STANDAR OPERASIONAL PROSEDUR (SOP)

KEAMANAN DATA & SISTEM ELEKTRONIK SMARTBOSP

Nomor Dokumen	SB-SOP-IT-004	**Tanggal Berlaku**	11 Juni 2026
Revisi	00 (Draf Awal)	**Sifat Dokumen**	Internal Terbatas (Rahasia)

Peringatan: Dokumen ini wajib dicetak dan menjadi panduan kerja internal SmartBosp. Penyebarluasan dokumen ini kepada pihak luar tanpa izin tertulis dari manajemen adalah pelanggaran.

A. Tujuan

- Menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data klien serta infrastruktur sistem SmartBosp dari potensi kebocoran data, modifikasi yang tidak sah, atau akses tanpa izin.
- Menciptakan standar kerja yang seragam bagi seluruh staf IT dan pengelola server dalam menjaga keandalan operasional layanan aplikasi SmartBosp.

B. Keamanan Infrastruktur dan Server (VPS)

- **Akses Server:** Setiap akses menuju server (SSH Login) wajib menggunakan otentikasi Secure Key (*Key-Pair Authentication*). Penggunaan kata sandi standar (*password-based login*) untuk akses root atau user istimewa dilarang keras.
- **Manajemen Firewall:** Port yang tidak digunakan atau tidak relevan dengan layanan wajib ditutup. Proses ini dilakukan menggunakan fitur Firewall yang dikelola melalui kontrol panel server atau sistem proteksi internal VPS.
- **Enkripsi Lalu Lintas Data:** Setiap domain dan sub-domain layanan SmartBosp wajib menerapkan enkripsi lalu lintas data secara menyeluruh menggunakan protokol HTTPS. Sertifikat SSL (menggunakan *Let's Encrypt* atau penyedia setara) harus diperbarui secara berkala dan otomatis sebelum masa berlakunya habis.

C. Manajemen dan Keamanan Database

- **Pencadangan (Backup):** Pencadangan seluruh database MySQL wajib dilakukan secara otomatis dan berkala (minimal harian). Data cadangan harus disimpan pada penyimpanan fisik atau ruang awan (*cloud storage*) yang terisolasi dan terpisah dari server utama guna mencegah kehilangan data ganda.
- **Migrasi Data:** Proses migrasi data antar-server wajib dilakukan menggunakan jalur terenkripsi (seperti rsync over SSH). Data pasca-migrasi wajib divalidasi keutuhannya (*data integrity check*) untuk memastikan tidak ada *corrupt data*.
- **Pembatasan Akses Basis Data:** Akses langsung ke basis data hanya diizinkan melalui IP `localhost` (internal) atau alamat IP publik tertentu yang telah didaftarkan secara resmi ke dalam daftar putih (*Whitelist*).

D. Kendali Akses dan Logika Otentikasi

- **Penyimpanan Kredensial:** Kredensial pengguna dalam basis data, terutama kata sandi, wajib disimpan dalam format *hashing* satu arah yang kuat dan ditambah *salt* (misalnya menggunakan algoritma Bcrypt). Administrator dilarang memiliki visibilitas terhadap kata sandi asli pengguna.
- **Sistem Peringatan Dini:** Sistem peringatan keamanan dan validasi otentikasi vital harus diintegrasikan dengan sistem WhatsApp API gateway. Sistem ini bertugas memberikan notifikasi instan kepada tim IT dan pengguna jika terdeteksi login tidak wajar, perangkat baru, atau ada laporan anomali data.
- **Prinsip Hak Akses Minimal:** Hak akses seluruh karyawan internal dan admin dikelola berdasarkan prinsip *Least Privilege*. Karyawan hanya diberikan hak akses pada fitur atau modul sistem yang mutlak diperlukan sesuai dengan peran dan tanggung jawab jabatannya.

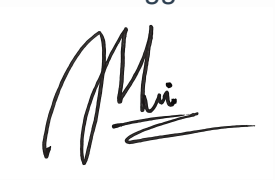
E. Penanganan Insiden Keamanan

- **Isolasi Sistem:** Jika sistem pendeteksi intrusi melaporkan adanya anomali pada trafik atau percobaan peretasan (*brute-force*, eksploitasi kerentanan), administrator sistem wajib melakukan isolasi jaringan VPS segera untuk mencegah pergerakan lateral peretas.
- **Eskalasi Insiden:** Pimpinan (**M I R Z A**) harus diberitahu terkait insiden keamanan dalam waktu kurang dari 1x24 jam. Selanjutnya, tim IT wajib melakukan audit log akses secara menyeluruh untuk mengidentifikasi sumber dan dampak serangan.
- **Pemulihan Kebocoran Data:** Apabila terjadi potensi kebocoran data pelanggan, perusahaan wajib segera memulihkan sistem menggunakan titik cadangan (*backup*) terakhir yang bersih.

Seluruh kunci enkripsi (*encryption keys*) dan kredensial API yang relevan wajib diubah atau diperbarui guna menutup akses tidak sah.

Ditetapkan di: **Aceh**

Tanggal: 02 Februari 2026



MIRZA

Pimpinan SmartBosp