



KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 4: Tanggap Insiden Siber

Subtopik 4.4: Peran Tim Tanggap Insiden Siber Klungkung



BUPATI KLUNGKUNG
PROVINSI BALI

KEPUTUSAN BUPATI KLUNGKUNG
NOMOR 272/12/HK/2025

TENTANG

PEMBENTUKAN TIM TANGGAP INSIDEN SIBER - *COMPUTER SECURITY*
INCIDENT RESPONSE TEAM KABUPATEN KLUNGKUNG

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025



KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *“Keamanan Siber untuk ASN dan Masyarakat”* dapat disusun hingga membahas subtopik penting mengenai *Peran Tim Tanggap Insiden Siber (TTIS) Klungkung*. Keberadaan TTIS bukan sekadar formalitas kelembagaan, tetapi menjadi garda depan perlindungan sistem elektronik daerah, termasuk layanan publik berbasis digital. Di era serangan siber yang semakin kompleks dan terotomatisasi, TTIS berfungsi sebagai pengawas, pengendali, dan penangan insiden yang memastikan operasional digital pemerintahan tetap berjalan dengan aman, cepat, dan terkoordinasi.

Melalui subtopik ini, diharapkan ASN dan masyarakat Kabupaten Klungkung mampu memahami bagaimana TTIS Klungkung berperan penting dalam menangani, memitigasi, dan mencegah serangan siber di lingkungan pemerintahan daerah. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa modul ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

KIWA TENGEN

Penyusun



DAFTAR ISI

KATA PENGANTAR	ii
DAFTAR ISI	iii
Tujuan Pembelajaran.....	4
Sasaran Peserta	4
A. Apa Itu TTIS Klungkung?	5
B. Fungsi dan Struktur TTIS Klungkung.....	5
C. Mekanisme Kerja dan Koordinasi TTIS Klungkung	8
D. Layanan dan Kolaborasi TTIS Klungkung (KLUNGKUNG-CSIRT)	10
E. Rekomendasi untuk ASN dan Masyarakat	13
Pertanyaan Reflektif	16
DAFTAR PUSTAKA	17

Tujuan Pembelajaran

Setelah mempelajari subtopik ini, peserta (ASN maupun masyarakat) diharapkan mampu:

1. Menjelaskan pengertian dan fungsi utama Tim Tanggap Insiden Siber (TTIS) Kabupaten Klungkung.
2. Memahami struktur organisasi, tanggung jawab, dan layanan utama TTIS Klungkung.
3. Mengetahui mekanisme koordinasi antara TTIS, perangkat daerah, dan CSIRT nasional.
4. Mengidentifikasi bagaimana ASN dan masyarakat dapat berkolaborasi dalam pencegahan insiden siber.
5. Membangun kesadaran kolektif bahwa keamanan digital merupakan tanggung jawab bersama.

Sasaran Peserta

1. ASN: agar memahami peran strategis TTIS Klungkung dalam menjaga sistem pemerintahan digital, serta mampu berkoordinasi dan melapor dengan benar jika terjadi insiden siber di lingkungan kerja.
2. Masyarakat: agar mengetahui fungsi TTIS Klungkung sebagai kanal resmi penanganan insiden siber daerah dan dapat memanfaatkan layanan ini untuk melaporkan kasus kebocoran data, penipuan digital, atau ancaman keamanan siber lainnya.

A. Apa Itu TTIS Klungkung?

Tim Tanggap Insiden Siber (TTIS) Klungkung adalah unit resmi yang dibentuk berdasarkan **KEPUTUSAN BUPATI KLUNGKUNG NOMOR 272/12/HK/2025 TENTANG PEMBENTUKAN TIM TANGGAP INSIDEN SIBER - *COMPUTER SECURITY INCIDENT RESPONSE TEAM* KABUPATEN KLUNGKUNG**, dengan mandat untuk menangani, mencegah, dan memulihkan insiden siber di lingkungan Pemerintah Kabupaten Klungkung.

TTIS ini juga dikenal secara nasional sebagai **Klungkung-CSIRT (Computer Security Incident Response Team)**, yang menjadi bagian dari ekosistem nasional tanggap insiden siber di bawah koordinasi **Badan Siber dan Sandi Negara (BSSN)**. Tujuan utamanya adalah memastikan sistem elektronik pemerintah daerah, seperti layanan SPBE, administrasi digital, dan data public, terlindungi dari ancaman siber yang dapat mengganggu layanan masyarakat.

B. Fungsi dan Struktur TTIS Klungkung

1. Fungsi Utama TTIS Klungkung

Berdasarkan *Keputusan Bupati Klungkung Nomor 272/12/HK/2025*, TTIS Klungkung memiliki fungsi utama dalam menjaga keamanan sistem elektronik pemerintahan daerah. Fungsi-fungsi tersebut meliputi:

- a. **Memberikan peringatan keamanan siber** kepada instansi atau pihak terkait jika ditemukan ancaman atau serangan siber.
- b. **Merumuskan panduan teknis penanganan insiden siber**, termasuk prosedur pencegahan, mitigasi, dan pemulihan.
- c. **Mencatat setiap laporan atau aduan insiden siber**, serta memberikan rekomendasi langkah penanganan awal kepada pihak terdampak.
- d. **Melakukan pemilahan (triage)** terhadap insiden siber berdasarkan tingkat risiko dan dampaknya.
- e. **Mengkoordinasikan penanganan insiden siber** antar perangkat daerah atau

lembaga yang terlibat.

- f. **Menyebarkan informasi** untuk mencegah atau mengurangi dampak serangan siber di lingkungan Pemerintah Kabupaten Klungkung.

Selain fungsi utama tersebut, TTIS Klungkung juga memiliki **fungsi tambahan** untuk memperkuat kesiapsiagaan siber, yaitu:

- a. **Penanganan kerentanan sistem elektronik**, termasuk pengujian keamanan dan patching.
- b. **Penanganan artefak digital**, seperti bukti serangan dan log sistem.
- c. **Pendeteksian dan analisis risiko keamanan siber.**
- d. **Memberikan konsultasi teknis** kepada perangkat daerah mengenai kesiapan penanganan insiden.

2. Struktur Organisasi TTIS Klungkung

Struktur TTIS Klungkung terdiri dari **Pengarah, Pelaksana, dan Agen Keamanan Siber** di masing-masing perangkat daerah. Struktur ini menjamin bahwa pengawasan dan penanganan insiden dilakukan secara cepat, terkoordinasi, dan akuntabel.

◆ a. Pengarah

Terdiri dari:

Ketua: Bupati Klungkung

Menjamin terselenggaranya pengelolaan penanggulangan dan pemulihan insiden siber, termasuk penyediaan SDM dan anggaran.

Wakil Ketua: Sekretaris Daerah Kabupaten Klungkung

Membantu Ketua dalam memberikan pembinaan dan kebijakan teknis.

Anggota: Asisten Perekonomian dan Pembangunan Sekda

Memberikan masukan teknis dan dukungan operasional kepada tim pelaksana.

◆ b. Pelaksana

Dipimpin oleh **Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung**, yang berperan sebagai **Ketua Pelaksana TTIS**, dengan **Sekretaris Dinas Kominfo** sebagai Sekretaris Tim.



Pelaksana ini membawahi tiga unit teknis utama:

1) Unit Monitoring dan Aksi

Koordinator: Kepala Bidang Telematika

Anggota: Staf Bidang Telematika

Tugas dan Fungsi: Melakukan perencanaan, pengawasan, dan evaluasi terhadap operasional monitoring, tanggap Insiden Siber, dan uji penetrasi sistem.

2) Unit Penanganan Kerentanan

Koordinator: Kepala Bidang Statistik dan Persandian

Anggota: Staf Bidang Statistik dan Persandian

Tugas dan Fungsi: Melakukan perencanaan, pelaksanaan, pengawasan dan evaluasi terhadap penelitian kerentanan, penerimaan laporan kerentanan, analisis kerentanan, koordinasi dan pengungkapan kerentanan, dan respons kerentanan.

3) Unit Pembinaan dan Publikasi

Koordinator: Kepala Bidang Komunikasi

Anggota: Staf Bidang Komunikasi

Tugas dan Fungsi: Melakukan perencanaan, pelaksanaan, pengawasan dan evaluasi terhadap berbagi informasi, peningkatan kesadaran keamanan siber, dan pelatihan keamanan siber.

♦ c. Agen Keamanan Siber

Agen Keamanan Siber merupakan perpanjangan tangan TTIS di **setiap perangkat daerah dan desa/kelurahan** di Kabupaten Klungkung. Mereka bertugas Melakukan monitoring sistem elektronik pada masing-masing perangkat daerah dan melaporkan kejadian insiden siber yang terjadi kepada koordinator. Total terdapat lebih dari **70 agen keamanan siber** dari dinas, badan, kecamatan, dan desa. Agen inilah yang menjadi garda terdepan dalam pelaporan dini dan penanganan insiden secara cepat di tingkat instansi dan desa.

C. Mekanisme Kerja dan Koordinasi TTIS Klungkung

Agar penanganan insiden siber dapat dilakukan cepat, tepat, dan terkoordinasi, TTIS Klungkung memiliki **mekanisme kerja berlapis** sesuai ketentuan dalam *Keputusan Bupati Klungkung Nomor 272/12/HK/2025* dan panduan *Computer Security Incident Response Team (CSIRT) Framework* dari BSSN.

♦ 1. Alur Kerja Umum TTIS Klungkung

Proses kerja TTIS berlangsung dalam empat tahap utama yang saling berkesinambungan:

a. Tahap Deteksi Awal

Setiap perangkat daerah atau agen keamanan siber wajib melaporkan tanda-tanda anomali sistem seperti *phishing*, *malware*, atau akses tidak sah ke TTIS. TTIS melalui Unit Monitoring & Aksi akan melakukan analisis cepat terhadap laporan dan mengidentifikasi potensi ancaman. Jika terbukti ada indikasi serangan, status insiden ditingkatkan menjadi **“terverifikasi”** dan diteruskan ke tahap penanganan.

b. Tahap Penanganan Insiden

TTIS mengisolasi sistem yang terdampak untuk mencegah penyebaran serangan. Melakukan analisis forensik digital dan log jaringan untuk menemukan sumber serangan. Mengambil tindakan pemulihan sementara seperti menonaktifkan akun pengguna, mengganti kata sandi, atau menutup port yang berisiko. Melaporkan kejadian ke **BSSN dan CSIRT Nasional** bila serangan berskala besar atau melibatkan data publik strategis.

c. Tahap Pemulihan Sistem

Setelah sistem aman, TTIS membantu perangkat daerah memulihkan layanan yang terdampak. Melakukan pengujian ulang keamanan sebelum sistem diaktifkan kembali. Mengeluarkan laporan hasil pemulihan dan rekomendasi teknis kepada OPD terkait. Membantu ASN melakukan pembaruan kata sandi

dan memperbaiki prosedur keamanan internal.

d. Tahap Evaluasi dan Pembelajaran

Setiap insiden yang selesai ditangani akan dievaluasi secara internal oleh TTIS. Hasil evaluasi digunakan untuk memperbarui SOP dan meningkatkan literasi keamanan bagi ASN. Jika diperlukan, TTIS akan mengadakan simulasi (drill) bersama OPD terkait agar kesiapsiagaan meningkat.

◆ 2. Mekanisme Koordinasi Internal

Koordinasi internal TTIS dijalankan melalui jalur formal antara:

Ketua TTIS (Kadis Kominfo) → sebagai pengendali utama.

Koordinator Unit Teknis (Bidang Telematika, Statistik, dan Komunikasi) → sebagai pelaksana lapangan.

Agen Keamanan Siber di setiap OPD → sebagai pelapor insiden dan penghubung di tingkat instansi.

Koordinasi dilakukan menggunakan sistem pelaporan daring berbasis *helpdesk* CSIRT yang diintegrasikan ke situs resmi:

 <https://csirtklungkung.klungkungkab.go.id>

Setiap laporan yang masuk akan diverifikasi otomatis oleh petugas piket TTIS dan disalurkan ke unit terkait sesuai kategori ancaman (teknis, data, atau publikasi).

◆ 3. Mekanisme Koordinasi Eksternal

TTIS Klungkung beroperasi dalam jaringan kerja sama nasional dan regional.

Hubungan koordinatif meliputi:

- a. **BSSN (Badan Siber dan Sandi Negara):** sebagai pembina utama nasional dan penyedia sistem peringatan dini nasional (*Indonesia Security Operations Center*).
- b. **CSIRT Nasional:** sebagai pusat eskalasi insiden lintas daerah dan lembaga.
- c. **Diskominfo Provinsi Bali:** sebagai penghubung koordinasi keamanan siber antarkabupaten.
- d. **Lembaga Keamanan dan Penegak Hukum:** seperti Kepolisian RI dan

Kejaksaan Negeri dalam hal penanganan insiden yang berindikasi tindak pidana siber.

- e. Selain itu, TTIS juga menjalin kerja sama dengan **perguruan tinggi dan komunitas keamanan siber** di Bali untuk memperkuat riset dan pelatihan keamanan digital daerah.

◆ 4. Mekanisme Pelaporan Insiden

ASN maupun masyarakat dapat melaporkan insiden melalui:

Portal Resmi TTIS Klungkung: <https://csirtklungkung.klungkungkab.go.id>

Hotline Diskominfo Klungkung: 0366 5551705

Koordinator Agen Siber di masing-masing OPD/desa.

Setiap laporan yang diterima akan diverifikasi dalam waktu maksimal **1×24 jam** dan diberikan tanggapan resmi berupa analisis awal serta rekomendasi tindak lanjut.

D. Layanan dan Kolaborasi TTIS Klungkung (KLUNGKUNG-CSIRT)

◆ 1. Layanan Utama TTIS Klungkung

Berdasarkan *Keputusan Bupati Klungkung Nomor 272/12/HK/2025*, Tim Tanggap Insiden Siber atau **KLUNGKUNG-CSIRT (Computer Security Incident Response Team Kabupaten Klungkung)** memiliki **tiga jenis layanan utama** dalam menjalankan tugasnya, yaitu:

a. Penanggulangan dan Pemulihan Insiden Siber

Layanan ini mencakup seluruh tindakan yang dilakukan ketika terjadi gangguan, serangan, atau kebocoran data di sistem elektronik pemerintah daerah. TTIS bertugas untuk:

- a. Mengidentifikasi, menganalisis, dan menangani insiden yang terjadi.
- b. Mengisolasi sistem terdampak agar serangan tidak menyebar.
- c. Melakukan pemulihan sistem dan data agar layanan publik dapat kembali

berjalan normal.

⚙️ *Tujuannya:* meminimalkan dampak serangan terhadap pelayanan publik serta menjaga kepercayaan masyarakat terhadap sistem digital pemerintah.

b. Penyampaian Informasi Insiden Siber kepada Pihak Terkait

TTIS memiliki tanggung jawab untuk menyampaikan setiap kejadian atau potensi ancaman keamanan siber kepada:

- Perangkat daerah yang terlibat atau terdampak langsung.
- Pihak eksternal yang berwenang, seperti **BSSN** dan **CSIRT Nasional**, bila insiden memiliki dampak lintas instansi.
- Masyarakat, melalui publikasi resmi di situs TTIS, bila diperlukan untuk tujuan kewaspadaan publik.

🕒 *Prinsipnya:* semua informasi insiden disampaikan secara cepat, akurat, dan terverifikasi untuk mendukung penanganan yang terkoordinasi.

c. Diseminasi Informasi Pencegahan dan Edukasi Siber

Selain menangani insiden, TTIS Klungkung juga memberikan **edukasi dan peringatan dini** kepada ASN dan masyarakat mengenai potensi ancaman digital, seperti:

- Peringatan serangan phishing, ransomware, atau kebocoran data.
- Panduan keamanan penggunaan sistem elektronik pemerintah.
- Rekomendasi teknis pencegahan agar kejadian serupa tidak terulang.


📌 *Hasil akhirnya:* meningkatnya kesadaran digital ASN dan masyarakat agar mampu melindungi diri dari ancaman siber yang berkembang.

♦ 2. Fungsi Utama TTIS Klungkung

Selain menyediakan layanan, TTIS Klungkung memiliki **fungsi utama** sebagaimana tercantum dalam Diktum Ketiga *Keputusan Bupati Klungkung Nomor 272/12/HK/2025*, yaitu:

- Pemberian peringatan terkait keamanan siber** di lingkungan Pemerintah Kabupaten Klungkung.


- b. **Perumusan panduan teknis penanganan insiden siber** untuk seluruh perangkat daerah.
- c. **Pencatatan setiap laporan atau aduan insiden siber** serta pemberian rekomendasi penanganan awal.
- d. **Pemilahan (triage) insiden siber**, yaitu mengelompokkan dan memprioritaskan insiden sesuai tingkat risiko.
- e. **Koordinasi antarinstansi** dalam penanganan dan pemulihan insiden.
- f. **Diseminasi informasi keamanan siber**, baik internal (ASN) maupun eksternal (publik), untuk mencegah dan mengurangi dampak insiden.

 *Maknanya:* TTIS tidak hanya bertugas saat terjadi serangan, tetapi juga berperan aktif dalam mempersiapkan sistem agar lebih tangguh terhadap ancaman digital.

◆ 3. Fungsi Pendukung dan Tambahan

Sebagai pelengkap fungsi utama, TTIS Klungkung juga memiliki **fungsi tambahan** yang bersifat teknis dan mendukung kesiapan daerah menghadapi ancaman siber, meliputi:

- a. **Penanganan kerentanan sistem elektronik**, termasuk pengujian keamanan (security testing) dan pembaruan sistem.
- b. **Penanganan artefak digital**, yaitu bukti elektronik dari insiden yang digunakan untuk investigasi atau laporan resmi.
- c. **Pemberitahuan hasil pengamatan potensi ancaman**, baik dari pemantauan internal maupun kerja sama dengan BSSN.
- d. **Pendeteksian serangan dan anomali digital** melalui sistem pemantauan terpusat.
- e. **Analisis risiko keamanan siber** terhadap sistem elektronik pemerintah daerah.
- f. **Konsultasi kesiapan penanganan insiden siber**, termasuk memberikan bimbingan teknis kepada perangkat daerah.

 *Kesimpulannya:* TTIS tidak hanya merespons, tetapi juga membangun sistem pertahanan yang siap siaga dan berkelanjutan.

◆ 4. Konstituen dan Kolaborasi

TTIS Klungkung memiliki **konstituen utama**, yaitu seluruh **perangkat daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Klungkung**.

Dalam pelaksanaan tugasnya, TTIS dapat **berkoordinasi dan bekerja sama** dengan:

- a. Badan Siber dan Sandi Negara (BSSN) sebagai pembina teknis nasional.
- b. CSIRT Nasional dan CSIRT daerah lainnya di Provinsi Bali.
- c. Aparat penegak hukum bila insiden berdampak hukum.
- d. Perguruan tinggi dan komunitas keamanan digital untuk penguatan kapasitas dan riset.

E. Rekomendasi untuk ASN dan Masyarakat

Tim Tanggap Insiden Siber atau **KLUNGKUNG-CSIRT** merupakan langkah strategis Pemerintah Kabupaten Klungkung untuk memperkuat pertahanan digital daerah dan memastikan penyelenggaraan pemerintahan berbasis elektronik (SPBE) berjalan aman serta andal.

Keberadaan TTIS bukan hanya simbol komitmen keamanan, tetapi juga bagian dari sistem kerja terintegrasi yang melibatkan **ASN, perangkat daerah, dan masyarakat**. Melalui fungsi utamanya, **peringatan dini, penanganan insiden, pemulihan, dan diseminasi informasi**, TTIS Klungkung menjadi pusat kendali keamanan siber daerah yang sigap, adaptif, dan kolaboratif.

Dengan dukungan BSSN dan partisipasi aktif seluruh konstituen, TTIS Klungkung diharapkan menjadi model **tanggap insiden siber daerah** yang berkelanjutan dan mampu menumbuhkan budaya aman digital di Kabupaten Klungkung.

1. Rekomendasi untuk ASN

Aparatur Sipil Negara (ASN) memiliki peran kunci dalam menjaga keandalan sistem pemerintahan digital. Untuk itu, ASN diharapkan:

- a. **Melaporkan setiap insiden atau aktivitas mencurigakan** melalui portal resmi <https://csirtklungkung.klungkungkab.go.id>.

- b. **Mengikuti pelatihan keamanan siber** yang diselenggarakan oleh Diskominfo dan TTIS minimal dua kali dalam setahun.
- c. **Menjaga kerahasiaan akun dinas** dan tidak membagikan kredensial kerja kepada rekan atau pihak luar.
- d. **Melakukan pemantauan berkala** terhadap perangkat kerja untuk mencegah potensi penyusupan.
- e. **Mendukung agen keamanan siber di masing-masing OPD**, agar koordinasi dengan TTIS berjalan cepat dan efektif.

💡 *Ingat:* keamanan digital instansi tidak hanya bergantung pada teknologi, tetapi juga kedisiplinan ASN yang menggunakannya.

2. Rekomendasi untuk Masyarakat

Masyarakat Klungkung juga menjadi bagian penting dari rantai keamanan digital daerah. Oleh karena itu, masyarakat diimbau untuk:

- a. **Tidak membagikan data pribadi** (NIK, KK, atau dokumen resmi) melalui pesan atau situs yang tidak terverifikasi.
- b. **Melaporkan insiden penipuan digital, akun palsu, atau kebocoran data pribadi** ke TTIS Klungkung.
- c. **Mengikuti kegiatan edukasi keamanan digital** yang digelar di tingkat desa, sekolah, dan komunitas.
- d. **Meningkatkan kewaspadaan di media sosial** agar tidak mudah terpengaruh oleh tautan atau pesan mencurigakan.
- e. **Menggunakan perangkat dan aplikasi resmi**, serta memperbarui sistem keamanan secara rutin.

Dengan keterlibatan masyarakat, ekosistem digital Klungkung akan semakin kuat dan tangguh dalam menghadapi serangan siber.

“Ketahanan siber daerah bukan hanya tugas pemerintah,
tetapi gerakan bersama seluruh ASN dan masyarakat.
Dengan TTIS Klungkung, kita jaga ruang digital Klungkung
tetap aman, bersih, dan terpercaya.”

Melalui kerja sama dan kesadaran kolektif, Klungkung dapat menjadi **daerah percontohan keamanan siber di Provinsi Bali**, serta inspirasi bagi pemerintahan daerah lain dalam membangun keamanan digital yang adaptif dan berkelanjutan.



Pertanyaan Reflektif

1. Saat sistem kerja Anda tiba-tiba mengalami gangguan atau data tidak bisa diakses, bagaimana langkah awal yang sebaiknya dilakukan sebelum menghubungi TTIS Klungkung?
2. Seorang rekan ASN menggunakan email pribadi untuk mengirim dokumen dinas penting. Bagaimana Anda akan menjelaskan risiko keamanan dari tindakan tersebut dengan cara yang membangun?
3. Ketika masyarakat menemukan situs palsu yang meniru halaman resmi pemerintah daerah, langkah konkret apa yang bisa dilakukan untuk melindungi warga lain dari penipuan digital serupa?
4. Dalam koordinasi penanganan insiden, TTIS Klungkung melibatkan berbagai perangkat daerah dan agen keamanan siber. Bagaimana kolaborasi ini bisa mempercepat proses tanggap dan pemulihan insiden?
5. Sebagai bagian dari masyarakat digital Klungkung, bagaimana Anda dapat mendukung kegiatan edukasi keamanan siber agar semakin banyak orang memahami pentingnya perlindungan data pribadi?
6. Jika Anda menjadi bagian dari tim TTIS Klungkung, nilai-nilai profesionalisme dan tanggung jawab seperti apa yang menurut Anda harus dijaga dalam menangani insiden siber yang sensitif?
7. Banyak masyarakat yang belum memahami peran TTIS. Bagaimana cara terbaik Anda membantu menyebarkan informasi mengenai layanan dan manfaat TTIS Klungkung di lingkungan sekitar?

DAFTAR PUSTAKA

Pemerintah Kabupaten Klungkung. (2025). *Keputusan Bupati Klungkung Nomor 272/12/HK/2025 tentang Pembentukan Tim Tanggap Insiden Siber (Computer Security Incident Response Team) Kabupaten Klungkung (KLUNGKUNG-CSIRT)*. Klungkung: Pemerintah Kabupaten Klungkung.

Pemerintah Kabupaten Klungkung. (2022). *Keputusan Bupati Klungkung Nomor 349/12/HK/2022 tentang Pembentukan Computer Security Incident Response Team Kabupaten Klungkung (dicabut dan tidak berlaku)*. Klungkung: Pemerintah Kabupaten Klungkung.

