
(2) Permohonan keringanan sanksi harus diajukan secara tertulis dalam waktu maksimal 7 (tujuh) hari kerja setelah sanksi diberikan.
(3) Rektor UNILA dapat memutuskan:
   a. Mengurangi tingkat sanksi yang diberikan;
   b. Menerima atau menolak banding berdasarkan rekomendasi dari UPA TIK.

BAB VII

PEMBIAYAAN

Pasal 31

(1) Rektor dapat mengalokasikan dana khusus kepada UPA TIK untuk pengelolaan sistem terintegrasi, infrastruktur jaringan, dan keamanan siber Unila.
(2) Dana khusus sebagaimana dimaksud pada ayat (1) dialokasikan untuk:
   a. Pengembangan Sistem Terintegrasi, berupa pengadaan perangkat lunak dan perangkat keras yang mendukung sistem informasi.
   b. Peningkatan Infrastruktur Jaringan:
      1) Pembangunan dan pemeliharaan jaringan kabel dan nirkabel;
      2) Penyediaan pusat data utama dan cadangan.
   c. Keamanan Siber:
      1) Implementasi perangkat keamanan seperti firewall, antivirus, dan enkripsi data;
      2) Penyediaan dana untuk Tim Tanggap Insiden Siber.
   d. Pelatihan dan Sosialisasi:
      1) Program pelatihan keamanan siber untuk staf dan mahasiswa;
      2) Sosialisasi kebijakan terkait penggunaan sistem dan jaringan.

e. Pemeliharaan dan Operasional:
   1) Pemeliharaan perangkat keras dan perangkat lunak secara berkala;
   2) Biaya operasional tim teknis untuk mendukung keberlangsungan layanan.

(3) Prioritas alokasi pembiayaan ditentukan berdasarkan tingkat urgensi kebutuhan operasional.

(4) UPA TIK bertanggung jawab untuk:
   a. Menyusun laporan penggunaan dana setiap triwulan;
   b. Mengajukan revisi anggaran jika terdapat perubahan kebutuhan mendesak.

BAB VIII

KETENTUAN PERALIHAN

Pasal 32

(1) Unit kerja yang belum memenuhi standar sistem terintegrasi, infrastruktur jaringan, dan keamanan siber sesuai dengan peraturan rektor ini diberikan waktu penyesuaian paling lambat 6 (enam) bulan sejak peraturan rektor ini berlaku.

(2) Dalam masa peralihan, UPA TIK bertanggung jawab memberikan:
   a. Panduan teknis kepada unit kerja terkait penerapan sistem baru;
   b. Pelatihan dan pendampingan untuk memastikan kepatuhan terhadap peraturan rektor ini.

BAB IX
KETENTUAN PENUTUP

Pasal 33

Peraturan Rektor ini berlaku sejak tanggal disahkan.
Agar Sivitas Akademika dan Tenaga Kependidikan Unila mengetahuinya, memerintahkan penyebarluasannya dalam Jaringan Dokumentasi dan Informasi Hukum Unila.

Disahkan di Bandar Lampung
Pada tanggal 09 April 2026
REKTOR,

TTD

LUSMEILIA AFRIANI

Salinan sesuai dengan aslinya,
Kepala Biro Keuangan, Kepegawaian dan Umum
Universitas Lampung,

Indrayati Putri Idrus, S.H., M.H.