

LAPORAN
TAHUNAN MANUAL PENGGUNAAN DAN KEAMANAN
TEKNOLOGI INFORMASI (TI)



PROGRAM STUDI PENDIDIKAN AGAMA ISLAM
FAKULTAS AGAMA ISLAM
UNIVERSITAS MUHAMMADIYAH PAREPARE
TAHUN 2025

I. Pendahuluan

Pengelolaan sarana dan prasarana merupakan salah satu aspek strategis yang memiliki peran sangat penting dalam menunjang penyelenggaraan tridharma perguruan tinggi, yaitu pendidikan dan pengajaran, penelitian, serta pengabdian kepada masyarakat. Sarana dan prasarana yang memadai, layak, aman, serta berfungsi secara optimal menjadi prasyarat utama dalam menciptakan lingkungan akademik yang kondusif, efektif, dan berkelanjutan. Dengan kondisi fasilitas yang baik, proses pembelajaran dapat berlangsung dengan lebih nyaman, aktivitas penelitian dapat didukung oleh fasilitas yang relevan, serta pelaksanaan pengabdian kepada masyarakat dapat dilakukan secara lebih profesional dan berdampak luas.

Ketersediaan sarana dan prasarana tidak hanya berorientasi pada kuantitas, tetapi juga kualitas, pemeliharaan, dan keberlanjutan pemanfaatannya. Oleh karena itu, pengelolaan aset kampus harus dilakukan secara sistematis melalui perencanaan, pemeliharaan, pengawasan, serta evaluasi secara berkala. Upaya ini diperlukan agar seluruh fasilitas yang dimiliki universitas dapat berfungsi sesuai standar, memiliki masa pakai yang optimal, serta mampu memenuhi kebutuhan sivitas akademika yang terus berkembang seiring dengan dinamika perkembangan ilmu pengetahuan, teknologi, dan perubahan lingkungan pendidikan tinggi.

Dalam konteks Universitas Muhammadiyah Parepare, pengelolaan sarana dan prasarana menjadi bagian integral dari upaya peningkatan kualitas layanan pendidikan tinggi. Universitas terus berupaya mengembangkan fasilitas yang mendukung proses akademik dan non-akademik, mulai dari ruang kuliah, laboratorium, perpustakaan, fasilitas olahraga, hingga infrastruktur penunjang lainnya. Upaya ini dilaksanakan dengan memperhatikan prinsip efisiensi, efektivitas, dan keberlanjutan, serta mengacu pada standar nasional maupun internasional yang relevan. Hal ini sejalan dengan visi dan misi universitas untuk mewujudkan lembaga pendidikan yang unggul, inovatif, dan berdaya saing.

Laporan Tahunan Sarana dan Prasarana Utama Universitas Muhammadiyah Parepare Tahun 2025 disusun sebagai bentuk pertanggungjawaban institusional terhadap seluruh pemangku kepentingan, baik internal maupun eksternal. Laporan ini merupakan dokumentasi resmi yang menyajikan gambaran menyeluruh mengenai kondisi fisik, tingkat kelayakan, serta pemanfaatan sarana dan prasarana yang dimiliki universitas pada tahun 2025. Penyusunan laporan ini didasarkan pada kebutuhan untuk memastikan bahwa pengelolaan aset kampus dilakukan secara transparan, akuntabel, dan berorientasi pada peningkatan kualitas layanan pendidikan tinggi.

Laporan ini disusun untuk memberikan informasi yang terperinci, objektif, dan sistematis mengenai kondisi aktual fasilitas kampus. Informasi yang disajikan meliputi hasil

inspeksi rutin, penilaian kondisi fisik, tingkat kelayakan, serta tingkat pemanfaatan sarana dan prasarana. Dengan demikian, laporan ini diharapkan dapat menjadi sumber data yang dapat dipercaya dalam melakukan perencanaan pemeliharaan, perbaikan, dan pengembangan fasilitas.

Laporan ini memiliki manfaat strategis sebagai dasar dalam perencanaan pengembangan sarana dan prasarana pada periode berikutnya. Dengan data dan informasi yang terstruktur, universitas dapat merumuskan program pemeliharaan, perbaikan, serta pengembangan fasilitas yang lebih terarah, efektif, dan sesuai dengan standar yang berlaku. Selain itu, laporan ini juga dapat digunakan sebagai alat monitoring dan evaluasi dalam rangka meningkatkan efisiensi pengelolaan aset, mengurangi risiko kerusakan, serta meningkatkan keamanan dan kenyamanan lingkungan kampus.

Penyusunan laporan ini dilandasi oleh komitmen Universitas Muhammadiyah Parepare dalam meningkatkan mutu layanan pendidikan tinggi secara berkelanjutan. Komitmen tersebut tercermin dalam upaya menjaga dan meningkatkan kualitas fasilitas kampus agar selalu siap mendukung kebutuhan akademik sivitas. Selain itu, laporan ini juga sejalan dengan prinsip tata kelola perguruan tinggi yang baik, yaitu transparansi, akuntabilitas, responsibilitas, independensi, dan kesetaraan. Dengan adanya laporan ini, universitas berharap dapat memastikan bahwa pengelolaan sarana dan prasarana dilaksanakan secara profesional dan berorientasi pada hasil yang berkelanjutan.

Dengan demikian, Laporan Tahunan Sarana dan Prasarana Utama Universitas Muhammadiyah Parepare Tahun 2025 diharapkan menjadi dokumen yang bermanfaat sebagai acuan dalam meningkatkan kualitas pengelolaan fasilitas kampus. Laporan ini diharapkan mampu mendukung upaya universitas dalam menciptakan lingkungan akademik yang lebih baik, aman, dan produktif, serta mendukung pencapaian visi dan misi institusi secara keseluruhan.

II. Panduan Penggunaan Perangkat TI

Penggunaan perangkat teknologi informasi (TI) di lingkungan Universitas Muhammadiyah Parepare mencakup pemanfaatan berbagai perangkat keras yang menjadi bagian penting dari infrastruktur akademik dan administratif. Perangkat keras tersebut meliputi komputer desktop, laptop, server, perangkat jaringan (seperti router, switch, access point), perangkat pendukung seperti printer, scanner, serta perangkat lainnya yang digunakan untuk mendukung aktivitas operasional kampus. Secara umum, perangkat TI yang tersedia dirancang dan disediakan untuk mendukung pelaksanaan kegiatan akademik, administrasi, penelitian,

serta layanan umum kampus yang bertujuan meningkatkan efisiensi, produktivitas, dan kualitas layanan institusi.

Sehubungan dengan fungsi strategis perangkat TI dalam mendukung kegiatan institusi, penggunaan perangkat harus dilakukan secara bertanggung jawab, terarah, dan selaras dengan tujuan Universitas. Pengguna yang berwenang diharapkan memanfaatkan perangkat sesuai dengan peran dan tanggung jawab masing-masing, serta memastikan bahwa penggunaan perangkat tidak mengganggu kinerja sistem secara keseluruhan. Hal ini mencakup pengelolaan waktu penggunaan perangkat, penggunaan aplikasi yang sesuai kebutuhan, serta menjaga ketertiban dalam pemanfaatan fasilitas TI agar tidak menimbulkan hambatan bagi pengguna lain.

Dalam rangka menjaga kondisi fisik perangkat dan keberlangsungan fungsi operasionalnya, pengguna wajib melakukan pemeliharaan sederhana secara berkala, seperti menjaga kebersihan perangkat, menghindari tindakan yang dapat menyebabkan kerusakan, serta meminimalkan penggunaan perangkat dalam kondisi yang berisiko tinggi (misalnya lingkungan yang lembap, panas berlebih, atau berdebu). Pengguna juga diharapkan menghindari tindakan yang dapat merusak atau mengganggu kinerja perangkat, seperti memindahkan perangkat secara sembarangan, membuka casing perangkat tanpa izin, memasang perangkat tambahan tanpa persetujuan, atau melakukan instalasi perangkat lunak yang tidak sesuai ketentuan.

Keamanan data dan akun merupakan aspek penting dalam pemanfaatan perangkat TI. Oleh karena itu, seluruh pengguna diwajibkan menjaga kerahasiaan akun dan data pribadi, serta tidak membagikan informasi login kepada pihak lain. Pengguna juga diharapkan melakukan pengelolaan kata sandi yang baik, misalnya menggunakan kombinasi yang kuat, mengganti kata sandi secara berkala, serta tidak menggunakan kata sandi yang sama untuk akun pribadi dan akun institusi. Selain itu, pengguna wajib melaporkan segera kepada pihak yang berwenang apabila menemukan indikasi pelanggaran keamanan, seperti adanya akses tidak sah, kehilangan perangkat, atau dugaan pencurian data.

Penggunaan perangkat untuk aktivitas yang melanggar aturan, seperti penyalahgunaan akses data, aktivitas ilegal, atau tindakan yang merugikan pihak lain, harus dihindari. Pelanggaran tersebut tidak hanya dapat menimbulkan risiko hukum bagi individu yang melakukan tindakan tersebut, tetapi juga dapat merusak reputasi institusi serta mengganggu kelancaran layanan kampus. Oleh karena itu, pengguna wajib mematuhi ketentuan dan regulasi yang berlaku serta mengikuti prinsip etika dalam pemanfaatan teknologi informasi.

Dalam hal pemanfaatan layanan TI berbasis aplikasi, pengguna juga diharapkan mengikuti prosedur yang telah ditetapkan oleh universitas. Hal ini mencakup penggunaan akun resmi universitas, menjaga kerahasiaan data akademik, serta mematuhi ketentuan penggunaan platform pembelajaran dan sistem informasi akademik. Penggunaan layanan digital untuk pelaksanaan kegiatan pembelajaran daring, pengumpulan tugas, serta komunikasi akademik harus dilakukan secara tertib, profesional, dan sesuai dengan norma akademik. Pengguna juga diharapkan menghindari penyebaran informasi yang tidak benar, konten yang tidak pantas, atau tindakan yang dapat menimbulkan konflik dalam lingkungan akademik.

Seluruh aktivitas pemanfaatan teknologi informasi di lingkungan Universitas Muhammadiyah Parepare harus dilaksanakan dengan tetap memperhatikan etika penggunaan teknologi, keamanan data, serta tanggung jawab sosial. Dengan demikian, penggunaan perangkat TI dapat memberikan manfaat optimal bagi sivitas akademika, mendukung terciptanya proses pembelajaran yang efektif, layanan administrasi yang efisien, serta peningkatan kualitas penelitian dan pengabdian kepada masyarakat.

III. Praktik Keamanan TI

Keamanan teknologi informasi (TI) menjadi aspek yang sangat krusial dalam menghadapi tantangan digital yang semakin kompleks di lingkungan perguruan tinggi. Perkembangan teknologi yang pesat membawa banyak kemudahan dalam pelaksanaan kegiatan akademik, administrasi, penelitian, dan layanan umum kampus. Namun, perkembangan tersebut juga menimbulkan risiko baru berupa ancaman siber yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data serta sistem informasi. Ancaman seperti malware, phishing, kebocoran data, serangan jaringan, dan tindakan akses tidak sah menjadi tantangan utama yang perlu diantisipasi secara serius. Jika tidak ditangani dengan baik, ancaman tersebut dapat berdampak signifikan terhadap kelancaran layanan akademik dan administratif, menurunkan kepercayaan sivitas akademika, serta merusak reputasi institusi.

Dalam rangka menjaga keamanan lingkungan digital, Universitas Muhammadiyah Parepare menetapkan praktik keamanan TI yang wajib dipatuhi oleh seluruh sivitas akademika. Praktik ini dirancang untuk membangun budaya keamanan siber yang kuat dan berkelanjutan, serta mengurangi risiko yang timbul dari penggunaan teknologi informasi dalam aktivitas sehari-hari. Implementasi praktik keamanan ini tidak hanya menjadi tanggung jawab unit TI, tetapi juga melibatkan peran aktif seluruh pengguna dalam menjaga keamanan sistem dan data institusi.

Praktik keamanan yang harus diikuti meliputi penggunaan kata sandi yang kuat dan tidak mudah ditebak. Kata sandi yang baik sebaiknya memiliki kombinasi huruf besar dan

kecil, angka, serta karakter khusus, serta tidak menggunakan informasi pribadi yang mudah diketahui. Selain itu, pengguna wajib menjaga kerahasiaan akun dan tidak membagikan informasi login kepada pihak lain. Untuk meningkatkan tingkat keamanan, pengguna juga diwajibkan melakukan perubahan kata sandi secara berkala sesuai ketentuan yang berlaku. Penggunaan kata sandi yang sama untuk beberapa akun, terutama antara akun pribadi dan akun institusi, sangat tidak dianjurkan karena meningkatkan risiko kebocoran data apabila salah satu akun terkena serangan.

Selain itu, pengguna juga diharapkan mengaktifkan mekanisme keamanan tambahan seperti autentikasi dua faktor (two-factor authentication/2FA) apabila tersedia pada layanan yang digunakan. Autentikasi dua faktor dapat meningkatkan lapisan keamanan dengan memerlukan verifikasi tambahan selain kata sandi, sehingga meminimalkan risiko akses tidak sah meskipun kata sandi telah bocor. Pengguna juga harus menghindari penggunaan perangkat pribadi untuk mengakses data penting tanpa proteksi yang memadai, seperti perangkat yang tidak memiliki sistem keamanan terbaru atau perangkat yang digunakan secara umum oleh banyak orang.

Perangkat yang digunakan untuk mengakses jaringan kampus harus memiliki perlindungan dasar yang memadai. Hal ini mencakup pemasangan perangkat lunak antivirus, firewall, serta memastikan sistem operasi dan aplikasi selalu diperbarui secara berkala. Pembaruan sistem (update) penting untuk menutup celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pengguna juga harus berhati-hati dalam mengunduh atau membuka lampiran yang mencurigakan, serta tidak mengakses tautan yang tidak jelas sumbernya. Praktik ini penting untuk mencegah penyebaran malware, ransomware, atau serangan phishing yang sering terjadi melalui email atau pesan tidak resmi.

Apabila terdapat indikasi ancaman atau aktivitas mencurigakan, pengguna wajib melaporkan kepada unit TI terkait untuk segera dilakukan penanganan. Laporan dapat mencakup indikasi seperti adanya notifikasi login dari lokasi tidak dikenal, munculnya pesan error yang tidak biasa, perubahan file tanpa sepengetahuan pengguna, atau perangkat yang tiba-tiba menjadi lambat dan tidak responsif. Penanganan cepat terhadap indikasi ancaman dapat mengurangi dampak kerugian dan mempercepat proses pemulihan sistem.

Selain perlindungan terhadap ancaman siber, praktik keamanan juga mencakup pengelolaan data dan dokumen digital. Pengguna diharapkan menyimpan data pada media yang aman dan sesuai prosedur, seperti menggunakan penyimpanan resmi yang telah disediakan oleh universitas. Pengelolaan data yang baik juga meliputi pembatasan akses hanya kepada pihak yang berwenang, serta memastikan data sensitif tidak disebarluaskan secara tidak sah. Untuk

mengantisipasi risiko kehilangan data, pengguna juga diwajibkan melakukan backup secara berkala. Backup data penting dilakukan untuk menjaga ketersediaan informasi jika terjadi kegagalan sistem, kerusakan perangkat, atau serangan siber.

Penggunaan layanan cloud dan penyimpanan data harus mengikuti ketentuan yang ditetapkan oleh universitas. Hal ini bertujuan untuk memastikan bahwa data institusi tetap terlindungi dan dapat dipertanggungjawabkan. Layanan cloud yang digunakan sebaiknya merupakan layanan resmi yang telah terverifikasi dan memenuhi standar keamanan. Pengguna juga harus memperhatikan aspek legalitas dan kepatuhan terhadap peraturan terkait perlindungan data. Dengan demikian, penggunaan teknologi informasi di lingkungan Universitas Muhammadiyah Parepare dapat berjalan dengan aman, tertib, dan mendukung terciptanya lingkungan akademik yang produktif dan terpercaya.

IV. Prosedur Operasional Standar (SOP) Penggunaan TI

Dalam rangka memastikan bahwa pemanfaatan teknologi informasi di lingkungan Universitas Muhammadiyah Parepare berjalan secara teratur, terkontrol, serta sesuai dengan tujuan institusi, universitas menetapkan prosedur operasional standar (SOP) yang menjadi acuan bagi seluruh pengguna dalam memanfaatkan layanan teknologi informasi. SOP ini dirancang sebagai pedoman operasional yang sistematis dan jelas, sehingga setiap pengguna dapat memahami tata cara penggunaan perangkat, akses layanan, serta mekanisme pelaporan dan koordinasi apabila terjadi kendala atau kebutuhan layanan TI.

SOP penggunaan TI mencakup berbagai aspek penting yang terkait dengan pemanfaatan teknologi informasi, mulai dari penggunaan perangkat, akses layanan, pengelolaan akun, hingga penanganan permasalahan teknis. Setiap pengguna diharapkan memahami dan mengikuti prosedur yang ditetapkan agar pemanfaatan layanan TI dapat berjalan efektif dan efisien. Selain itu, SOP ini juga menjadi landasan dalam memastikan bahwa penggunaan TI dilakukan dengan prinsip akuntabilitas, keamanan, dan kepatuhan terhadap ketentuan yang berlaku.

Salah satu fokus utama dalam SOP ini adalah penekanan pada kepatuhan terhadap kebijakan dan aturan yang berlaku. Pengguna diwajibkan menjaga integritas data, memastikan keakuratan informasi, serta tidak melakukan tindakan yang dapat mengubah, merusak, atau memanipulasi data tanpa wewenang. Selain itu, pengguna juga wajib menghormati hak kekayaan intelektual, termasuk hak cipta, lisensi perangkat lunak, serta hak atas karya akademik yang dibuat oleh sivitas akademika. Penggunaan konten digital yang dilindungi hak cipta harus dilakukan sesuai ketentuan, dan pengguna wajib menghindari tindakan pembajakan atau penggunaan materi tanpa izin.

Pengguna juga wajib mematuhi ketentuan penggunaan sistem informasi akademik dan aplikasi internal universitas. Hal ini mencakup penggunaan akun resmi, menjaga kerahasiaan data akademik, serta mengikuti prosedur yang berlaku dalam pengelolaan administrasi akademik melalui sistem digital. Setiap aktivitas yang dilakukan dalam lingkungan digital kampus harus selaras dengan ketentuan hukum dan etika yang berlaku, sehingga dapat menjaga reputasi universitas serta menciptakan lingkungan akademik yang sehat dan profesional.

Dalam hal penggunaan fasilitas jaringan, pengguna diwajibkan menggunakan jaringan kampus sesuai dengan aturan yang ditetapkan. Penggunaan jaringan harus dilakukan secara wajar dan proporsional, sehingga tidak membebani jaringan secara berlebihan yang dapat mengganggu kualitas layanan bagi pengguna lain. Pengguna juga tidak diperkenankan melakukan tindakan yang dapat merusak atau mengganggu layanan jaringan, seperti melakukan akses tidak sah, mengganggu koneksi, atau mengoperasikan perangkat yang dapat menyebabkan gangguan jaringan. Aktivitas yang tidak terkait dengan kepentingan akademik atau administratif, terutama yang bersifat ilegal atau merugikan pihak lain, harus dihindari.

Penggunaan jaringan untuk kegiatan yang dapat menimbulkan risiko keamanan, seperti penggunaan aplikasi berbagi file yang tidak sah, penyebaran konten negatif, atau penggunaan layanan yang melanggar hukum, juga tidak diperbolehkan. Pengguna diharapkan memanfaatkan jaringan kampus untuk tujuan yang mendukung proses pembelajaran, penelitian, dan layanan administrasi, serta menjaga etika dalam berkomunikasi dan berbagi informasi melalui media digital. Dengan demikian, penggunaan fasilitas jaringan dapat berjalan aman, tertib, dan mendukung terciptanya lingkungan akademik yang produktif dan terpercaya.

SOP ini juga menegaskan mekanisme pelaporan dan koordinasi apabila terjadi masalah teknis atau kebutuhan layanan TI. Pengguna diwajibkan melaporkan kendala melalui saluran resmi yang telah disediakan, sehingga unit TI dapat melakukan penanganan dengan cepat dan tepat. Pelaporan harus disertai informasi yang jelas mengenai jenis kendala, perangkat yang digunakan, serta waktu kejadian. Unit TI kemudian akan melakukan verifikasi, penanganan, dan tindak lanjut sesuai prosedur yang berlaku. Dengan adanya SOP ini, diharapkan pengelolaan layanan TI dapat berjalan lebih terstruktur, responsif, dan berkelanjutan, serta mampu mendukung kebutuhan sivitas akademika secara optimal.

V. Protokol Penanganan Masalah Teknis

Meskipun telah diterapkan berbagai langkah pencegahan dan penguatan sistem, masalah teknis tetap berpotensi terjadi dalam pemanfaatan layanan teknologi informasi (TI). Hal ini dapat disebabkan oleh berbagai faktor, seperti gangguan jaringan, kerusakan perangkat

keras, kegagalan perangkat lunak, maupun kesalahan operasional pengguna. Mengingat layanan TI merupakan bagian penting dalam mendukung aktivitas akademik, administrasi, penelitian, dan layanan umum kampus, penanganan masalah teknis harus dilakukan secara cepat, tepat, dan terstruktur agar dampak gangguan dapat diminimalkan.

Dalam rangka memastikan respons yang terarah, universitas menetapkan protokol penanganan masalah teknis sebagai panduan bagi pengguna dan unit TI dalam menyelesaikan kendala yang muncul. Protokol ini disusun untuk memastikan bahwa setiap masalah ditangani secara sistematis, mulai dari tahap identifikasi, pelaporan, diagnosis, hingga penyelesaian dan tindak lanjut. Dengan adanya protokol ini, universitas dapat menjaga kontinuitas layanan TI, meningkatkan kepuasan pengguna, serta mengurangi risiko gangguan yang berulang.

Protokol penanganan masalah teknis mencakup tahap awal identifikasi masalah, di mana pengguna diminta untuk melakukan pemantauan awal terhadap kendala yang dialami. Identifikasi ini mencakup pemahaman terhadap gejala masalah, seperti apakah masalah terjadi pada perangkat, aplikasi, jaringan, atau akun pengguna. Selain itu, pengguna juga diharapkan melakukan langkah-langkah awal yang sederhana, seperti memastikan koneksi jaringan stabil, melakukan restart perangkat, atau memeriksa konfigurasi dasar sebelum melaporkan masalah. Namun, apabila kendala tetap berlanjut, pengguna diwajibkan melaporkan masalah tersebut melalui kanal resmi yang telah disediakan oleh universitas.

Pelaporan masalah harus dilakukan dengan memberikan informasi yang jelas dan lengkap mengenai kendala yang dialami. Informasi yang diperlukan antara lain jenis perangkat yang digunakan, deskripsi masalah secara rinci, waktu kejadian, serta langkah-langkah yang telah dilakukan sebelumnya. Pengguna juga dapat melampirkan bukti pendukung seperti tangkapan layar (screenshot) atau rekaman video singkat untuk memperjelas permasalahan. Informasi yang lengkap sangat membantu tim TI dalam melakukan diagnosis lebih efektif dan menentukan langkah penanganan yang sesuai.

Setelah laporan diterima, tim TI akan melakukan koordinasi dan verifikasi untuk menentukan penyebab masalah. Proses diagnosis dilakukan berdasarkan informasi yang diberikan serta hasil pemantauan sistem yang relevan. Tim TI kemudian akan melakukan tindakan perbaikan yang diperlukan, seperti pembaruan sistem, perbaikan perangkat keras, konfigurasi ulang aplikasi, atau pemulihan akses layanan. Penanganan ini dilakukan dengan memperhatikan prioritas dan tingkat dampak terhadap layanan, sehingga masalah yang berdampak besar dapat ditangani dengan segera.

Selain penanganan langsung, protokol ini juga mencakup langkah pemulihan akses layanan serta tindakan pencegahan agar masalah serupa tidak terjadi kembali. Tindakan

pencegahan dapat berupa perbaikan sistem, peningkatan kapasitas jaringan, pembaruan kebijakan keamanan, atau pemberian edukasi kepada pengguna terkait penggunaan layanan yang benar. Unit TI juga bertanggung jawab melakukan pemantauan terhadap kinerja layanan secara berkala, termasuk melakukan pemeliharaan rutin, pemantauan keamanan, serta pengujian sistem untuk memastikan stabilitas operasional.

Sebagai bagian dari tanggung jawab institusi, unit TI juga wajib melakukan dokumentasi penanganan masalah. Dokumentasi ini meliputi catatan kronologi masalah, langkah penanganan yang dilakukan, serta hasil akhir penyelesaian. Dokumentasi ini penting untuk keperluan evaluasi internal, peningkatan layanan, serta sebagai referensi dalam menangani permasalahan serupa di masa mendatang. Dengan adanya protokol penanganan masalah teknis yang jelas dan terstruktur, diharapkan layanan TI di Universitas Muhammadiyah Parepare dapat berjalan lebih handal, responsif, dan mendukung kebutuhan sivitas akademika secara optimal.

VI. Evaluasi dan Pengembangan Layanan TI Tahun 2025

Selama Tahun 2025, implementasi manual penggunaan dan keamanan teknologi informasi (TI) di Universitas Muhammadiyah Parepare telah dilaksanakan melalui serangkaian kegiatan yang terstruktur dan berkelanjutan. Pelaksanaan manual ini mencakup kegiatan sosialisasi kebijakan penggunaan TI kepada sivitas akademika, pelatihan penggunaan aplikasi dan sistem informasi internal, serta pemantauan dan pengawasan penggunaan jaringan dan layanan digital. Sosialisasi dilakukan untuk memastikan bahwa seluruh pengguna memahami aturan, prosedur, serta konsekuensi dari pelanggaran kebijakan TI. Pelatihan dilaksanakan guna meningkatkan kemampuan pengguna dalam memanfaatkan aplikasi pembelajaran, sistem informasi akademik, serta layanan administrasi secara efektif. Selain itu, pemantauan dilakukan untuk memastikan bahwa penggunaan layanan TI sesuai dengan ketentuan, serta untuk mengidentifikasi potensi masalah teknis atau pelanggaran keamanan yang perlu segera ditangani.

Evaluasi terhadap pelaksanaan manual ini dilakukan dengan menggunakan beberapa indikator penilaian yang relevan, antara lain tingkat kepatuhan pengguna terhadap kebijakan, frekuensi insiden keamanan yang terjadi, serta kualitas layanan TI berdasarkan umpan balik dari pengguna. Penilaian tingkat kepatuhan dilakukan melalui observasi, monitoring, dan laporan pelanggaran yang tercatat selama periode pelaksanaan. Sedangkan evaluasi frekuensi insiden keamanan meliputi pencatatan kejadian seperti upaya akses tidak sah, serangan phishing, malware, atau pelanggaran penggunaan data yang terdeteksi oleh sistem keamanan.

Sementara itu, kualitas layanan TI dinilai melalui survei kepuasan pengguna, tingkat kelancaran akses aplikasi, serta waktu respons penanganan kendala oleh unit TI.

Secara umum, hasil evaluasi menunjukkan bahwa pemanfaatan layanan TI di lingkungan kampus berjalan relatif baik dan stabil, dengan tingkat kepatuhan yang cukup tinggi dari sivitas akademika. Hal ini menunjukkan bahwa sosialisasi dan pelatihan yang dilaksanakan mampu meningkatkan kesadaran pengguna terhadap pentingnya penggunaan TI yang benar dan aman. Selain itu, kualitas layanan TI dinilai cukup memadai untuk mendukung kegiatan akademik dan administratif, meskipun masih terdapat beberapa kendala teknis yang perlu diperbaiki. Evaluasi ini juga menunjukkan bahwa unit TI telah mampu menjalankan peran operasionalnya secara konsisten dalam memberikan dukungan layanan, penanganan masalah, serta pemeliharaan sistem secara rutin.

Namun demikian, evaluasi juga mengungkapkan adanya beberapa area yang perlu mendapatkan perhatian lebih dalam pengembangan selanjutnya. Pertama, peningkatan literasi digital menjadi kebutuhan yang mendesak, terutama untuk meningkatkan pemahaman pengguna terhadap praktik keamanan siber, penggunaan aplikasi yang benar, serta kemampuan dasar dalam mengelola data digital. Kedua, penguatan mekanisme autentikasi, seperti implementasi autentikasi dua faktor (2FA) pada layanan penting, perlu diperkuat untuk mengurangi risiko akses tidak sah. Ketiga, peningkatan kesadaran pengguna terhadap praktik keamanan, seperti pengelolaan kata sandi, kewaspadaan terhadap phishing, serta kebiasaan backup data, masih perlu terus ditingkatkan melalui program edukasi dan kampanye keamanan yang lebih intensif.

Selain itu, evaluasi juga menunjukkan adanya kebutuhan peningkatan kapasitas jaringan dan peningkatan kualitas layanan aplikasi agar dapat mendukung kebutuhan akademik yang terus berkembang. Perkembangan aktivitas akademik yang semakin digital, seperti pembelajaran daring, penggunaan platform kolaborasi, serta akses sistem informasi akademik secara masif, menuntut kapasitas jaringan yang lebih besar dan stabil. Demikian pula, kualitas layanan aplikasi perlu ditingkatkan agar mampu memberikan pengalaman pengguna yang lebih baik, termasuk aspek kecepatan akses, stabilitas sistem, serta ketersediaan fitur yang relevan dengan kebutuhan akademik.

Sebagai tindak lanjut dari hasil evaluasi, universitas perlu mengembangkan program pelatihan keamanan TI secara berkala yang ditujukan untuk seluruh sivitas akademika. Program ini dapat mencakup materi dasar keamanan siber, praktik aman dalam penggunaan internet, pengelolaan data, serta simulasi penanganan insiden. Selain itu, universitas juga perlu meningkatkan koordinasi antarunit dalam pengelolaan layanan digital, sehingga kebijakan,

prosedur, dan implementasi operasional dapat berjalan selaras dan terintegrasi. Penguatan infrastruktur jaringan dan sistem informasi juga menjadi langkah strategis yang perlu dilakukan untuk mendukung kebutuhan layanan yang terus meningkat.

Pengembangan kebijakan dan pedoman penggunaan TI juga harus disesuaikan dengan perkembangan teknologi dan ancaman siber yang terus berubah. Oleh karena itu, universitas perlu melakukan evaluasi dan revisi kebijakan secara berkala agar tetap relevan dan efektif dalam menjaga keamanan serta kenyamanan pengguna. Dengan demikian, pengelolaan penggunaan dan keamanan TI dapat berjalan secara berkelanjutan, mendukung terciptanya lingkungan akademik yang aman, produktif, dan terpercaya.

VII. Penutup

Dengan tersusunnya Manual Penggunaan dan Keamanan Teknologi Informasi (TI), Universitas Muhammadiyah Parepare diharapkan mampu menciptakan lingkungan penggunaan teknologi yang lebih aman, efektif, dan terkelola secara profesional. Manual ini menjadi pedoman resmi yang mengatur tata kelola penggunaan perangkat, akses layanan, serta praktik keamanan dalam pemanfaatan layanan TI di lingkungan kampus. Dengan adanya pedoman yang jelas, seluruh sivitas akademika memiliki acuan yang sama dalam menjalankan aktivitas digital, sehingga penggunaan teknologi dapat berjalan secara konsisten, tertib, dan sesuai dengan standar yang ditetapkan.

Manual ini juga berperan sebagai instrumen penjaminan mutu dalam pengelolaan layanan teknologi informasi. Melalui pedoman ini, universitas dapat memastikan bahwa pemanfaatan TI dilakukan dengan prinsip akuntabilitas, transparansi, dan kepatuhan terhadap aturan yang berlaku. Selain itu, manual ini juga menjadi dasar dalam evaluasi dan pengembangan layanan TI secara berkelanjutan, karena pedoman ini memberikan kerangka kerja yang dapat digunakan untuk mengukur efektivitas penggunaan, tingkat keamanan, serta kualitas layanan yang disediakan.

Keberlanjutan pengembangan TI di universitas sangat bergantung pada komitmen seluruh pihak dalam menerapkan praktik keamanan yang baik dan konsisten. Dengan mengintegrasikan prinsip-prinsip keamanan dalam setiap aspek penggunaan teknologi, universitas dapat meminimalkan risiko ancaman siber, menjaga integritas data, serta memastikan ketersediaan layanan yang stabil. Praktik keamanan yang baik juga akan meningkatkan kepercayaan pengguna terhadap sistem dan layanan digital, sehingga proses akademik dan administrasi dapat berjalan lebih lancar dan produktif.

Lebih lanjut, keberhasilan implementasi manual ini juga akan berdampak pada peningkatan kualitas layanan akademik dan administrasi. Dengan sistem yang aman dan

terkelola, kegiatan pembelajaran, penelitian, dan pelayanan administrasi dapat dilakukan dengan lebih efisien dan efektif. Selain itu, penggunaan TI yang baik akan mendukung inovasi dalam proses pembelajaran dan pengembangan sistem informasi yang lebih adaptif terhadap kebutuhan pengguna. Dengan demikian, universitas dapat meningkatkan daya saing institusi serta memperkuat posisi sebagai perguruan tinggi yang unggul dan inovatif.

Akhirnya, Manual Penggunaan dan Keamanan TI ini diharapkan menjadi bagian integral dalam upaya Universitas Muhammadiyah Parepare mewujudkan visi dan misi institusi. Dengan dukungan infrastruktur TI yang handal, kebijakan yang jelas, serta budaya keamanan yang kuat, universitas dapat memperkuat fondasi pengelolaan pendidikan tinggi yang berkualitas. Semoga pedoman ini dapat menjadi landasan bagi seluruh sivitas akademika dalam memanfaatkan teknologi secara bertanggung jawab, serta menjadi dasar bagi pengembangan layanan TI yang lebih baik di masa mendatang.

Parepare, 12 November 2025



Dr. Sumadin, S.Pd.I., M.Pd.I.

NBM : 1037444