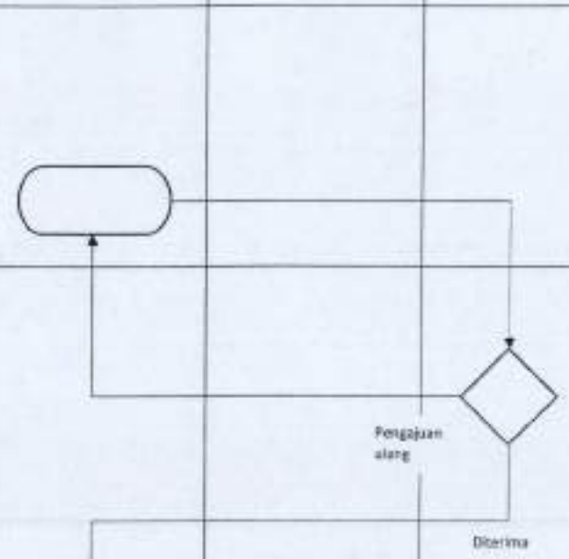
STANDAR OPERASIONAL PROSEDUR (SOP)
PENGUJIAN KEAMANAN INFORMASI SECARA RUTIN

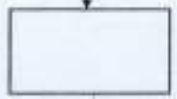
DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN
KOTA YOGYAKARTA

DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KOTA YOGYAKARTA	**Nomor SOP**	102/SANDI/2023
	Tanggal Pembuatan	
	Tanggal Revisi	
	Tanggal Pengesahan	
	Disahkan oleh	Kepala Ignatius Trihastono, S.Sos., M.M. NIP 19690723 199603 1 005
	Nama SOP	Pengujian Keamanan Informasi Secara Rutin

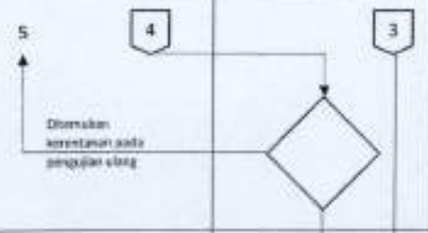
Dasar Hukum:	**Kualifikasi Pelaksana:**
1. Peraturan Daerah Kota Yogyakarta Nomor 10 Tahun 2021 tentang Pengelolaan dan Pemanfaatan Teknologi Informasi dan Komunikasi; 2. Peraturan Walikota Yogyakarta Nomor 105 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi, dan Tata Kerja Dinas Komunikasi Informatika dan Persandian; 3. Peraturan Walikota Yogyakarta Nomor 113 Tahun 2019 tentang Sistem Manajemen Keamanan Informasi;	1. Ketua Tim Kerja Pengamanan Informasi: S1 bidang Informatika/Teknik Elektro/Elektronika dan Instrumentasi, diutamakan S2 Informatika/Teknik Elektro/S2 yang serumpun 2. Sandiman: S1 bidang Informatika/Teknik Elektro/Elektronika dan Instrumentasi atau bidang serumpun 3. Pengelola Teknologi Informasi: DIII bidang Teknik Infomatika/Manajemen Teknik Infomatika/Telekomunikasi
Keterkaitan:	**Peralatan/Perlengkapan:**
	1. Komputer/Laptop 2. Jaringan Internet 3. Alat Pemindai Teknologi Informasi
Peringatan:	**Pencatatan dan Pendataan:**

No	Aktivitas	Pelaksana				Mutu Baku			Keterangan
		Tim Kerja Pengamanan Informasi	PIC Sistem	Ketua Tim Kerja	Kepala Bidang Persandian	Kelengkapan	Waktu	Output	
1	Tim Pengamanan Informasi memilih dan mengajukan sistem yang akan diuji dari daftar pengujian rutin					Daftar sistem yang akan diuji	120 menit	Sistem yang akan diuji	Tim Pengamanan Informasi melakukan pemilihan dan pengajuan ke Tim Kerja Pengamanan Informasi melalui daftar rutin pengujian sistem yang telah dibuat di awal tahun
2	Tim Pengamanan Informasi meminta persetujuan Ketua Tim Kerja Pengamanan Informasi terkait sistem rutin yang akan diuji oleh tim.					Sistem yang akan diuji	240 menit	- Persetujuan sistem yang akan diuji - Sistem yang akan diuji	
3	Ketua Tim Kerja Pengamanan Informasi menyetujui dan memerintahkan tim pengamanan informasi untuk melaksanakan pengujian			-	-	- Sistem yang akan diuji	240 menit	Perintah Pelaksanaan Pengujian Keamanan Informasi	Tim pengamanan informasi memilih personil yang akan melakukan pengujian dan memilih waktu pelaksanaan
4	Tim Pengamanan Informasi melakukan *information gathering* menggunakan *tools*.					- *Tools Scanner*	420 menit	- Informasi sistem berdasarkan *scanning* - permodelan ancaman - Temuan kerentanan	penguji melakukan scanning versi OS, port dan layanan yang berjalan. validasi CVE pada teknologi yang digunakan berdasarkan scanning sistem. Penguji juga melakukan pembuktian apakah CVE tersebut memungkinkan untuk dieksploitasi pada sistem tersebut atau tidak.



6	Tim Pengamanan Informasi melakukan *information gathering* pada aplikasi.			-	-	- Tools Penetration - Browser	420 menit	- Informasi sistem - Permodelan ancaman - Temuan kerentanan	Penguji masuk ke sistem dan melakukan pencarian informasi sebanyak – banyaknya. Pada tahap ini penguji mencari semua kemungkinan fitur dan informasi yang dapat dieksploitasi dari sistem, apabila ada penguji melakukan pembuktian kerentanan berdasarkan CVE yang ditemukan.
7	Tim Pengamanan Informasi melakukan pemindaian pada aplikasi berdasarkan url.			-	-	- Dokumen sistem - Tools Penetration - Browser Tool Scanning	420 menit	- Daftar url aplikasi - Temuan kerentanan	Penguji melakukan pemindaian url kemudian melakukan percobaan eksploitasi pada url yang dirasa dapat menjadi sebuah kerentanan
8	Tim Pengamanan Informasi melakukan pengecekkan input validasi, eksploitasi dan injeksi *payload* berdasarkan temuan kerentanan			-	-	- Dokumen sistem - Tools Penetration - Browser - Temuan Kerentanan	420 menit	- Temuan kerentanan	Penguji melakukan pengecekkan validasi input pada sistem, pada tahap ini penguji juga melakukan percobaan eksploitasi pada sistem dengan cara melakukan injeksi *malicious payload* pada fitur atau url yang dimungkinkan rentan.
9	Tim Pengamanan Informasi melakukan pembuatan Laporan Pengujian Keamanan Informasi berdasarkan temuan yang diperoleh.			-	-	- Word Editor		- Draft Laporan Pengujian Keamanan Informasi	
10	Ketua Tim Kerja Pengamanan Informasi melakukan reviu laporan Pengujian Keamanan Informasi yang telah dibuat.				-	- Draft Laporan Pengujian Keamanan Informasi - Panther	420 menit	- Laporan Pengujian Keamanan Informasi	Ketua Tim Kerja Pengamanan Informasi dan Kepala Bidang Persandian melakukan reviu laporan, apabila diterima maka akan dibubuhi tanda tangan

11	Kepala Bidang Persandian melakukan konfirmasi dan tanda tangan Laporan Pengujian Keamanan Informasi yang telah dibuat.			2		Laporan Pengujian Keamanan Informasi	120 menit	- Bukti Pengiriman Laporan	
11	Tim Pengamanan Informasi melakukan pengiriman Laporan ke PIC sistem diketahui oleh Bidang SIS dan Infrastruktur			-	-	- Laporan Pengujian Keamanan Informasi	120 menit	- Bukti Pengiriman Laporan	
12	PIC sistem mengirimkan balasan dari Laporan	Sudah diperbaiki Belum atau tidak ada perbaikan		-	-	- Perbaikan sistem berdasarkan Laporan Pengujian Keamanan Informasi	840 menit	- Feedback koordinasi dengan tim pengamanan informasi	PIC sistem wajib menginformasikan sistem sudah diperbaiki atau belum, diwajibkan berkoordinasi dengan tim pengamanan informasi (apabila tidak ada balasan dalam kurun waktu 2 x 24 jam diasumsikan pemohon menerima risiko kerentanan
13	Tim Pengamanan Informasi melakukan Pengujian ulang kerentanan dari sistem yang telah diperbaiki			-	-	- Perbaikan sistem berdasarkan Laporan Pengujian Keamanan Informasi	420 menit	- Hasil pengujian ulang keamanan informasi	
14	Tim Pengamanan Informasi menginformasikan hasil pengujian ulang ke PIC Sistem	5 4	3	-	-	- Hasil pengujian ulang keamanan informasi	840 menit	- Konfirmasi penerimaan hasil pengujian ulang dari PIC Sistem	

15	PIC Sistem menginformasikan ke Tim Pengamanan informasi terkait perbaikan kerentanan pada sistem dari hasil pengujian ulang		-	-	- Perbaikan sistem berdasarkan informasi hasil Pengujian ulang keamanan informasi	840 menit	- Feedback koordinasi dengan tim pengamanan informasi	PIC Sistem wajib menginformasikan sistem sudah diperbaiki atau belum. diwajibkan berkoordinasi dengan tim pengamanan informasi (apabila tidak ada balasan dalam kurun waktu 2 x 24 jam diasumsikan PIC Sistem menerima risiko kerentanan
16	Tim pengamanan informasi melakukan *update feedback* pada daftar sistem yang diuji		-	-	-	120 menit	-	