SOP Integrasi Sistem Aplikasi (API Universitas Sumatera Selatan)

1. Tujuan

Menetapkan tata cara, standar keamanan, dan tanggung jawab dalam pembuatan, penggunaan, dan pengelolaan integrasi antar sistem aplikasi berbasis Application Programming Interface (API) di lingkungan Universitas Sumatera Selatan (USS), agar pertukaran data antar aplikasi berjalan aman, efisien, dan terdokumentasi.

2. Ruang Lingkup

SOP ini mencakup seluruh kegiatan integrasi sistem yang dilakukan antar aplikasi internal kampus maupun dengan sistem eksternal, termasuk:

- Sistem internal: SIMAK, ELibrary, LMS, PMB, Repositori, SI-Ortu, Jurnal, CMS Fakultas/Prodi/Lembaga.
- Sistem eksternal: SISTER Kemdikbud, NeoFeeder PDDikti, layanan email institusi, dan API pihak ketiga yang sah.
- Proses pembuatan, publikasi, konsumsi, dan keamanan API.

3. Dasar Kebijakan

1. Kebijakan Keamanan Data dan Privasi Informasi STK.
2. Standar RESTful API Design & Security (RFC 7231, OWASP API Security).
3. Peraturan perundangan yang berlaku terkait keamanan data dan interoperabilitas sistem pendidikan tinggi.

4. Definisi

Istilah	Keterangan
API (Application Programming Interface)	Antarmuka yang memungkinkan sistem aplikasi saling berkomunikasi dan bertukar data secara terstruktur.
Endpoint	URL tujuan yang menerima atau mengirim data API.
Token / Secret Key	Kunci autentikasi untuk mengamankan akses API.
Provider API	Sistem yang menyediakan API dan datanya bisa diambil oleh sistem lain.
Consumer API	Sistem yang menggunakan (mengambil) data dari API sistem lain.
STK (Sistem Teknologi dan Komunikasi)	Unit yang bertanggung jawab atas perancangan, keamanan, dan dokumentasi API di lingkungan USS.

5. Tanggung Jawab Unit

Unit / Pihak	Tanggung Jawab
STK	Menyusun standar API, menyimpan dokumentasi, mengelola gateway dan keamanan API, serta melakukan audit.
Pengembang Sistem	Mengimplementasikan endpoint, mengatur otorisasi token, dan memastikan kompatibilitas data.

Unit / Pihak	Tanggung Jawab
Pemilik Aplikasi	Menentukan kebutuhan data dan hak akses integrasi dengan sistem lain.
Admin Aplikasi	Melakukan konfigurasi token/API key dan memverifikasi log akses.

6. Prosedur Operasional

A. Perencanaan Integrasi

1. Unit pemilik aplikasi (misal Akademik, Perpustakaan, PMB) mengajukan kebutuhan integrasi kepada STK.
2. STK melakukan analisis kebutuhan meliputi:
    - Jenis data yang akan diintegrasikan (misal data mahasiswa, status kehadiran, pustaka).
    - Arah komunikasi data (satu arah / dua arah).
    - Frekuensi pertukaran data (real-time / batch).
3. STK bersama tim pengembang menyusun Dokumen Desain Integrasi (DDI) yang berisi:
    - Struktur endpoint dan metode HTTP.
    - Format data (JSON/XML).
    - Mekanisme autentikasi.
    - Hak akses masing-masing sistem.

B. Pembuatan dan Konfigurasi API

1. API Internal (Antar Sistem Kampus)

- Pusat Integrasi: berada di SIMAK (https://simak.uss.ac.id) sebagai hub utama data akademik.
- Setiap sistem lain (Elibrary, LMS, Repositori, Jurnal, SI-Ortu, dsb) wajib menyediakan endpoint API dengan:
    - Autentikasi Bearer Token atau HMAC Secret Key.
    - Filter parameter (misal NIM, ID Kelas) agar hanya data relevan yang dikirim.
    - Pembatasan akses (rate limit) sesuai kebutuhan.

Contoh Skema:
SIMAK (consumer) ---> ELibrary (provider)
GET https://elibrary.uss.ac.id/api/v1/mahasiswa?nim=202301234
Header: Authorization: Bearer {token}

2. API Eksternal

- SISTER (Kemdikbud) dan NeoFeeder PDDikti sudah menyediakan endpoint API resmi.
- STK bertanggung jawab atas:
    - Penyimpanan dan perlindungan API credentials (client_id, secret).
    - Penjadwalan sinkronisasi data otomatis.
    - Validasi hasil transfer data dan logging.

3. Keamanan API

- Setiap endpoint wajib melalui verifikasi berikut:
    - Hanya melayani permintaan dari IP whitelist sistem internal.
    - Semua koneksi menggunakan HTTPS dengan sertifikat valid.
    - Token atau secret key disimpan di environment variable, bukan di file publik.

    - Token diganti setiap 6 bulan sekali atau saat ada pergantian admin.
    - Gunakan rate limiting untuk mencegah flood request.
- Audit keamanan API dilakukan minimal 2 kali per tahun oleh STK.

C. Pengujian dan Dokumentasi

1. Sebelum API aktif, dilakukan pengujian (unit test dan integrasi test) antara provider dan consumer.
2. Dokumentasi API mencakup:
    - Deskripsi endpoint dan parameter.
    - Contoh request dan response.
    - Kode status HTTP.
    - Mekanisme error handling.
3. Dokumentasi disimpan di Portal API STK (internal) atau sistem version control (misalnya GitLab/GitHub kampus).

D. Pemeliharaan dan Monitoring

1. Setiap API memiliki log aktivitas:
    - Catatan waktu akses, endpoint, IP, dan hasil response (status code).
    - Disimpan minimal 6 bulan untuk keperluan audit.
2. STK melakukan pemantauan uptime dan performa API, dan hasilnya dapat dipantau publik melalui:
   🔗 https://usscampus.instatus.com
3. Jika ditemukan error (misal 500 Internal Server Error, atau timeout >10 detik), sistem akan otomatis memberi notifikasi ke admin STK.
4. Versi API yang sudah usang (deprecated) harus diberi notifikasi 30 hari sebelum dinonaktifkan.

E. Manajemen Akses dan Keamanan Data

1. Permintaan token API dilakukan oleh admin aplikasi ke STK dengan form permintaan resmi.
2. Token bersifat individual per sistem (bukan per user).
3. Setiap akses ke data pribadi mahasiswa/dosen wajib:
    - Menggunakan enkripsi SSL/TLS.
    - Mematuhi aturan perlindungan data pribadi.
    - Tidak boleh menyimpan data sensitif secara permanen di sistem eksternal tanpa izin tertulis.

F. Integrasi Khusus

Sistem	Arah Integrasi	Status	Keterangan
SIMAK ↔ ELibrary	Dua arah	Aktif	Mengambil data mahasiswa & peminjaman buku via API.
SIMAK ↔ LMS	Dua arah	Aktif	Sinkronisasi daftar kuliah dan peserta otomatis.

Sistem	Arah Integrasi	Status	Keterangan
SIMAK ↔ PMB	Satu arah	Aktif	Import mahasiswa baru dari hasil seleksi PMB.
SIMAK ↔ NeoFeeder	Dua arah	Aktif	Sinkronisasi data akademik ke PDDikti.
SIMAK ↔ SISTER	Satu arah	Aktif	Pengambilan data dosen & aktivitas tridarma.
SIMAK ↔ SI-Ortu	Satu arah	Aktif	Menampilkan nilai dan status kehadiran mahasiswa.
SIMAK ↔ Repositori	Satu arah	Aktif	Sinkronisasi data tugas akhir mahasiswa.

7. Penanganan Gangguan Integrasi
    1. Jika terjadi kegagalan integrasi:
        - Lakukan pemeriksaan endpoint dan token di sisi provider dan consumer.
        - Cek log API untuk memastikan status kode error.
        - Jika berkaitan dengan sistem eksternal (misal NeoFeeder), lakukan pelaporan ke pihak penyedia API eksternal.
    2. Catat kejadian dan tindakan korektif di log insiden STK.

8. Evaluasi dan Review
    - Review konfigurasi dan arsitektur integrasi dilakukan minimal setiap semester.
    - Audit API (keamanan, performa, dokumentasi) dilakukan minimal setiap 6 bulan.
    - Versi API diperbarui mengikuti perubahan struktur data SIMAK atau sistem terkait.

9. Referensi
    - Dokumentasi resmi Moodle REST API.
    - Dokumentasi SISTER API (Kemdikbud).
    - Dokumentasi NeoFeeder API (PDDikti).
    - Standar OWASP API Security Top 10.
    - Kebijakan Keamanan Data dan Jaringan STK USS.