PEMERINTAH
KABUPATEN BANGKA

PEDOMAN TEKNIS INOVASI

SIPAKSI

(SISTEM PENDATAAN KERENTANAN PERANGKAT DAN APLIKASI SEBAGAI BAGIAN DARI SISTEM MANAJEMEN KEAMANAN INFORMASI DI DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK KABUPATEN BANGKA)

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK
KABUPATEN BANGKA

A. Latar Belakang

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam tata kelola pemerintahan, terutama dalam pengelolaan layanan publik dan data strategis. Teknologi memberikan kemudahan akses informasi serta meningkatkan efektivitas kinerja organisasi. Namun, di sisi lain perkembangan tersebut juga menghadirkan tantangan baru berupa ancaman siber yang semakin kompleks. Oleh karena itu, instansi pemerintah perlu memiliki sistem keamanan informasi yang terstruktur dan berkelanjutan. Pada praktiknya, masih ditemukan beberapa kendala dalam pengelolaan keamanan informasi di instansi pemerintah. Salah satunya adalah belum adanya standar baku dalam penerapan keamanan informasi, sehingga langkah pengamanan yang dilakukan belum seragam dan sulit untuk dievaluasi. Selain itu, sebagian perangkat keras yang digunakan sudah usang (outdated) sehingga berpotensi menimbulkan gangguan kinerja serta menurunkan produktivitas kerja.

Permasalahan lainnya adalah penggunaan perangkat lunak yang belum diperbarui secara berkala, yang dapat meningkatkan risiko kerentanan terhadap serangan siber. Rendahnya hasil penilaian Tingkat Maturitas Penanganan Insiden (TMPI) juga menunjukkan bahwa tata kelola keamanan informasi dan efektivitas layanan berbasis teknologi informasi belum sepenuhnya memenuhi standar yang ditetapkan pemerintah. Kondisi tersebut diperparah dengan belum tersusunnya dokumentasi keamanan informasi secara menyeluruh sehingga proses mitigasi risiko belum berjalan secara sistematis. Apabila kondisi ini dibiarkan, maka dapat menimbulkan berbagai dampak negatif seperti meningkatnya risiko kebocoran data, terganggunya layanan publik, serta menurunnya kepercayaan masyarakat terhadap pemerintah. Oleh karena itu, diperlukan langkah strategis berupa penerapan sistem pengelolaan keamanan informasi yang lebih terarah melalui pendataan perangkat dan aplikasi secara menyeluruh. Pendataan tersebut diharapkan dapat membantu mengidentifikasi potensi kerentanan sejak dini serta menjadi dasar dalam memperkuat ketahanan sistem informasi dan meningkatkan kualitas pelayanan publik.

B. Penjaringan Ide Inovasi

Penjaringan ide dilakukan melalui observasi dilapangan, pendataan, dan focus group discussion melibatkan pemangku kepentingan yaitu pemerintah kabupaten Bangka, badan kepegawaian dan pengembangan sumber daya manusia daerah kabupaten Bangka, BAPPEDA, masyarakat, pihak bank sumsel babel dan pusat riset dan inovasi institut pahlawan 12 Bangka Belitung serta Politeknik Manufaktur Negeri Bangka Belitung.

C. Pemilihan Ide Inovasi

Pemilihan ide inovasi praktik penerapan “Sistem Pendataan Kerentanan Perangkat Dan Aplikasi Sebagai Bagian Dari Sistem Manajemen Keamanan Informasi Di Dinas Komunikasi Informatika Dan Statistik Kabupaten Bangka” dilakukan berdasarkan hasil observasi lapangan, pendataan, dan diskusi bersama pemangku kepentingan terkait. Dari beberapa isu tersebut dilakukan analisis menggunakan metode APKL (Aktual, Problematik, Kekhalayakan, Layak) dan USG (Urgency, Seriousness, Growth) untuk menentukan isu prioritas. Hasil analisis menunjukkan bahwa isu “Belum diterapkannya Sistem Manajemen Keamanan Informasi (SMKI)” memperoleh skor tertinggi sehingga dipilih sebagai core issue yang akan diselesaikan melalui kegiatan aktualisasi.

D. Tujuan Inovasi

Tujuan dari kegiatan aktualisasi ini adalah:

1. Menyusun sistem pendataan kelayakan perangkat keras secara terstruktur dan terdokumentasi.
2. Mengidentifikasi perangkat yang masih layak digunakan dan yang sudah tidak memadai.
3. Meningkatkan kesadaran pegawai terhadap pentingnya pengelolaan perangkat keras dan perangkat lunak dalam mendukung kinerja organisasi.

E. Manfaat Inovasi

Manfaat dari kegiatan aktualisasi ini antara lain:

1. Menyediakan basis data perangkat yang dapat menjadi dasar pengambilan keputusan terkait pengadaan dan peremajaan perangkat.
2. Meningkatkan efektivitas kinerja ASN karena didukung perangkat kerja yang memadai.
3. Mengurangi risiko keamanan informasi akibat penggunaan perangkat yang sudah usang atau software yang tidak diperbarui.
4. Mendukung peningkatan kualitas pelayanan publik melalui sistem yang lebih optimal.

F. Hasil

Hasil yang diharapkan dari kegiatan aktualisasi ini adalah tersusunnya instrumen pendataan perangkat dan aplikasi yang dapat digunakan sebagai alat untuk melakukan identifikasi dan pencatatan secara sistematis terhadap seluruh perangkat yang digunakan di instansi. Melalui kegiatan ini juga diharapkan dapat tercatat dengan jelas kondisi perangkat keras maupun perangkat lunak yang digunakan oleh pegawai, sehingga instansi memiliki data yang akurat mengenai kelayakan dan kondisi perangkat yang ada. Selain itu, kegiatan ini diharapkan mampu menghasilkan data mengenai potensi kerentanan perangkat yang dapat dijadikan sebagai dasar dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI). Dengan adanya data tersebut, organisasi diharapkan dapat lebih memahami pentingnya pengelolaan perangkat teknologi informasi secara baik sehingga dapat meningkatkan kesadaran serta komitmen dalam menjaga keamanan informasi di lingkungan kerja.

G. Tahapan Kegiatan

Tahapan	Kegiatan	Waktu Pelaksanaan
Persiapan	Konsultasi dengan mentor dan penyiapan bahan kegiatan serta penyusunan rencana pendataan perangkat dan aplikasi	1–10 September 2024
Penjaringan Ide	Diskusi dengan mentor dan rekan kerja mengenai inovasi pendataan kerentanan perangkat dan aplikasi untuk mendukung penerapan SMKI	11–20 September 2024
Pemilihan Ide	Menentukan inovasi berupa sistem pendataan kerentanan perangkat dan aplikasi sebagai langkah awal penerapan Sistem Manajemen Keamanan Informasi (SMKI)	21–30 September 2024

Perancangan	Penyusunan instrumen pendataan perangkat keras, perangkat lunak, dan aplikasi serta pembuatan format dokumentasi kerentanan sistem	1-15 Oktober 2024
Pelaksanaan	Melaksanakan pendataan perangkat dan aplikasi, mengidentifikasi kerentanan, serta menginput data hasil pendataan ke dalam sistem dokumentasi	16 Oktober 2024 – 30 Januari 2025
Evaluasi	Evaluasi hasil pendataan kerentanan perangkat dan aplikasi serta penyusunan laporan hasil kegiatan aktualisasi	1–15 Februari 2025

H. SOP

NO	Uraian Prosedur	Pelaksana (ASN)	Mentor	Admin Sistem	Sistem Data	Kelengkapan	Waktu	Output
1.	Konsultasi awal dan penyusunan rencana pendataan					Rencana Kegiatan	3 Hari	Perseteujuan
2.	Diskusi dan Penjaringan Ide Inovasi					Notulen	5 Hari	Alternatif Ide
3.	Penentuaan Inovasi (SMKI)					Dokumen Ide	5 Hari	Keputusan
4.	Penyusunan Instrumen Pendataan Perangkat dan Aplikasi					Format Data	10 Hari	Instrumen
5.	Pelaksanaan Pendataan Perangkat dan Aplikasi					Data Perangkat	30 Hari	Data Terkumpul
6.	Identifikasi Kerentanan perangkat dan Sistem					Data Analisis	15 Hari	Data Kerentanan
7.	Validasi:Data Sudah Lengkap dan sesuai		Tidak			Data	2 Hari	Status
								Data Diperbaiki
8.	Input dan Dokumentasi Data ke Sistem					Database	10 Hari	Data Tersimpan
9.	Penyusunan Laporan Hasil Pendataan					Laporan	7 Hari	Draft laporan
10.	Validasi: Laporan Disetujui					Laporan	2 Hari	Status
			YA					Laporan Revisi
11.	Finalisasi Laporan					Laporan Akhir	3 Hari	Laporan Final
12.	Evaluasi dan Rekomendasi					Laporan	5 Hari	

Pedoman teknis inovasi — SIPAKSI

1. Persiapan dan pembentukan tim pelaksana Bentuk tim lintas fungsi yang melibatkan **ASN pengguna perangkat, mentor teknis, admin sistem, dan perwakilan keamanan informasi**; tetapkan peran dan tanggung jawab tertulis. Susun rencana kerja yang memuat tujuan pendataan, cakupan perangkat dan aplikasi, jadwal, serta daftar peralatan dan akses yang diperlukan. Dokumentasikan persetujuan pimpinan dan surat tugas sebelum kegiatan lapangan dimulai.

2. Standar instrumen pendataan dan format dokumentasi Gunakan **instrumen baku** untuk mencatat atribut perangkat dan aplikasi (merk, model, OS, versi, lokasi penggunaan, pemilik, status patch, umur perangkat) serta format penilaian kerentanan yang terstandar. Tentukan format file dan struktur basis data yang konsisten agar mudah diintegrasikan ke sistem manajemen keamanan informasi. Sertakan kolom rekomendasi tindakan (peremajaan, patching, mitigasi) dan prioritas risiko untuk setiap entri.

3. Prosedur pelaksanaan pendataan dan identifikasi kerentanan Jalankan workflow terurut: sosialisasi ke unit → pengisian instrumen oleh pengguna → verifikasi lapangan oleh tim teknis → analisis kerentanan → input ke sistem dokumentasi. Terapkan validasi dua tahap (cek lapangan dan review admin) sebelum data dinyatakan final. Pastikan dokumentasi bukti (foto perangkat, screenshot versi, log update) disimpan untuk audit dan tindak lanjut.

4. Pengamanan data, monitoring, dan tindak lanjut Atur **hak akses berbasis peran** pada sistem data, aktifkan logging aktivitas, dan terapkan kebijakan backup berkala untuk mencegah kehilangan data. Tetapkan indikator keberhasilan (persentase perangkat terdokumentasi, jumlah kerentanan tertangani, waktu respons) dan jadwalkan monitoring serta evaluasi berkala. Susun rencana tindak lanjut termasuk rekomendasi pengadaan, jadwal patching, dan program pelatihan untuk meningkatkan kesadaran pegawai terhadap praktik keamanan informasi.