SOP Instalasi dan Update Sistem

Kategori: IT & Sistem

No. Dokumen: SOP-0059

Tanggal Terbit: 20/04/2026

Sumber: GajiHub SOP — sop.gajihub.com

Prosedur standar untuk instalasi dan pembaruan sistem TI perusahaan secara aman, terkontrol, dan terdokumentasi.

Tujuan

SOP ini disusun untuk memastikan bahwa seluruh proses instalasi dan pembaruan (update) sistem teknologi informasi di lingkungan perusahaan dilaksanakan secara terstruktur, aman, terdokumentasi, dan sesuai dengan standar operasional serta regulasi yang berlaku di Indonesia. Dengan adanya SOP ini, diharapkan risiko gangguan operasional, kerusakan sistem, kehilangan data, maupun celah keamanan dapat diminimalkan. Selain itu, SOP ini bertujuan untuk menciptakan konsistensi dalam pelaksanaan pekerjaan oleh tim IT, meningkatkan akuntabilitas, serta mendukung keberlangsungan bisnis perusahaan melalui pengelolaan sistem yang andal dan efisien.

Ruang Lingkup

SOP ini berlaku untuk seluruh aktivitas instalasi sistem baru maupun pembaruan sistem yang sudah berjalan, termasuk perangkat lunak (software), sistem operasi, aplikasi bisnis, serta patch keamanan di seluruh infrastruktur TI perusahaan. Ruang lingkup mencakup server, komputer pengguna, perangkat jaringan, serta sistem berbasis cloud yang digunakan oleh perusahaan. SOP ini juga mengatur peran dan tanggung jawab tim IT, manajemen, serta pengguna akhir dalam mendukung kelancaran proses instalasi dan update sistem. Seluruh unit kerja yang menggunakan sistem TI wajib mematuhi prosedur ini untuk menjaga stabilitas dan keamanan operasional.

Definisi

Istilah	Definisi
Instalasi Sistem	Proses pemasangan dan konfigurasi awal perangkat lunak atau sistem pada perangkat keras agar dapat digunakan sesuai kebutuhan operasional.
Update Sistem	Proses pembaruan perangkat lunak untuk meningkatkan fitur, memperbaiki bug, atau menutup celah keamanan.

Istilah	Definisi
Patch	Perbaikan kecil pada perangkat lunak yang dirilis untuk mengatasi masalah tertentu atau meningkatkan keamanan.
Backup Data	Proses pencadangan data untuk mencegah kehilangan informasi penting akibat kegagalan sistem atau kesalahan operasional.
Downtime	Periode waktu ketika sistem tidak dapat digunakan karena proses instalasi, update, atau gangguan teknis.

Tanggung Jawab

Pihak	Tanggung Jawab
Manajer IT	Menyetujui rencana instalasi dan update sistem, memastikan kesesuaian dengan kebijakan perusahaan, serta mengawasi pelaksanaan SOP.
Tim IT Infrastruktur	Melaksanakan proses instalasi dan update sistem, melakukan pengujian, serta memastikan sistem berjalan dengan baik setelah implementasi.
Tim Keamanan Informasi	Melakukan evaluasi risiko keamanan sebelum dan sesudah instalasi atau update serta memastikan tidak ada celah keamanan.
User/Pengguna	Memberikan persetujuan jadwal downtime dan melaporkan kendala yang terjadi setelah sistem diperbarui.
Quality Assurance IT	Melakukan pengujian sistem dan verifikasi bahwa sistem berfungsi sesuai standar sebelum digunakan secara penuh.

Prosedur

Tahap 1: Perencanaan Instalasi dan Update

Tahap ini bertujuan untuk memastikan bahwa seluruh proses instalasi dan update direncanakan secara matang, termasuk analisis kebutuhan dan risiko.

1. Mengidentifikasi kebutuhan instalasi atau update berdasarkan permintaan bisnis atau rekomendasi keamanan.
2. Melakukan analisis dampak terhadap sistem yang sedang berjalan, termasuk potensi downtime.
3. Menyusun rencana kerja lengkap beserta jadwal pelaksanaan dan kebutuhan sumber daya.

Penanggung Jawab: Manajer IT dan Tim IT Infrastruktur

Tahap 2: Persiapan Teknis dan Backup

Tahap ini memastikan seluruh data dan sistem dalam kondisi aman sebelum dilakukan perubahan.

1. Melakukan backup seluruh data penting dan konfigurasi sistem yang akan diperbarui.
2. Memastikan ketersediaan file instalasi atau patch yang valid dan bebas dari malware.
3. Menyiapkan lingkungan uji coba (staging) untuk simulasi instalasi atau update.

Penanggung Jawab: Tim IT Infrastruktur

Tahap 3: Pelaksanaan Instalasi atau Update

Tahap implementasi dilakukan sesuai rencana dengan memperhatikan standar keamanan dan prosedur teknis.

1. Melaksanakan instalasi atau update sesuai panduan teknis dan jadwal yang telah disetujui.
2. Memonitor proses instalasi untuk memastikan tidak terjadi error atau kegagalan sistem.
3. Mendokumentasikan setiap langkah dan perubahan konfigurasi yang dilakukan.

Penanggung Jawab: Tim IT Infrastruktur

Tahap 4: Pengujian dan Validasi Sistem

Setelah instalasi atau update, sistem harus diuji untuk memastikan fungsi berjalan dengan baik dan tidak ada gangguan.

1. Melakukan pengujian fungsional terhadap sistem yang telah diinstal atau diperbarui.
2. Melakukan pengujian keamanan untuk memastikan tidak ada celah baru yang muncul.
3. Meminta persetujuan dari user atau stakeholder terkait sebelum sistem digunakan secara penuh.

Penanggung Jawab: Quality Assurance IT dan Tim Keamanan Informasi

Tahap 5: Implementasi dan Monitoring

Tahap ini memastikan sistem berjalan dengan baik dalam operasional sehari-hari setelah update dilakukan.

1. Mengaktifkan sistem secara penuh untuk digunakan oleh seluruh pengguna.
2. Melakukan monitoring performa sistem secara intensif selama periode awal pasca update.
3. Menangani segera jika terjadi gangguan atau error yang dilaporkan.

Penanggung Jawab: Tim IT Infrastruktur

Tahap 6: Dokumentasi dan Evaluasi

Tahap akhir untuk memastikan seluruh proses terdokumentasi dan menjadi bahan evaluasi ke depan.

1. Menyusun laporan lengkap mengenai proses instalasi atau update yang telah dilakukan.
2. Melakukan evaluasi terhadap kendala yang terjadi selama proses.
3. Menyimpan seluruh dokumen sebagai arsip dan referensi audit.

Penanggung Jawab: Manajer IT

Dokumen Terkait

- Form Permintaan Perubahan Sistem (Change Request Form)
- Dokumen Kebijakan Keamanan Informasi Perusahaan
- Checklist Backup dan Recovery Data
- Log Aktivitas Sistem IT
- Dokumen Standar Konfigurasi Sistem

Referensi

- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi
- Peraturan Menteri Kominfo No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi
- Best Practice ITIL (Information Technology Infrastructure Library)