Standar Operasional Prosedur (SOP)
PENANGANAN INSIDEN SIBER APLIKASI

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI

UNIVERSITAS AIRLANGGA

DIREKTORAT SISTEM INFORMASI DAN DIGITALISASI

2025

Identitas SOP

Nama SOP	Penanganan Insiden Siber Aplikasi	
Nomor SOP	SOP-UNAIR-SID-15	
Tanggal Pembuatan	14 Februari 2023	
Revisi	-	
Tanggal Revisi	-	
Tanggal Efektif	18 Juli 2025	
Perumusan: **Abdur Rahman Sadad, S.Kom** **NIP. 198805142018013101**	**Penetapan:** **Yunus Abdul Halim, S.Si., M.Kom.** **NIP. 197501232008121002**	**Pengendalian:** **Rachmad Setiawan, S.Kom.** **NIP.197008272006041002**

A. DASAR HUKUM

1. Peraturan Presiden (Perpres) Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
2. Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi No. 35/2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi.
3. Pemerintah Peraturan Menteri Riset, Teknologi dan Pendidikan Tinggi No. 71/2017 tentang Pedoman Penyusunan dan Evaluasi Peta Proses Bisnis dan Strandar Operasional Prosedur di Lingkungan Kemenristekdikti.
4. Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi No. 19/2018 tentang Penyusunan Peta Proses Bisnis Instansi Pemerintah

B. KETERKAITAN

1. Surat Keputusan Rektor tentang Penetapan *Computer Security Incident Response Team* (CSIRT) di Universitas Airlangga
2. SOP Penetration Testing Website

C. KUALIFIKASI PELAKSANA

Tim Teknis yang meliputi :

a. Sekretariat CSIRT
   - Menerima laporan insiden siber aplikasi dari pihak eksternal.
   - Meneruskan informasi kepada *Red Team* untuk validasi.
   - Menyampaikan laporan hasil validasi oleh *Red Team* kepada Pemilik Aplikasi.
   - Mengumpulkan laporan tindak lanjut dari Pemilik Aplikasi.
   - Menginstruksikan *Blue Team* untuk membatasi akses jika tindak lanjut tidak dilakukan.

b. *Red Team* CSIRT
   - Melakukan validasi terhadap laporan insiden atau kerentanan yang ditemukan.
   - Melakukan *penetration testing* dan eksploitasi terhadap aplikasi.
   - Mengidentifikasi tingkat keparahan kerentanan (kritikal atau non-kritikal).
   - Menyusun laporan hasil validasi dan menyampaikan ke Sekretariat CSIRT.

c. *Blue Team* CSIRT
   - Membatasi akses atau mengambil langkah mitigasi jika ada kegagalan respon dari Pemilik aplikasi.

D. PERALATAN/PERLENGKAPAN

1. Komputer / Laptop
2. Internet

E. PERINGATAN

-

F. URAIAN SOP PENANGANAN INSIDEN APLIKASI

a. **Sekretariat CSIRT** menerima **informasi/laporan** dari pihak eksternal tentang adanya serangan siber/adanya celah kerentanan aplikasi, dan meneruskan informasi tersebut ke **Red Team** pada **hari yang sama**.

b. **Red Team** melakukan validasi dan membuat **laporan hasil validasi** kepada **Sekretariat CSIRT** maksimal :
   - Kerentanan kritikal, di **hari yang sama**.
   - Bukan kritikal, **1 hari** setelah laporan diterima.

c. **Sekretariat CSIRT** meneruskan **laporan hasil validasi** dari **Red Team** kepada **Pemilik Aplikasi** pada **hari yang sama**.

d. **Sekretariat CSIRT** menerima **laporan tindak lanjut** dari **Pemilik Aplikasi** berupa laporan tindakan apa saja yang telah dikerjakan dan *file log server* maksimal **1 hari** setelah laporan hasil validasi dari **Red Team** dikirim.

e. **Sekretariat CSIRT** meminta **Blue Team** untuk membatasi **hak akses aplikasi** apabila **Pemilik Aplikasi** tidak mengirimkan laporan tindak lanjut maksimal **1 hari** setelah laporan hasil validasi dari **Red Team** dikirim

G. PENCATATAN DAN PENDATAAN

Data-data yang didokumentasikan adalah:

- Aplikasi yang memiliki kerentanan
- *Vulnerability* dari aplikasi
- *Log Server*
- Laporan tindak lanjut aplikasi yang mengalami kerentanan

Diagram Alur Penanganan Insiden Siber Aplikasi Dari Temuan Eksternal