SOP Manajemen Password Universitas Sumatera Selatan (USS)

1. Tujuan
Menetapkan standar dan tata cara pengelolaan password yang aman untuk seluruh akun dan sistem informasi di lingkungan Universitas Sumatera Selatan (USS), guna melindungi akses pengguna dari risiko kebocoran data, peretasan, atau penyalahgunaan akun.

2. Ruang Lingkup
SOP ini berlaku untuk seluruh civitas akademika USS (dosen, staf, dan mahasiswa) yang memiliki akun pada sistem atau layanan berikut:

- SIMAK – https://simak.uss.ac.id
- E-Library – https://elibrary.uss.ac.id
- LMS – https://lms.uss.ac.id
- PMB – https://pmb.uss.ac.id
- Repositori – https://repositori.uss.ac.id
- Jurnal – https://jurnal.uss.ac.id
- Email Kampus – https://admin.google.com
- SISTER, SIMLITABMAS, SINTA, dan aplikasi eksternal lainnya
- Sistem CMS Website Fakultas, Prodi, Lembaga, dan SI-Ortu – https://ortu.uss.ac.id

3. Kebijakan Umum Password

1. Setiap pengguna wajib menjaga kerahasiaan password dari seluruh akun yang dimiliki.
2. Password untuk setiap akun tidak boleh digunakan secara sama di beberapa sistem (no password reuse).
3. Panjang minimal password adalah 12 karakter dengan kombinasi:
    - Huruf besar
    - Huruf kecil
    - Angka
    - Simbol khusus
4. Password harus diganti secara berkala setiap 6 bulan atau segera jika dicurigai terjadi kebocoran.
5. Dilarang menulis atau menyimpan password secara terbuka di catatan fisik atau file tanpa enkripsi.
6. Pengguna sangat disarankan menggunakan aplikasi password manager resmi untuk mengelola seluruh akun.

4. Penggunaan Aplikasi Password Manager
A. Aplikasi yang Direkomendasikan
Aplikasi Bitwarden direkomendasikan sebagai pengelola password resmi oleh STK USS.
Bitwarden bersifat open-source, multi-platform, dan mendukung sinkronisasi antar perangkat.
B. Langkah Pembuatan Akun Bitwarden

1. Kunjungi laman https://bitwarden.com.

2. Klik Create Account dan isi data yang diperlukan (nama, email, dan password utama/master).
3. Password master harus:
    - Mudah diingat oleh pengguna
    - Tidak digunakan di layanan lain
    - Tidak dibagikan kepada siapa pun
4. Lakukan verifikasi email sesuai instruksi dari Bitwarden.
5. Login ke akun Bitwarden setelah verifikasi selesai.

C. Menambahkan Informasi Akun ke Bitwarden

1. Setelah login, klik tombol "+ Add Item".
2. Pada *Type*, pilih Login.
3. Masukkan:
    - Name: Nama layanan (misal "Akun SIMAK USS")
    - Username: Username/NIM/email akun tersebut
    - Password: Password aktif akun
    - URL: Alamat login layanan (misal https://simak.uss.ac.id)
4. Klik Save untuk menyimpan.
5. Ulangi langkah di atas untuk setiap akun (SISTER, SIMLITABMAS, SINTA, Email, LMS, dsb).

D. Mengakses Akun melalui Bitwarden

1. Login ke aplikasi Bitwarden (web, desktop, atau mobile).
2. Klik akun yang ingin diakses.
3. Tekan ikon Launch untuk membuka situs terkait.
4. Gunakan ikon Copy Username dan Copy Password untuk login tanpa mengetik manual.

E. Sinkronisasi Data

1. Bitwarden mendukung sinkronisasi antar perangkat (PC, laptop, dan smartphone).
2. Untuk perangkat mobile:
    - Unduh aplikasi dari Google Play Store atau Apple App Store.
    - Login menggunakan email dan password master yang sama.
3. Semua data akan otomatis tersinkronisasi dan terenkripsi end-to-end.

F. Fitur Tambahan

1. Gunakan fitur Password Generator Bitwarden untuk membuat password acak yang kuat.
2. Simpan hasilnya langsung di aplikasi tanpa perlu mengingat semua password.
3. Gunakan fitur Vault Timeout agar aplikasi terkunci otomatis setelah tidak aktif beberapa menit.

5. Reset atau Lupa Password Master

1. Password master tidak dapat direset oleh pihak STK atau Bitwarden; pengguna bertanggung jawab penuh atas penyimpanannya.
2. Jika lupa password master:
    - Buat akun Bitwarden baru.

    - Reset semua password akun penting (SIMAK, email, LMS, dll).
    - Simpan kembali di akun Bitwarden yang baru.
3. STK hanya membantu proses reset password akun internal kampus, bukan password Bitwarden.

6. Keamanan Data Password

1. Semua data di Bitwarden disimpan dengan enkripsi AES-256, salted hashing, dan PBKDF2 SHA-256.
2. Password master tidak pernah dikirim ke server Bitwarden (zero-knowledge encryption).
3. Pengguna disarankan untuk mengaktifkan:
    - Two-Factor Authentication (2FA) di akun Bitwarden.
    - 2FA di email kampus untuk perlindungan tambahan.

7. Tanggung Jawab

Pihak	Tanggung Jawab
Pengguna (Dosen/Staf/Mahasiswa)	Menjaga kerahasiaan password dan mengelola akun pribadi di Bitwarden.
Unit STK	Memberikan edukasi, panduan resmi, dan dukungan teknis dasar terkait password manager.
Admin Sistem Aplikasi	Menyediakan fitur reset password sesuai SOP dan memastikan mekanisme login aman.

8. Penyimpanan dan Audit

- STK tidak menyimpan password pengguna; semua data dikelola oleh pengguna masing-masing.
- Audit keamanan password dilakukan secara umum (misal: mendeteksi akun yang sering gagal login atau aktivitas mencurigakan).
- Edukasi ulang tentang manajemen password dilakukan setiap awal semester.

9. Sanksi

Setiap pelanggaran terhadap kebijakan keamanan password, seperti:

- Membocorkan password ke pihak lain,
- Menggunakan password lemah di sistem kampus, atau
- Menolak mengganti password setelah peringatan,

dapat dikenai sanksi sesuai peraturan kampus yang berlaku.

10. Referensi

- Kebijakan Keamanan Jaringan dan Server STK USS
- SOP Pembuatan, Penghapusan, dan Reset Akun Pengguna
- SOP Penanganan Insiden Keamanan Siber
- Tutorial Manajemen Password di USS