Standard Operating Procedure (SOP)

Vulnerability Management

No.517/IT1.B05.3/OT/2021

DIREKTORAT SISTEM DAN TEKNOLOGI INFORMASI
INSTITUT TEKNOLOGI BANDUNG
2021

Standard Operating Procedure (SOP)

JUDUL : Vulnerability Management	NOMOR : 517/IT1.B05.3/OT/2021 REVISI KE : 0 BERLAKU TMT : 28 Desember 2021 HALAMAN : 1 dari 4

RIWAYAT REVISI

-

LEMBAR PENGESAHAN

Disiapkan oleh:	
Kepala Seksi Perencanaan dan Tata Kelola Sistem dan Teknologi Informasi **Gulam Fakih, S.Kom., M.T.** **Nopeg. 117000032**	Kepala Sub Direktorat Perencanaan dan Pengembangan Sistem dan Teknologi Informasi **Mugi Sugiarto, S.Si. M.AB.** **Nopeg. 106000608**
Tgl:	Tgl:

Disetujui oleh:
Direktur Sistem dan Teknologi Informasi, **Dr.Ir. Arry Akhmad Arman, M.T.** **NIP 196504141991021001**

Standard Operating Procedure (SOP)

JUDUL : Vulnerability Management	NOMOR : 517/IT1.B05.3/OT/2021 REVISI KE : 0 BERLAKU TMT : 28 Desember 2021 HALAMAN : 2 dari 4

DAFTAR ISI

JUDUL : Vulnerability Management	NOMOR : 517/IT1.B05.3/OT/2021 REVISI KE : 0 BERLAKU TMT : 28 Desember 2021 HALAMAN : 3 dari 4

I. UNIT KERJA TERKAIT

N/A

II. TUJUAN

Dokumen SOP ini disusun untuk mengatur mekanisme manajemen kerentanan (*vulnerability Management*) di DSTI.

III. REFERENSI

-

IV. PENGERTIAN & BATASAN

A. PENGERTIAN

1. **Seksi Operasional** adalah seksi di DSTI yang bertanggung jawab terhadap kegiatan operasional infrastruktur TI dan Aplikasi sehari-hari dan mengoprasikan Jaringan network dan Aplikasi yang menjadi tanggung jawab DSTI.
2. **Seksi Pengembangan** adalah seksi di DSTI yang bertanggung jawab terhadap pengembangan sistem dan teknologi informasi di DSTI dan mengelola proses implementasi atau penerapan perubahan konfigurasi / *upgrade* / pemasangan baru perangkat jaringan teknologi informasi.
3. ***Vulnerability Assesment*** adalah adalah proses mendefinisikan, mengidentifikasi dan mengklasifikasikan lubang keamanan dalam sistem teknologi informasi.
4. ***Penetration Testing*** adalah adalah serangan siber resmi yang disimulasikan pada sistem komputer, dilakukan untuk mengevaluasi keamanan sistem.
5. ***System Hardening*** adalah kumpulan alat, teknik, dan praktik terbaik untuk mengurangi kerentanan dalam aplikasi teknologi, sistem, infrastruktur, firmware, dan area lainnya.

B. BATASAN

1. Dokumen ini menjelaskan prosedur manajemen kerentanan.keamanan TI yang berlaku di DSTI.

V. PROSEDUR

1. Seksi Operasional dan Seksi Pengembangan melakukan Persiapan kegiatan *Vulnerability Assessment* dengan membuat Rencana Detail Kegiatan *Assessment*.

2. Kemudian Seksi Operasional dan Seksi Pengembangan bersama-sama melakukan kegiatan *Vulnerability Assessment*/Monitoring. Dari kegiatan ini menghasilkan dokumentasi Hasil *Vulnerability Assessment*.
3. Dokumentasi tersebut menjadi rujukan bagi Seksi Operasional dan Seksi Pengembangan untuk melakukan *Penetration Testing*.
4. Dari hasil *Penetration Testing* tersebut maka Seksi Operasional dan Seksi Pengembangan melakukan identifikasi apakah terdapat celah kerentanan keamanan yang dapat dieksploitasi atau tidak pada sistem.
5. Apabila terdapat celah kerentanan keamanan, maka Seksi Operasional dan Seksi Pengembangan bersama-sama melakukan kegiatan *System Hardening* hingga celah kerentanan keamanan tersebut teratasi.

VI. INDIKATOR KEBERHASILAN

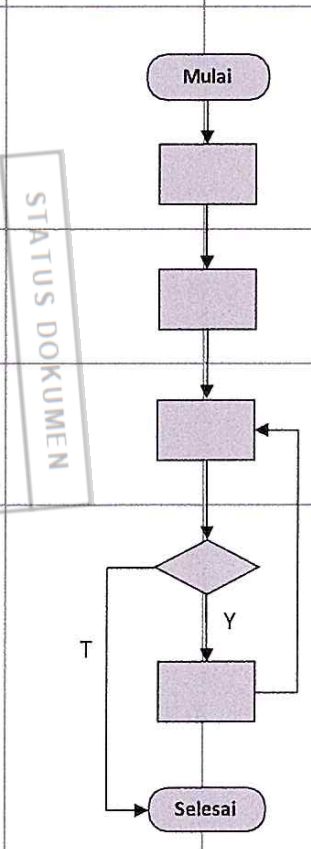
1. Manajemen kerentanan (*Vulnerability Management*) berhasil dilakukan.

VII. LAMPIRAN

Lampiran 1 – Diagram Alir Prosedur *Vulnerability Management*

Lampiran 1 – 517/IT1.B05.3/OT/2021

Diagram Alir Prosedur *Vulnerability Management*

No.	Uraian Kegiatan	Pelaksana		Input	Output
		Seksi Operasional	Seksi Pengembangan		
1	Persiapan kegiatan *Vulnerability Assessment*				Rencana Detail Kegiatan *Assessment*
2	*Vulnerability Assessment/Monitoring*				Dokumentasi Hasil *Vulnerability Assessment*
3	*Penetration Testing*			Dokumentasi Hasil *Vulnerability Assessment*	Dokumentasi hasil Pentest
4	Apakah terdapat kerentanan yang dapat dieksploitasi? Jika ya, maka akan dilakukan kegiatan *System Hardening*				Dokumentasi *Hardening*