

SOP Penggunaan Email Perusahaan

Kategori: IT & Sistem

No. Dokumen: SOP-0056

Tanggal Terbit: 20/04/2026

Sumber: GajiHub SOP — sop.gajihub.com

Pedoman resmi penggunaan email perusahaan untuk memastikan komunikasi profesional, aman, dan sesuai kebijakan organisasi.

Tujuan

SOP ini disusun untuk memberikan pedoman yang jelas dan terstandar terkait penggunaan email perusahaan oleh seluruh karyawan. Tujuannya adalah untuk memastikan komunikasi bisnis berjalan secara profesional, efisien, dan aman, serta meminimalkan risiko kebocoran data, penyalahgunaan fasilitas perusahaan, dan pelanggaran hukum. Selain itu, SOP ini juga bertujuan untuk menjaga reputasi perusahaan dalam setiap komunikasi elektronik yang dilakukan oleh karyawan, baik internal maupun eksternal, serta memastikan kepatuhan terhadap regulasi yang berlaku di Indonesia.

Ruang Lingkup

SOP ini berlaku untuk seluruh karyawan, manajemen, tenaga kontrak, dan pihak lain yang diberikan akses ke sistem email perusahaan. Ruang lingkup mencakup penggunaan email untuk komunikasi internal dan eksternal, pengelolaan akun email, pengiriman dan penerimaan informasi, keamanan data, penyimpanan arsip email, serta pengawasan penggunaan email oleh perusahaan. SOP ini juga mencakup penggunaan perangkat pribadi yang terhubung dengan email perusahaan serta kebijakan terkait konten yang diperbolehkan dan dilarang dalam komunikasi email.

Definisi

Istilah	Definisi
Email Perusahaan	Akun email resmi yang disediakan oleh perusahaan untuk keperluan komunikasi bisnis.
Pengguna	Karyawan atau pihak lain yang memiliki akses ke email perusahaan.
Informasi Rahasia	Informasi yang bersifat sensitif dan tidak boleh disebarluaskan tanpa izin, termasuk data pelanggan, keuangan, dan strategi bisnis.

Istilah	Definisi
Phishing	Upaya penipuan melalui email untuk memperoleh informasi sensitif dengan menyamar sebagai pihak terpercaya.
Administrator IT	Pihak yang bertanggung jawab atas pengelolaan sistem email perusahaan.

Tanggung Jawab

Pihak	Tanggung Jawab
Karyawan	Menggunakan email perusahaan secara profesional, menjaga kerahasiaan informasi, serta mematuhi seluruh kebijakan yang ditetapkan dalam SOP ini.
Atasan Langsung	Mengawasi penggunaan email oleh anggota tim dan memastikan kepatuhan terhadap SOP.
Departemen IT	Mengelola sistem email, menjaga keamanan sistem, melakukan monitoring, serta menangani insiden terkait email.
Manajemen	Menetapkan kebijakan penggunaan email dan memastikan implementasinya berjalan efektif di seluruh organisasi.

Prosedur

Tahap 1: Pembuatan dan Pengelolaan Akun Email

Proses pembuatan, perubahan, dan penghapusan akun email perusahaan dilakukan secara terkontrol untuk menjaga keamanan dan integritas sistem.

- Departemen HR mengajukan permintaan pembuatan akun email baru kepada Departemen IT untuk karyawan yang baru bergabung.
- Departemen IT membuat akun email sesuai dengan format standar perusahaan dan memberikan kredensial awal kepada pengguna.
- Pengguna wajib mengganti kata sandi awal saat pertama kali login dan menjaga kerahasiaannya.
- Perubahan akses atau penonaktifan akun dilakukan berdasarkan permintaan resmi dari HR atau manajemen.
- Akun email yang tidak aktif selama periode tertentu akan dievaluasi dan dapat dinonaktifkan oleh Departemen IT.

Penanggung Jawab: Departemen IT dan HR

Tahap 2: Penggunaan Email untuk Komunikasi Bisnis

Penggunaan email harus mencerminkan profesionalisme dan mendukung efektivitas komunikasi bisnis perusahaan.

1. Pengguna wajib menggunakan bahasa yang sopan, jelas, dan profesional dalam setiap email.
2. Subjek email harus ditulis secara ringkas dan menggambarkan isi pesan.
3. Pengiriman email massal harus mendapatkan persetujuan dari atasan atau pihak terkait.
4. Pengguna wajib menggunakan tanda tangan email resmi perusahaan.
5. Email harus digunakan hanya untuk keperluan bisnis, bukan untuk kepentingan pribadi yang tidak relevan.

Penanggung Jawab: Seluruh Karyawan

Tahap 3: Keamanan dan Kerahasiaan Email

Langkah-langkah untuk memastikan keamanan data dan mencegah akses tidak sah terhadap email perusahaan.

1. Pengguna dilarang membagikan kata sandi email kepada pihak lain tanpa izin resmi.
2. Pengguna wajib mengaktifkan autentikasi dua faktor jika tersedia.
3. Email yang mencurigakan atau diduga phishing harus segera dilaporkan ke Departemen IT.
4. Pengiriman informasi rahasia harus menggunakan enkripsi atau metode keamanan tambahan.
5. Perangkat yang digunakan untuk mengakses email harus dilindungi dengan antivirus dan sistem keamanan terbaru.

Penanggung Jawab: Departemen IT dan Seluruh Pengguna

Tahap 4: Pengarsipan dan Penyimpanan Email

Pengelolaan arsip email dilakukan untuk memastikan ketersediaan data dan kepatuhan terhadap regulasi.

1. Email penting harus disimpan dan diarsipkan sesuai dengan kebijakan retensi data perusahaan.
2. Pengguna wajib mengorganisasi email dalam folder yang sistematis.
3. Departemen IT melakukan backup data email secara berkala.
4. Email yang berkaitan dengan transaksi bisnis harus disimpan minimal sesuai ketentuan hukum yang berlaku.
5. Penghapusan email harus dilakukan dengan hati-hati dan sesuai kebijakan perusahaan.

Penanggung Jawab: Departemen IT dan Pengguna

Tahap 5: Monitoring dan Evaluasi Penggunaan Email

Perusahaan melakukan pengawasan terhadap penggunaan email untuk memastikan kepatuhan dan mencegah penyalahgunaan.

1. Departemen IT melakukan monitoring aktivitas email secara berkala.

2. Audit penggunaan email dilakukan untuk mendeteksi pelanggaran kebijakan.
3. Pelanggaran SOP akan dikenakan sanksi sesuai dengan peraturan perusahaan.
4. Hasil evaluasi digunakan untuk meningkatkan kebijakan dan sistem keamanan email.
5. Pelatihan berkala diberikan kepada karyawan terkait penggunaan email yang aman dan efektif.

Penanggung Jawab: Departemen IT dan Manajemen

Dokumen Terkait

- Kebijakan Keamanan Informasi Perusahaan
- Peraturan Perusahaan tentang Etika Kerja
- Panduan Penggunaan Sistem IT
- Form Permintaan Akses Sistem
- Laporan Insiden IT

Referensi

- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi
- Kebijakan Internal Perusahaan terkait Teknologi Informasi