SOP Penanganan Insiden Keamanan Siber (hacker, malware)

Unit: Sistem Teknologi dan Komunikasi (STK)
Lingkup: Seluruh sistem dan aplikasi berbasis web di lingkungan Universitas Sumatera Selatan (USS)

1. Tujuan
Memberikan panduan terstruktur dalam mendeteksi, menangani, memulihkan, dan mencegah kembali terjadinya insiden keamanan siber, seperti peretasan (hacking), malware injection, atau kompromi sistem web, dengan menjaga integritas dan ketersediaan layanan kampus.

2. Ruang Lingkup
SOP ini berlaku untuk semua sistem dan server kampus yang dikelola STK, termasuk:

- VPS atau server fisik milik kampus maupun pihak penyedia eksternal (grup perusahaan kampus).
- Aplikasi web seperti: SIMAK, PMB, LMS, Repositori, E-Library, SI-Ortu, Jurnal, CMS Fakultas/Prodi/Lembaga, dan sistem lainnya.
- Integrasi API antar sistem dan layanan eksternal (NeoFeeder, SISTER, dsb).

3. Dasar Kebijakan

1. Kebijakan Keamanan Informasi Universitas Sumatera Selatan.
2. Pedoman Keamanan Sistem Informasi Pendidikan Tinggi (Kemdikbudristek).
3. Standar Internasional ISO/IEC 27035 – Information Security Incident Management.
4. Panduan OWASP untuk mitigasi serangan web.

4. Definisi

Istilah	Keterangan
Insiden Keamanan Siber	Kejadian yang mengancam kerahasiaan, integritas, atau ketersediaan sistem (hacker, deface, malware, data leak).
Isolation (Isolasi)	Pemutusan sementara akses ke sistem yang terindikasi terinfeksi untuk mencegah penyebaran.
WAF (Web Application Firewall)	Lapisan keamanan untuk menyaring dan memblokir serangan HTTP/S terhadap aplikasi web.
Hardening	Proses penguatan sistem untuk meminimalkan celah keamanan.
Staging Server	Server non-produksi yang digunakan untuk pengujian sebelum deployment ke sistem aktif.

5. Tanggung Jawab Unit

Pihak	Tanggung Jawab
STK	Menangani insiden keamanan, koordinasi dengan penyedia VPS, melakukan isolasi, forensik, dan pemulihan.

Pihak	Tanggung Jawab
Penyedia VPS	Membantu isolasi server dan memfasilitasi snapshot atau akses forensik.
Admin Aplikasi / Unit Pemilik Sistem	Memberikan informasi terkait aktivitas terakhir, log, dan konfigurasi aplikasi.
Pimpinan Universitas / Rektorat	Menyetujui langkah pemulihan strategis dan komunikasi resmi kepada pengguna atau publik jika diperlukan.

6. Tahapan Penanganan Insiden

A. 1. Deteksi Awal

- Sumber deteksi dapat berasal dari:
  - Laporan pengguna (web deface, login error, downtime).
  - Alert dari monitoring (https://usscampus.instatus.com).
  - Notifikasi keamanan (CSF, WAF, IDS).
- STK mencatat waktu, sistem terdampak, dan jenis gejala yang muncul.
- Jika terindikasi serangan aktif (deface, RCE, data leak), segera lanjut ke tahap isolasi.

B. 2. Isolasi Sistem

- Koordinasi langsung dengan penyedia VPS untuk menutup sementara akses publik:
  - Nonaktifkan interface jaringan atau ubah firewall rule agar hanya IP STK yang bisa masuk.
  - Jika di hosting di Centminmod, ubah konfigurasi csf -d 0.0.0.0/0 untuk deny semua kecuali IP admin.
- Buat snapshot atau image backup VPS sebelum modifikasi apa pun untuk keperluan forensik.
- Catat seluruh tindakan isolasi di *Incident Log Sheet* STK.

C. 3. Analisis dan Forensik Awal

- STK memeriksa:
  - Log web server (Nginx/Apache), log sistem (/var/log/secure, /var/log/messages).
  - File yang baru diubah (gunakan find / -mtime -1 -type f).
  - Aktivitas login mencurigakan (last, who, journalctl).
  - File berisi script injeksi atau backdoor (gunakan grep -R base64_decode atau eval pada web root).
- Pastikan tidak ada cronjob atau service yang menjalankan script berbahaya.
- Jika infeksi berat, backup hanya data bersih (database dan file penting), bukan seluruh root filesystem.

D. 4. Pemulihan Sistem di Staging Server

1. Siapkan staging server baru (VPS bersih) dengan OS dan spesifikasi serupa.
2. Install ulang stack menggunakan Centminmod versi stabil (sesuai panduan resmi).
3. Restore data dari backup terakhir yang aman (via Restic dari Wasabi atau snapshot sebelum insiden).

4. Lakukan hardening server dan aplikasi:
    - Nonaktifkan login root via password, gunakan SSH key.
    - Update semua paket OS (dnf update -y).
    - Pastikan firewall CSF aktif dan terkonfigurasi minimal port 22, 80, 443.
    - Instalasi ulang plugin atau tema web dari sumber resmi.
    - Ubah semua password database dan aplikasi.
    - Pastikan WAF aktif di layer provider (jika tersedia).
5. Lakukan uji coba fungsionalitas aplikasi:
    - Pastikan tidak ada sisa kode injeksi.
    - Pastikan autentikasi dan data pengguna berjalan normal.
    - Jalankan tes performa dan keamanan dasar (OWASP Zap atau Nikto).

E. 5. Validasi dan Deployment ke Produksi

- Setelah hasil uji di staging positif (bersih, stabil, dan aman):
    - Migrasikan kembali ke server produksi baru.
    - Update DNS/Load Balancer agar mengarah ke IP server baru.
    - Verifikasi bahwa layanan publik kembali normal.
- Dokumentasikan seluruh tahapan pemulihan di log insiden STK.

F. 6. Pasca-Insiden dan Pencegahan

1. Audit Keamanan Menyeluruh
    - Periksa akun admin dan akses lama yang tidak terpakai.
    - Perkuat konfigurasi CSF (deny IP mencurigakan, aktifkan rate limit).
    - Integrasikan dengan WAF (Web Application Firewall) jika belum aktif.
    - Aktifkan Fail2Ban atau fitur login brute-force protection di Centminmod.
2. Update Aplikasi
    - Jika aplikasi (CMS, LMS, Jurnal, OJS, dll) sudah tersedia versi stabil baru, segera lakukan upgrade.
    - Hilangkan plugin/tema yang tidak dipakai.
3. Backup dan Redundansi
    - Pastikan backup harian berjalan normal (Restic + Wasabi).
    - Simulasikan restore setiap 3 bulan.
4. Dokumentasi dan Edukasi
    - Laporan lengkap insiden dibuat maksimal 3 hari setelah pemulihan.
    - STK mengedukasi admin aplikasi agar tidak mengunggah file sembarangan dan rutin update.

7. Dokumentasi Wajib

Setiap insiden wajib memiliki dokumen berikut:

1. Formulir Laporan Insiden Keamanan Siber (isi: waktu, sistem terdampak, jenis serangan, penanganan, dampak).
2. Log Bukti Teknis (Forensik) dari server terdampak.
3. Tindakan Pemulihan yang dilakukan.
4. Laporan Evaluasi Pasca-Insiden (post-mortem).

5. Bukti integrasi WAF atau konfigurasi hardening baru.

---

8. Komunikasi dan Eskalasi

Level	Situasi	Tindakan
Level 1 – Minor	Malware terdeteksi di satu aplikasi non-kritis	Isolasi & perbaikan oleh STK.
Level 2 – Moderat	Web deface atau indikasi eksploitasi akun admin	Koordinasi STK + unit pemilik sistem.
Level 3 – Kritis	Data bocor, ransomware, atau eksploitasi lintas sistem	Isolasi total, koordinasi dengan penyedia VPS, laporan resmi ke pimpinan.

9. Evaluasi dan Review

- Review SOP dilakukan minimal setiap 12 bulan atau setelah terjadi insiden besar.
- Audit keamanan dilakukan setiap semester meliputi patch management, konfigurasi firewall, dan update aplikasi.
- Hasil review digunakan untuk meningkatkan prosedur hardening dan backup.

10. Referensi

- ISO/IEC 27035: Information Security Incident Management
- OWASP Server Security Checklist
- Panduan Centminmod Security (https://centminmod.com)
- Panduan Restic Backup (https://restic.readthedocs.io)
- Kebijakan Keamanan Jaringan dan Server STK USS