LAPORAN GAGASAN KELITBANGAN

Periode - Juni 2025

JUDUL

"Strategi Keamanan Digital untuk Menjaga Reputasi Pelayanan Publik Digital di Kabupaten Klungkung"

Fokus Strategis

Bidang Komunikasi dan Informatika

Tim Ahli

Prof. Dr. Ir. I Made Oka Widyantara, S.T., M.T., IPU., ASEAN Eng.

Tenaga Ahli Bidang Teknologi Informatika

Badan Riset dan Inovasi Daerah

Kabupaten Klungkung

Jl. Kartini No.33 Semarapura _ brida@klungkungkab.go.id _ https://sadarindah.sbm-app.id/

Latar belakang-Transformasi digital pelayanan publik adalah agenda nasional yang diturunkan ke daerah melalui kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE). Kabupaten Klungkung telah menunjukkan komitmen kuat melalui berbagai inisiatif digital seperti peluncuran aplikasi “Klungkung Dalam Genggaman”, integrasi single-sign-on OPD, serta penerapan transaksi non-tunai untuk pembayaran retribusi dan pajak daerah. Semua inovasi ini menjadikan website www.klungkungkab.go.id sebagai digital gateway utama yang menghubungkan masyarakat dengan sistem birokrasi pemerintahan yang semakin terotomatisasi dan berbasis data.

Dalam konteks ini, keandalan website tidak lagi bersifat teknis semata, melainkan telah menjadi simbol keandalan layanan publik itu sendiri. Bila website mengalami gangguan, maka masyarakat tidak hanya menghadapi masalah teknis, melainkan kehilangan akses terhadap berbagai layanan penting seperti pendaftaran izin usaha, konsultasi layanan kesehatan, pelaporan pengaduan publik, hingga transparansi anggaran. Dengan kata lain, website adalah wajah digital pemerintah—dan kualitas pelayanan daring kini sangat bergantung pada performa, keamanan, dan ketersediaan (availability) dari situs tersebut.

Namun demikian, fakta menunjukkan bahwa website www.klungkungkab.go.id dan sub-domain terkait beberapa kali mengalami serangan peretasan sepanjang 2024–2025. Mulai dari insiden defacement, pengalihan DNS, penyisipan web-shell, hingga potensi kebocoran data di layanan e-Surat dan RS Gema Santi. Serangan ini menunjukkan bahwa seiring dengan meningkatnya adopsi teknologi digital di sektor publik, permukaan serangan (attack surface) pun semakin meluas dan kompleks. Ancaman ini tidak dapat dianggap insidental,

melainkan sebagai dampak langsung dari belum optimalnya penerapan arsitektur keamanan yang berlapis (layered security), serta belum adanya sistem manajemen keamanan informasi yang terintegrasi.

Kerentanan website ini menjadi ancaman serius bagi reputasi digitalisasi pelayanan publik Kabupaten Klungkung. Di era digital trust, masyarakat menuntut bahwa semua kanal daring pemerintah harus dapat diakses secara aman, stabil, dan berkelanjutan. Sekali terjadi insiden peretasan, kredibilitas pemerintah dapat menurun drastis, bahkan memicu ketidakpercayaan terhadap transformasi digital yang sedang dibangun. Hal ini akan menghambat akselerasi program-program unggulan seperti Smart Governance, Smart Health, hingga layanan publik berbasis aplikasi.

Oleh karena itu, diperlukan strategi keamanan digital yang bersifat teknis sekaligus kebijakan. Dari sisi teknis, Pemkab Klungkung perlu segera membangun infrastruktur keamanan siber berbasis zero-trust, menerapkan Web Application Firewall (WAF), SIEM (Security Information and Event Management), MFA (Multi-Factor Authentication), serta melakukan audit kerentanan berkala. Dari sisi kebijakan, pemerintah perlu menetapkan standar minimum anggaran keamanan TI di setiap OPD, memperkuat peran CSIRT Daerah, serta mengintegrasikan indikator keamanan SPBE dalam evaluasi kinerja pimpinan perangkat daerah.

Keterpaduan antara strategi teknis dan kebijakan ini tidak hanya akan mengurangi risiko insiden di masa depan, tetapi juga menjaga reputasi Pemkab Klungkung sebagai daerah yang siap bertransformasi digital dengan mengedepankan prinsip secure by design. Kepercayaan publik terhadap layanan digital hanya bisa dibangun di atas fondasi keamanan yang andal dan tata kelola yang kuat.

I. Maksud dan Tujuan

Maksud

Kajian ini dimaksudkan untuk merumuskan strategi inovasi penguatan keamanan website Pemerintah Kabupaten Klungkung (www.klungkungkab.go.id) sebagai bagian dari upaya mendukung transformasi digital pelayanan publik yang andal, aman, dan berkelanjutan. Dengan meningkatnya frekuensi dan kompleksitas serangan siber yang menargetkan sistem digital pemerintah daerah, kajian ini bertujuan mengembangkan solusi teknis dan tata kelola yang dapat meningkatkan ketahanan website terhadap ancaman, menjaga reputasi layanan publik digital, serta memperkuat kepercayaan masyarakat terhadap penyelenggaraan pemerintahan berbasis elektronik.

Tujuan

Secara khusus, kajian ini bertujuan untuk:

1. Mengidentifikasi dan menganalisis bentuk-bentuk kerentanan pada website dan sub-domain milik Pemerintah Kabupaten Klungkung yang dapat dimanfaatkan oleh pelaku peretasan.
2. Mengevaluasi insiden-insiden keamanan siber yang telah terjadi pada sistem digital Pemkab Klungkung sebagai pembelajaran dan dasar penetapan prioritas penguatan.
3. Merumuskan strategi teknis

pengamanan website secara menyeluruh, meliputi penggunaan Web Application Firewall (WAF), deteksi dan respons insiden (SIEM), hardening server, MFA, serta sistem backup dan pemulihan data.
4. Mengembangkan kerangka kebijakan dan tata kelola keamanan digital, seperti penguatan peran CSIRT Daerah, penyusunan SOP respons insiden, serta pengintegrasian keamanan informasi dalam indikator kinerja OPD.
5. Menyediakan rekomendasi program inovasi BRIDA untuk menjadi rujukan dalam pengambilan keputusan, penganggaran, serta pelaksanaan transformasi digital yang aman dan berkelanjutan di Kabupaten Klungkung.
6. Menjaga dan meningkatkan reputasi digital Pemerintah Kabupaten Klungkung agar tetap dipercaya oleh masyarakat, mitra strategis, serta lembaga nasional sebagai penyelenggara layanan publik berbasis digital yang profesional dan aman.

II. Ide dan Gagasan

Dalam upaya memperkuat transformasi digital di sektor pelayanan publik, Kabupaten Klungkung menghadapi tantangan nyata berupa meningkatnya risiko serangan siber yang menargetkan sistem website pemerintahan. Kejadian peretasan pada domain utama www.klungkungkab.go.id dan subdomain layanan strategis seperti e-surat, RS Gema Santi, dan PAD, menunjukkan bahwa keandalan website kini tidak dapat dipisahkan dari kepercayaan publik terhadap kinerja pemerintah daerah.

Untuk itu, diperlukan sebuah pendekatan inovatif yang mampu menjawab ancaman tersebut secara menyeluruh, namun tetap realistis untuk diterapkan di tingkat daerah. Gagasan yang ditawarkan dalam kajian ini adalah pembangunan program KAWAL-WEB (Keamanan Website Layanan Klungkung), sebuah strategi terintegrasi untuk meningkatkan ketahanan siber website pemerintah Kabupaten Klungkung melalui pendekatan teknis, kelembagaan, regulatif, dan partisipatif.

Program ini dibangun di atas enam pilar utama yang saling mendukung dan dapat diimplementasikan secara bertahap, dengan melibatkan peran aktif ASN, OPD, komunitas IT lokal, akademisi, dan pemangku kepentingan eksternal. Berikut penjelasan rinci dari masing-masing pilar:

PILAR 1: Audit Keamanan Dasar Website Pemerintah Daerah

Audit keamanan merupakan langkah awal yang fundamental dalam membangun ketahanan digital. Pilar pertama ini bertujuan untuk mendeteksi secara dini berbagai celah keamanan yang ada pada website utama www.klungkungkab.go.id serta seluruh subdomain strategisnya. Audit dilakukan dengan memanfaatkan perangkat lunak legal dan gratis (open-source) seperti OWASP ZAP, WPScan, dan Nikto, yang dapat mengidentifikasi kelemahan sistem seperti plugin usang, form input yang tidak tervalidasi, konfigurasi server tidak aman, serta potensi kebocoran direktori. Dalam pelaksanaannya, Pemerintah Kabupaten Klungkung melalui Diskominfo dapat menjalin kemitraan dengan perguruan tinggi lokal seperti Universitas Udayana, Institut Teknologi dan Bisnis (INSTIKI) Indonesia atau Universitas Pendidikan Ganesha, serta komunitas profesional TI untuk menyediakan pendampingan teknis dan memvalidasi hasil audit secara independen. Pendekatan kolaboratif ini sekaligus membuka ruang bagi mahasiswa magang atau tugas akhir

yang berbasis studi kasus riil.

Alur Proses:

1. Inventarisasi semua domain dan subdomain website Pemkab Klungkung. Instalasi dan konfigurasi tools audit pada perangkat uji (laptop/server).
2. Pelaksanaan audit keamanan oleh tim internal dengan pendampingan kampus/komunitas TI.
3. Penyusunan laporan hasil temuan dan rekomendasi teknis per subdomain.
4. Presentasi hasil dan rencana tindak lanjut kepada Diskominfo, BRIDA, dan OPD terkait.

PILAR 2: Pemasangan Web Application Firewall (WAF)

Untuk memberikan perlindungan aktif terhadap ancaman eksternal, pemasangan Web Application Firewall (WAF) menjadi pilar kedua dalam inovasi ini. WAF berfungsi sebagai penyaring lalu lintas internet yang masuk ke sistem web, secara otomatis memblokir serangan seperti SQL Injection, Cross-Site Scripting (XSS), dan brute force login. Pemerintah daerah dapat memanfaatkan solusi WAF berbasis open-source seperti ModSecurity untuk server lokal, atau layanan berbasis cloud seperti Cloudflare WAF versi gratis untuk domain utama. Kolaborasi dengan profesional TI atau vendor lokal diundang untuk asistensi instalasi dan pelatihan teknis. Sementara akademisi dapat dilibatkan dalam uji coba dan simulasi penetrasi setelah WAF diaktifkan, guna memastikan efektivitas proteksi terhadap ancaman nyata.

Alur Proses:

1. Penentuan subdomain prioritas yang akan diamankan dengan WAF.
2. Instalasi dan konfigurasi WAF (ModSecurity/Cloudflare) pada server web.
3. Pengujian simulasi serangan untuk mengukur efektivitas filter.
4. Pelatihan admin web OPD dalam membaca log dan mengatur aturan WAF.
5. Evaluasi kinerja WAF dan penguatan konfigurasi berdasarkan pola serangan yang terdeteksi.

PILAR 3: Penerapan Autentikasi Ganda dan Pembatasan Akses Admin

Pilar ketiga berfokus pada perlindungan akses ke sistem administrasi website. Banyak serangan terjadi bukan karena kelemahan teknis server, tetapi akibat kredensial admin yang mudah ditebak, dibagikan tanpa kontrol, atau tidak diamankan dengan otentikasi ganda. Oleh karena itu, seluruh akun administrator yang mengelola sistem web Pemkab Klungkung wajib diintegrasikan dengan Two-Factor Authentication (2FA), rotasi password berkala, dan pembatasan hak akses berbasis peran. Pelaksanaan teknis dilakukan oleh Diskominfo dengan pendampingan profesional keamanan TI, sedangkan dokumen kebijakan dan SOP akses dapat dikembangkan bersama akademisi bidang manajemen sistem informasi dari kampus mitra.

Alur Proses:

1. Audit dan verifikasi seluruh akun administrator subdomain.
2. Instalasi dan aktivasi fitur 2FA pada CMS dan panel server.
3. Penyesuaian hak akses (role-based access control) dan pembatasan admin.
4. Penyusunan dan sosialisasi SOP pengelolaan akses akun.
5. Pelatihan penggunaan 2FA dan praktik keamanan akun kepada pengelola sistem.

PILAR 4: Penyusunan SOP Respons Insiden dan Pelatihan ASN

Kemampuan teknis saja tidak cukup jika tidak dibarengi dengan kesiapan prosedural. Pilar ini mendorong penyusunan dokumen Standar Operasional Prosedur (SOP) Tanggap Insiden Siber, yang memuat langkah-langkah sistematis saat website mengalami serangan atau gangguan. SOP ini harus menjadi rujukan semua OPD, disusun oleh tim lintas instansi dengan melibatkan BRIDA, Diskominfo, dan didampingi oleh akademisi bidang tata kelola TI atau manajemen risiko. Setelah SOP tersusun, dilakukan pelatihan kepada ASN pengelola aplikasi dan web untuk membangun pemahaman kolektif, disertai simulasi insiden atau table-top exercise minimal dua kali setahun.

Alur Proses:

1. Pembentukan tim penyusun SOP lintas OPD dan BRIDA.
2. Drafting SOP berdasarkan referensi BSSN dan ISO/IEC 27035.
3. Simulasi skenario serangan (deface, DDoS, data breach) sebagai uji SOP.
4. Revisi SOP berdasarkan hasil evaluasi simulasi.
5. Pelatihan dan sosialisasi SOP ke seluruh OPD pengelola sistem digital.

PILAR 5: Pembentukan Mini-CSIRT (Computer Security Incident Response Team)

Untuk menjamin keberlanjutan keamanan digital, diperlukan struktur organisasi yang memiliki mandat dan kompetensi khusus dalam merespons dan mengoordinasikan insiden keamanan. Oleh karena itu, dibentuk unit Mini-CSIRT di bawah koordinasi Diskominfo, yang terdiri dari tim teknis internal, perwakilan BRIDA, serta admin sistem dari OPD kunci. Tim ini bertugas mengelola insiden siber, melakukan pelaporan rutin, memantau tren ancaman, dan menjadi penghubung dengan CSIRT Provinsi maupun Nasional (BSSN). Untuk penguatan kapasitas, Mini-CSIRT juga dapat bermitra dengan konsultan keamanan TI atau kampus penyedia laboratorium keamanan siber, guna mendapatkan pembinaan teknis dan peluang capacity building lanjutan.

Alur Proses:

1. Penyusunan SK pembentukan Mini-CSIRT dan penunjukan anggota tetap.
2. Definisi peran, tugas, dan alur kerja internal tim.
3. Pengembangan sistem pelaporan insiden (dashboard atau form elektronik).
4. Pelatihan teknis lanjutan dari mitra eksternal (kampus/komunitas IT).
5. Penyusunan laporan triwulan dan evaluasi kinerja keamanan digital daerah.

PILAR 6: Pengaktifan Tim Koordinasi SPBE dan Penyusunan Regulasi Daerah tentang Keamanan Informasi

Keberhasilan transformasi digital dan perlindungan sistem informasi pemerintah tidak hanya bertumpu pada solusi teknis, namun juga harus ditopang oleh struktur kelembagaan yang aktif dan regulasi daerah yang jelas. Oleh karena itu, Pilar 6 dalam program KAWAL-WEB menekankan pentingnya mengaktifkan kembali peran Tim Koordinasi SPBE Kabupaten Klungkung yang selama ini cenderung pasif, serta mendorong penyusunan Peraturan Bupati atau Peraturan Daerah yang secara khusus mengatur sistem manajemen keamanan informasi (SMKI) di lingkungan pemerintah daerah.

Tim Koordinasi SPBE memiliki peran

strategis sebagai wadah sinergi lintas perangkat daerah dalam merencanakan, memantau, dan mengevaluasi penerapan kebijakan SPBE, termasuk aspek keamanan siber. Pengaktifan tim ini akan memberikan legitimasi terhadap implementasi program KAWAL-WEB dan menjamin bahwa keamanan website menjadi bagian dari pengelolaan SPBE secara menyeluruh. Di sisi lain, dengan adanya regulasi daerah yang memuat standar teknis, prosedur, dan kewajiban setiap OPD dalam menjaga keamanan informasi, maka keberlanjutan program dapat terjamin, termasuk dalam hal penganggaran, pengawasan, dan integrasi indikator dalam kinerja birokrasi.

Untuk mewujudkan hal tersebut, Pemerintah Kabupaten Klungkung dapat bekerja sama dengan akademisi bidang hukum dan kebijakan publik, serta melibatkan BRIDA dan Bagian Hukum Setda dalam penyusunan regulasi yang mengacu pada Peraturan BSSN No. 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE, serta SNI ISO/IEC 27001. Regulasi ini tidak harus langsung berbentuk Perda; dapat dimulai dari Peraturan Bupati (Perbup) sebagai regulasi teknis pelaksanaan kebijakan SPBE.

Alur Proses:

1. Identifikasi status terkini Tim Koordinasi SPBE dan penetapan ulang keanggotaannya melalui SK Bupati yang baru (jika diperlukan).
2. Pengaktifan pertemuan rutin Tim Koordinasi SPBE, minimal dua kali dalam setahun, dengan agenda khusus membahas integrasi keamanan informasi dalam program digitalisasi OPD.
3. Penyusunan naskah akademik dan draft awal Perbup/Perda tentang Manajemen Keamanan Informasi Daerah.
4. Konsultasi publik dan FGD bersama perwakilan OPD, Diskominfo, BRIDA, CSIRT, dan akademisi.
5. Pengesahan dan sosialisasi regulasi, diikuti dengan integrasi indikator keamanan informasi ke dalam sistem evaluasi kinerja SPBE dan perencanaan tahunan OPD.

Dengan keenam pilar tersebut, KAWAL-WEB tidak hanya memberikan solusi teknis untuk mencegah peretasan website pemerintah, tetapi juga membentuk struktur kelembagaan dan kebijakan yang mendukung keberlanjutan transformasi digital. Pendekatan ini akan menjadikan Kabupaten Klungkung sebagai pelopor daerah dengan sistem keamanan informasi yang tangguh, kolaboratif, dan berbasis inovasi.

III. Rekomendasi

Berdasarkan analisis kerentanan, kebutuhan kelembagaan, dan potensi strategi penguatan sistem keamanan informasi yang telah dirumuskan dalam enam pilar program KAWAL-WEB, maka berikut adalah rekomendasi yang diajukan untuk Pemerintah Kabupaten Klungkung guna mendukung keberhasilan implementasi inovasi ini secara terintegrasi dan berkelanjutan:

1. **Penetapan Program KAWAL-WEB sebagai Program Prioritas Daerah**. Pemerintah Kabupaten Klungkung melalui BRIDA dan Diskominfo disarankan menetapkan program KAWAL-WEB sebagai bagian dari prioritas inovasi daerah dalam dokumen perencanaan (Renstra, Renja, RKPD), serta mengintegrasikannya ke dalam strategi transformasi digital dan penguatan SPBE di lingkup OPD.

2. **Penguatan Kapasitas Teknis dan SDM Melalui Kolaborasi Multi-Pihak**. Diperlukan kerja sama aktif dengan mitra eksternal seperti perguruan tinggi lokal (Unud, Undiksa, INSTIKI Indonesia), komunitas profesional TI (ID-CERT, APJII Bali), dan praktisi keamanan informasi untuk mendampingi pelaksanaan audit, pelatihan, dan pemantauan sistem keamanan web. Kolaborasi ini juga menciptakan ekosistem pengembangan talenta lokal di bidang keamanan siber.
3. **Pemberlakuan Kebijakan Teknis Keamanan Informasi di Tingkat OPD.** Setiap OPD yang mengelola sistem berbasis web atau subdomain harus menerapkan kebijakan teknis minimum seperti: penggunaan 2FA, manajemen akun admin, SOP tanggap insiden, dan pencadangan sistem berkala. Diskominfo bertindak sebagai focal point dalam menyusun dan memantau pelaksanaan kebijakan ini.
4. **Aktivasi Tim Koordinasi SPBE dan Pembentukan Mini-CSIRT**. Pemerintah perlu mengaktifkan kembali Tim Koordinasi SPBE dan membentuk Mini-CSIRT Kabupaten Klungkung dengan penugasan yang jelas, struktur koordinatif, dan pelatihan teknis yang terjadwal. Tim ini akan menjadi tulang punggung penanganan insiden keamanan informasi lintas OPD.
5. **Penyusunan dan Pengesahan Regulasi Daerah tentang Keamanan Informasi**. Dianjurkan untuk menyusun dan mengesahkan Peraturan Bupati (Perbup) atau Peraturan Daerah (Perda) mengenai Sistem Manajemen Keamanan Informasi Daerah, sebagai payung hukum bagi seluruh aktivitas pengamanan website, pembentukan CSIRT, penggunaan anggaran pengamanan TIK, serta evaluasi kinerja SPBE berbasis risiko siber.
6. **Penyediaan Anggaran Khusus untuk Keamanan Digital dalam APBD.** Alokasi anggaran yang memadai untuk belanja keamanan TIK perlu dimasukkan secara khusus dalam dokumen perencanaan anggaran OPD terkait (Diskominfo, BRIDA, dan OPD pengelola aplikasi kritikal), termasuk untuk biaya audit, pelatihan, langganan sistem WAF, dan pengembangan sistem pelaporan insiden.
7. **Monitoring dan Evaluasi Berkala atas Implementasi Enam Pilar KAWAL-WEB**. Setiap pilar dalam program KAWAL-WEB harus memiliki indikator keberhasilan (KPI) yang terukur dan dilaporkan secara berkala kepada Bupati melalui Tim Koordinasi SPBE. Evaluasi dilakukan setiap triwulan, dengan penyesuaian strategi berdasarkan hasil audit dan log insiden yang terjadi.

Semarapura, 12 Juni 2025
Disahkan oleh:

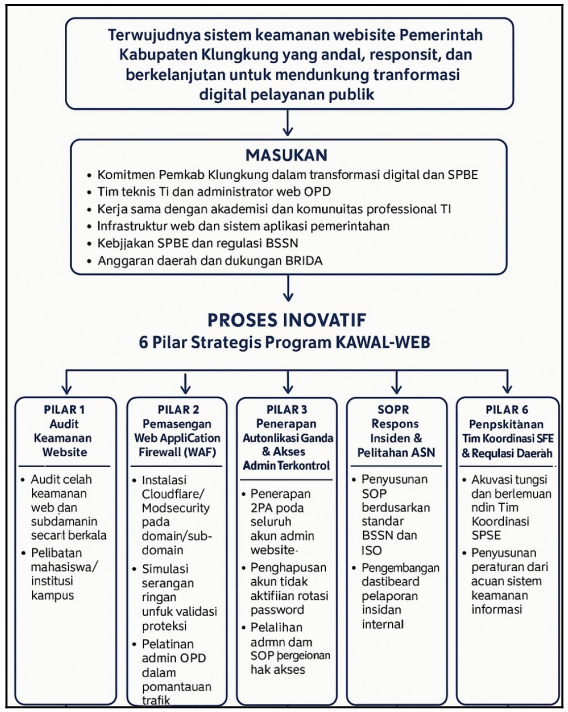
Kepala Badan Riset
dan Inovasi Daerah
Kabupaten Klungkung

IV. Kegiatan Kelompok Ahli

No.	Nama Kegiatan	Hari/Tgl	Lokasi Kegiatan	Materi Kegiatan	Isi Bahasan	Simpulan dan Saran
1.	Sosialisasi Rencana Penangan Pantai Nusa Penida dan Nusa Lembongan	Kamis/15 Mei 2025	Praja Mandala Kabupaten Klungkung	Desain penangan pantai oleh konsultan NIPPON KOEI	Materi paparan: • Identifkasi kerusakan dan perubahan garis pantai Nusa Lembongan dan Nusa Penida • Karakteristik Gelombang • Layout penanganan • Desain rinci penanganan • Penataan kawasan • Tim koordinasi manajemen pengelolaan pantai (TKMPP)	Saran dan Pertimbangan: • Gunakan kombinasi soft structure (pengisian pasir, vegetasi pantai) dan hard structure (revetment, groin) agar tercapai keseimbangan antara perlindungan fisik dan estetika alam. • Gunakan batu armor dan pasir yang memenuhi standar mutu, serta cocok dengan kondisi lokal untuk menghindari degradasi lingkungan. • Perlu revisi atau penguatan Perda/RTRW yang menetapkan zona konservasi, zona infrastruktur wisata, dan zona publik, untuk mencegah pembangunan liar di sempadan pantai. P • enanganan di zona-zona seperti Pura Batu Mas Kuning harus memperhatikan nilai sakral dan akses umat, serta tidak mengganggu integritas struktur pura. P • astikan pembangunan pesisir selaras dengan upaya rehabilitasi ekosistem bawah laut (terumbu karang) dan hutan mangrove, terutama di wilayah Nusa Lembongan.

No.	Nama Kegiatan	Hari/Tgl	Lokasi Kegiatan	Materi Kegiatan	Isi Bahasan	Simpulan dan Saran
2.	Persampahan Kabupaten Klungkung	Jumat/16 Mei 2025	BRIDA Kabupaten Klungkung	Rekomendasi Tindak Lanjut kajian Tiiping Fee	Rekomendasi teknis dari BRIDA terkait surat permohonan kajian Tipping Fee pengelolaan sampah di TOSS Center dengan investor dengan skema KPBU	Tahapan Kerjasama KPBU Atas Prakarsa Badan Usaha (Unsolicited) Skema unsolicited adalah KPBU yang diusulkan oleh badan usaha swasta, bukan berasal dari daftar proyek pemerintah. Pemerintah dapat menyetujui usulan ini jika proyek dinilai layak dan bermanfaat bagi publik. 1. Pengajuan Usulan oleh Badan Usaha 2. Penilaian Awal oleh Penanggung Jawab Proyek Kerja Sama (PJPK) 3. Penyusunan Dokumen Studi Kelayakan 4. Penetapan sebagai Usulan yang Layak 5. Pelelangan Proyek KPBU 6. Penunjukan Badan Usaha Pelaksana 7. Penandatanganan Perjanjian KPBU 8. Konstruksi dan Operasional 9. Monitoring dan Evaluasi

V. Lampiran


Terwujudnya sistem keamanan webisite Pemerintah Kabupaten Klungkung yang andal, responsit, dan berkelanjutan untuk mendunkung tranformasi digital pelayanan publik
MASUKAN
• Komitmen Pemkab Klungkung dalam transformasi digital dan SPBE
• Tim teknis Ti dan administrator web OPD
• Kerja sama dengan akademisi dan komunuitas professional TI
• Infrastruktur web dan sistem aplikasi pemerintahan
• Kebjjakan SPBE dan regulasi BSSN
• Anggaran daerah dan dukungan BRIDA
PROSES INOVATIF
6 Pilar Strategis Program KAWAL-WEB
PILAR 1 Audit Keamanan Website
• Audit celah keamanan web dan subdamanin secarl berkala
• Pelibatan mahasiswa/ institusi kampus
PILAR 2 Pemasengan Web AppliCation Firewall (WAF)
• Instalasi Cloudflare/ Modsecurity pada domain/sub-domain
• Simulasi serangan ringan unfuk validasi proteksi
• Pelatinan admin OPD dalam pomantauan trafik
PILAR 3 Penerapan Autonlikasi Ganda & Akses Admin Terkontrol
• Penerapan 2PA poda seluruh akun admin website·
• Penghapusan akun tidak aktifiian rotasi password
• Pelalihan admn dam SOP pergeionan hak akses
SOPR Respons Insiden & Pelitahan ASN
• Penyusunan SOP berdusarkan standar BSSN dan ISO
• Pengembangan dastibeard pelaporan insidan internal
PILAR 6 Penpskitànan Tim Koordinasi SFE & Requlasi Daerah
• Akuvasi tungsi dan berlemuan ndin Tim Koordinasi SPSE
• Penyusunan peraturan dari acuan sistem keamanan informasi