



**PEMERINTAH
KABUPATEN BANGKA**

PEDOMAN TEKNIS INOVASI

PENDEKAR

**PENINGKATAN EDUKASI KEAMANAN SIBER MELALUI PEMBUATAN KONTEN DI MEDIA SOSIAL
DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KABUPATEN BANGKA**



**DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK
KABUPATEN BANGKA**

A. Latar Belakang

Perkembangan teknologi informasi yang semakin pesat menuntut instansi pemerintah untuk mampu mengelola sistem informasi secara aman, efektif, dan terstruktur. Penggunaan perangkat keras dan perangkat lunak yang terus berkembang di lingkungan instansi juga meningkatkan potensi risiko terhadap keamanan informasi apabila tidak dikelola dengan baik. Oleh karena itu, diperlukan suatu sistem pengelolaan perangkat dan aplikasi yang terdata secara jelas sehingga dapat mendukung penerapan keamanan informasi di organisasi. Pada praktiknya, masih ditemukan permasalahan dalam pengelolaan perangkat teknologi informasi di instansi, seperti belum tersedianya data yang lengkap mengenai perangkat yang digunakan, belum adanya instrumen pendataan yang terstandar, serta kurangnya dokumentasi mengenai kondisi perangkat dan aplikasi yang digunakan. Hal ini dapat menyebabkan kesulitan dalam melakukan pemantauan, pemeliharaan, maupun identifikasi potensi kerentanan terhadap sistem informasi yang digunakan oleh organisasi.

Untuk mengatasi permasalahan tersebut, diperlukan upaya penyusunan instrumen pendataan perangkat keras dan perangkat lunak yang digunakan oleh instansi. Instrumen ini bertujuan untuk mempermudah proses identifikasi, pendataan, serta pemantauan terhadap perangkat teknologi informasi yang ada. Dengan adanya data yang terstruktur dan terdokumentasi dengan baik, instansi dapat mengetahui kondisi perangkat yang digunakan serta potensi risiko keamanan yang mungkin muncul. Kegiatan aktualisasi ini dilakukan melalui penyusunan instrumen pendataan perangkat dan aplikasi sebagai bagian dari upaya mendukung penerapan Sistem Manajemen Keamanan Informasi (SMKI). Melalui kegiatan ini diharapkan tersedia data yang akurat mengenai perangkat yang digunakan sehingga dapat menjadi dasar dalam pengelolaan keamanan informasi yang lebih baik. Dengan demikian, pengelolaan teknologi informasi di instansi dapat berjalan lebih efektif, terorganisir, serta mendukung peningkatan kualitas tata kelola keamanan informasi di lingkungan organisasi.

B. Penjaringan Ide Inovasi

Dilakukan melalui observasi lapangan, pendataan, dan focus Group Discussion melibatkan pemangku kepentingan yaitu Pemerintah Kabupaten Bangka, Dinas Komunikasi, Informatika Dan Statistik 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 Peningkatan Edukasi Keamanan Siber Melalui Pembuatan Konten Di Media Sosial Dinas Komunikasi, Informatika Dan Statistik Kabupaten Bangka Dilakukan Berdasarkan Hasil Observasi Lapangan, Pendataan, Dan Diskusi Bersama Pemangku Kepentingan Terkait . Dipilih gagasan untuk menyusun instrumen pendataan perangkat dan aplikasi sebagai solusi terhadap permasalahan yang ada. Ide ini dipilih karena dinilai paling relevan dengan tugas dan fungsi unit kerja serta dapat memberikan kontribusi nyata dalam meningkatkan pengelolaan teknologi informasi dan keamanan informasi di instansi.

D. Tujuan Inovasi

Tujuan dari kegiatan aktualisasi ini adalah untuk menyusun instrumen pendataan perangkat keras dan perangkat lunak yang digunakan di instansi sebagai dasar dalam pengelolaan dan pemantauan perangkat teknologi informasi serta mendukung penerapan Sistem Manajemen Keamanan Informasi (SMKI).

E. Manfaat Inovasi

Kegiatan aktualisasi ini memberikan manfaat berupa tersedianya instrumen pendataan perangkat dan aplikasi yang dapat digunakan sebagai acuan dalam melakukan identifikasi, pencatatan, serta pemantauan perangkat teknologi informasi di instansi sehingga mempermudah proses pengelolaan perangkat, meningkatkan kesadaran terhadap pentingnya keamanan informasi, serta mendukung penerapan Sistem Manajemen Keamanan Informasi (SMKI) secara lebih terstruktur dan sistematis.

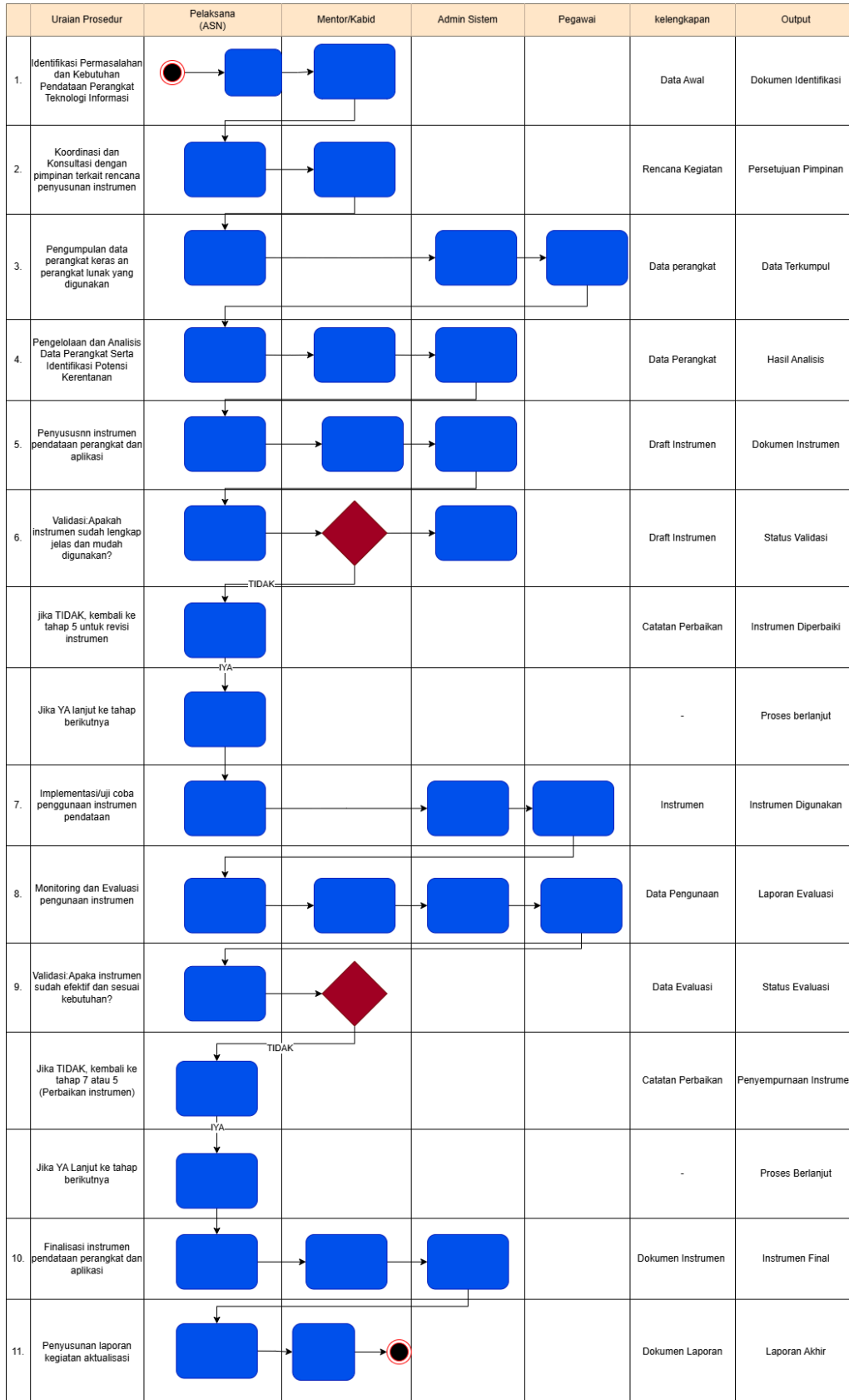
F. Hasil

Hasil yang diharapkan dari kegiatan aktualisasi ini adalah tersusunnya instrumen pendataan perangkat dan aplikasi, tercatatnya kondisi perangkat keras dan perangkat lunak yang digunakan di instansi, tersedianya data mengenai potensi kerentanan perangkat sebagai dasar dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI), serta meningkatnya kesadaran organisasi terhadap pentingnya pengelolaan keamanan informasi.

G. Tahapan Kegiatan

Tahapan	Kegiatan	Waktu Pelaksanaan
Persiapan	Pengumpulan data perangkat dan identifikasi permasalahan pengelolaan perangkat	1–31 Januari 2025
Pengumpulan Data	Pendataan perangkat keras dan perangkat lunak yang digunakan	1–28 Februari 2025
Pengolahan Data	Analisis data perangkat dan identifikasi potensi kerentanan	1–31 Maret 2025
Penyusunan Instrumen	Penyusunan format instrumen pendataan perangkat dan aplikasi	1–30 April 2025
Implementasi & Penyempurnaan	Uji penggunaan instrumen serta penyempurnaan dokumen	1–31 Mei 2025
Pelaporan	Penyusunan laporan hasil kegiatan aktualisasi	1–30 Juni 2025

H. SOP



Pedoman teknis inovasi — PENDEKAR (Edukasi Keamanan Siber)

1. Pembentukan tim dan ruang lingkup kegiatan Bentuk **Tim Edukasi Siber** yang melibatkan Koordinator Konten (Diskominfo), Pengembang Konten (penulis/desainer), Admin Media Sosial, dan Narasumber Teknis (tim keamanan informasi). Tetapkan ruang lingkup materi (phishing, kata sandi kuat, pembaruan perangkat lunak, proteksi data pribadi), target audiens (ASN, pelajar, UMKM), jadwal publikasi, dan mekanisme eskalasi untuk pertanyaan teknis. Semua penugasan didokumentasikan dalam SK dan rencana kerja triwulanan.

2. Standar konten dan spesifikasi teknis produksi Gunakan format konten baku: *ringkasan pesan (1–2 kalimat) → poin tindakan (3–5 langkah) → visual pendukung (infografis/video ≤60 detik) → tautan rujukan*. Terapkan pedoman teknis (resolusi gambar, subtitle video, ukuran file) dan gaya bahasa sederhana agar mudah dipahami. Sertakan checklist validasi fakta dan izin penggunaan materi sebelum publikasi.

3. Alur produksi, publikasi, dan moderasi Terapkan workflow terstruktur: pengumpulan bahan → pembuatan draft → validasi teknis oleh narasumber → desain → penjadwalan publikasi → monitoring respons. Gunakan kalender konten bersama dan label/penandaan untuk status (draft, review, terbit). Tetapkan prosedur moderasi komentar, penanganan hoaks, dan rujukan ke kanal resmi bila diperlukan; simpan arsip konten dan log keputusan untuk audit.

4. Monitoring, evaluasi, dan keberlanjutan Tetapkan indikator kinerja (jangkauan, engagement, tingkat pemahaman melalui kuis singkat, jumlah laporan insiden yang berkurang) dan lakukan monitoring berkala. Kumpulkan umpan balik pengguna untuk perbaikan konten dan jadwalkan pelatihan internal bagi tim setiap 3–6 bulan. Rencanakan mekanisme pembaruan materi sesuai perkembangan ancaman siber dan dokumentasikan SOP final agar dapat direplikasi di unit lain.