LAPORAN EVALUASI PENYELENGGARAAN TIM TANGGAP INSIDEN SIBER (TTIS) POSO CSIRT

KABUPATEN POSO
TAHUN ANGGARAN 2024

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

TTIS merupakan pilar penting keamanan siber. Hal ini disebabkan TTIS menjalankan peran tanggap insiden siber untuk meminimalisir dan mengontrol cakupan eskalasi yang terdampak insiden siber serta memulihkan Sistem dan Infrastruktur Teknologi Informasi dan Komunikasi pada kondisi normal sehingga Proses Kerja dan Layanan dapat berjalan normal kembali. Pada praktiknya, TTIS menyelenggarakan 3 (tiga) area layanan berupa Reaktif, Proaktif dan Manajamen Kualitas Keamanan untuk mendukung tata kelola keamanan siber yang mana, "Reaktif" dalam tanggap insiden siber terhadap pendampingan dan penanganan insiden siber pada konstituen dan "Aktif" dalam meningkatkan keamanan sistem dan infrastruktur sebelum insiden siber terjadi dan/ atau sebuah kondisi anomali terdeteksi serta "*lesson learned*" atas upaya penanganan insiden siber yang telah dilakukan dalam rangka perbaikan kebijakan keamanan siber.

Berdasarkan Peraturan Presiden nomor 18 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, diamanahkan kepada instansi pemerintah penyelenggara Sistem Pemerintahan Berbasis Elektronik (SPBE) untuk menyelenggarakan penanganan insiden keamanan SPBE. Adapun dalam praktiknya, penanganan insiden keamanan SPBE dilaksanakan oleh sebuah tim khusus yang disebut *Computer Security Incident Response Team* (TTIS). Dalam rangka Penyelenggaraan TTIS, setiap organisasi atau instansi pemerintah dapat mengacu pada Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 1 tahun 2024 tentang Pengelolaan Insiden Siber yang mana TTIS dikategorisasikan menjadi 3 (tiga) yaitu TTIS Nasional, TTIS Sektor, dan TTIS Organisasi. Masing-masing TTIS memiliki hak dan kewajiban sesuai dengan kategorisasinya.

Pemerintah Daerah Kabupaten Poso telah membentuk Tim Tanggap Insiden Siber yang diberi nama Poso CSIRT pada 12 Desember 2023 berdasarkan (SK Tim TTIS). TTIS merupakan TTIS Organisasi yang menginduk TTIS Sektor Pemerintah yang dilaksanakan oleh BSSN melalui Gov-TTIS Indonesia. BSSN sebagai pengampu TTIS Sektor Administrasi Pemerintahan memiliki tugas melakukan pembinaan dan penguatan TTIS Sektor Administrasi Pemerintahan sehingga nantinya masing-masing TTIS organisasi Instansi Pemerintah mampu melakukan pengelolaan insiden siber secara mandiri dan profesional.

Guna mewujudkan TTIS Organisasi yang mampu merespon insiden siber secara mandiri maka dilakukan Evaluasi Penyelenggaraan TTIS Kabupaten Poso untuk mengukur kematangan TTIS dalam melaksanakan layanan TTIS sesuai dengan RFC-2350 yang telah dideklarasikan. Adapun hasil evaluasi TTIS tersebut akan menjadi bahan masukan bagi Bupati Kabupaten Poso dan BSSN dalam menentukan kebijakan dan penguatan Poso CSIRT.

B. Dasar

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024
3. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital;
4. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber;
5. Peraturan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia Nomor 1 Tentang Pedoman Pembentukan Tim Tanggap Insiden Siber Sektor pemerintahan;

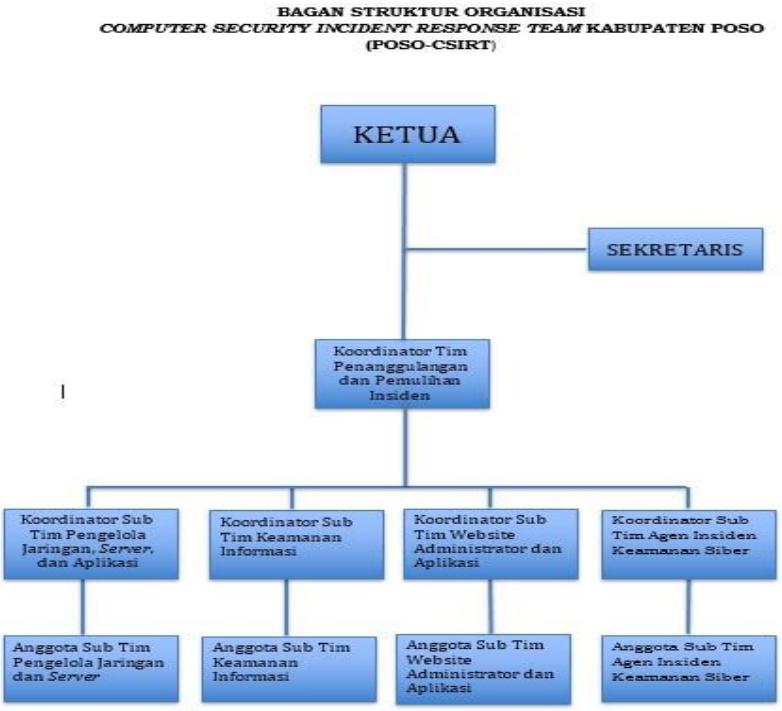
6. (SK Nomor 188.45/0804/2023 tentang pembentukan Tin Tanggap Insiden Siber)
7. (Surat Tanda Registrasi Nomor : 363/CSIRT.01.02.01/BSSN/06/2024).

C. Tujuan

Evaluasi Penyelenggaraan TTIS bertujuan untuk mengukur efektivitas penyelenggaraan TTIS dalam pengelolaan insiden siber di internal Pemerintah (Kabupaten Poso) serta menjaga keamanan layanan sistem elektornik milik Pemerintah (Kabupaten Poso).

BAB II
TTIS POSO CSIRT

Merujuk pada SK Tim TTIS. TTIS menyelenggarakan 1 (satu) fungsi utama. Fungsi Utama terdiri dari pemberian peringatan terkait keamanan siber; perumusan panduan teknis penganan insiden siber; pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak; pemilihan (triage) insiden siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan insiden siber yang akan ditangani; penyelenggaraan koordinasi penanganan insiden siber kepada pihak yang berkepentingan; dan pengelenggaraan fungsi lainnya sesuai kebutuhan.
Dalam rangka menyelenggarakan layanan tersebut, Pemerintah Kabupaten Poso menyusun struktur TTIS yang terdiri dari :



Gambar 1. Struktur Organisasi TTIS

1. Ketua, mempunyai tugas dan tanggungjawab yaitu:
   a. Memimpin pelaksanaan tugas dan bertanggung jawab atas kegiatan di POSO-CSIRT;
   b. Menyediakan Point Of Contact (POC) untuk POSO-CSIRT, berupa alamat email, nomor telepon, dan komunikasi lainnya;
   c. Bertanggung jawab dalam pengalokasian sumber daya yang dibutuhkan untuk mengoperasionalkan layanan POSO-CSIRT;
   d. Mengkoordinasikan POSO-CSIRT dengan instansi dan pihak-pihak terkait lainnya dalam rangka pelaksanaan tugas dan fungsi POSO-CSIRT, serta menjalin kerja sama antar CSIRT;
   e. Memantau operasional dan kinerja POSO-CSIRT;
   f. Membuat perencanaan operasional dan strategis mengenai POSO-CSIRT;
   g. Mengkoordinasikan edukasi dan pelatihan mengenai keamanan siber di lingkungan POSO-CSIRT;
   h. Menyusun dan menyampaikan laporan kepada Bupati Poso.

2. Sekretaris, mempunyai tugas dan tanggungjawab yaitu
   a. Melaksanakan fungsi kesekretariatan/ ketatausahaan meliputi administrasi dan dokumentasi pada operasional layanan POSO-CSIRT;

b. Membantu Ketua POSO-CSIRT dalam menjalankan tugas dan tanggung jawabnya;
c. Menyelenggarakan rapat-rapat koordinasi.

3. Koordinator Tim Penanggulangan dan Pemulihan Insiden tugas dan tanggungjawab :

a. Menerima koordinasi apabila terjadi insiden siber
b. Melakukan penanggulangan dan pemulihan insiden secara cepat dan tepat;
c. Melakukan tindakan korektif atas celah kerawanan (vulnerability) yang ditemukan;
d. Melakukan pemeriksaan dan analisis terhadap artifak yang ditemukan;
e. Melakukan analisis risiko;
f. Melakukan audit atau penilaian keamanan;
g. Menjadi tim teknis yang memberikan edukasi dan pelatihan.

BAB III PENYELENGGARAAN TTIS KABUPATEN POSO

Pemerintah Kabupeten Poso menyelenggarakan layanan TTIS terhadap seluruh konstituen sesuai dengan RFC-2350 yang meliputi Perangkat Daerah di Lingkungan Pemerintah Kabupeten Poso guna Visi dan Misi TTIS. Adapun dalam penyelenggaraannya, TTIS berkolaborasi dengan seluruh Organisasi Perangkat Daerah melalui agen siber yang tergabung dalam Tim TTIS. TTIS membuka layanan portal aduan siber dan menghimbau baik kepada pegawai internal maupun masyarakat luar untuk dapat melaporkan insiden siber jika terdapat gangguan atau tidak berjalannya sistem elektronik milik Pemerintah Kabupeten Poso ke alamat posokabcsirt@gmail.com

Selama dalam penyelenggaraan TTIS dalam (kurun waktu penyelenggaraan TTIS dari tanggal terbentuk sampai Desember 2024), Pemerintah (Kabupaten Poso) melalui Dinas Komunikasi dan Informatika dan Persandian belum melaksanakan evaluasi penyelenggaraan TTIS dan kematangan penanganan insiden siber berupa:

Fungsi Utama yang diselenggarakan berupa :

a. Pemberian peringatan terkait keamanan siber

   Fungsi ini berupa pemberian peringatan terkait informasi anomali atau ancaman siber kepada seluruh konstituen.

   TTIS (POSO CSIRT) telah rutin memberikan peringatan apabila informasi anomali atau ancaman siber kepada keseluruhan OPD melalui sistem monitoring Wazuh yang sudah terpasang pada semua aset milik OPD. Peringatan tersebut diberikan dalam bentuk laporan dan mewajibkan bagi pemilik aset untuk memberikan feedback berupa tindak lanjut atas peringatan terkait infrmasi anomali atau ancaman siber yang telah diberikan.

b. Perumusan panduan teknis penanganan Insiden Siber

   Fungsi ini berupa perumusan panduan teknis penanganan insiden siber. TTIS (POSO CSIRT) belum melakukan identifikasi dan perumusan panduan teknis yang disesuaikan dengan kondisi saat ini, dimana 3 panduan teknis yang harus dibuat yaitu, panduan teknis penanganan insiden Web Defacement, Ransomware, dan DDOS. Hal ini dilandasi karena belum adanya insiden siber web Defacement, Ransomware, maupun DDOS pada server.

c. Jika sudah melaksanakan identifikasi ancaman, Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;

A. Sumber Daya Penyelenggara TTIS

Sumber Daya Penyelenggara TTIS dilakukan pembaruan setiap tahun guna mengetahui kekuatan sumber daya TTIS dalam menyelenggarakan layanan terhadap konstituen.

1. Sumber Daya Manusia TTIS

Tabel 5. Sumber Daya Manusia TTIS

NO	NAMA	JABATAN
1.	I Wayan Susanto, STTP	Ketua
2.	Rastam Rabbie, S.Kom.,MM	Sekretaris
3.	Abdulhadi Hi Toba, S.Sos, M.AP	Koordinator Tim Penanggulangan dan Pemulihan Insiden
4.	Hendra Mardani, S.Sos	Koordinator Tim Pengelola Jaringan dan Server
5.	Sukaji, S.Kom	Anggota Tim Pengelola Jaringan Dan Server
6.	Roberth Son Sumampouw, ST	Koordinator Tim Keamanan Informasi
7.	Sandro Utama Putra Sepatondu, S.Kom	Anggota Tim Keamanan Informasi
8.	Rusman, S.Sos	Koordinator Tim Website Administrator dan Aplikasi
9.	Moh Rizky RM, S.Sos., MM	Anggota Tim Website Administrator dan Aplikasi
10.	Pejabat Penaggungjawab Website Bappeda	Sub Tim Agen Insiden Keamanan Siber.
	Adnan Mehingko, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
11.	Pejabat Penanggungjawab Website Badan Pendapatan Daerah	Sub Tim Agen Insiden Keamanan Siber
	Sepron Kamawo, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber

12.	Pejabat Penaggungjawab Website Badan Pengelola Keuangan dan Aset Daerah	Sub Tim Agen Insiden Keamanan Siber
	Jerry Kalvari Pelensa, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
13.	Pejabat Penaggungjawab Website bagian LPSE	Sub Tim Agen Insiden Keamanan Siber
	Aun Ponamon, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
14.	Pejabat Penanggungjawab Website Dinas Kependudukan dan Catatan Sipil	Sub Tim Agen Insiden Keamanan Siber
	Oktaviana Ruth Tomusu, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
15.	Pejabat Penanggungjwab Website BKPSDM	Sub Tim Agen Insiden Keamanan Siber
	Muhamad Ikra Chandra, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
16.	Pejabat Penanggungjawab Website Badan Inspektorat	Sub Tim Agen Insiden Keamanan Siber
	Sumanto, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
17.	Penaggung Jawab Website Komisi Pemilihan Umum Kabupaten Poso	Sub Tim Agen Insiden Keamanan Siber
	Muhamad Ikra Chandra, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber
18.	Pejabat Penanggungjawab Website Bagian Pembangunan	Sub Tim Agen Insiden Keamanan Siber
	Didin Lasauju, S.Kom	Anggota sub Tim Agen Insiden Keamanan Siber

2. Sumber Daya Perangkat TTIS

(Perangkat yang digunakan tim TTIS untuk publikasi, monitoring dan ticketing)

No	Nama	Spesifikasi	Jumlah	Unit Kerja/ Bidang Pengelola
1.	Computer Server CSIRT	Ubuntu 22.04 LTS (GNU/Linux 6.2.16-3-pve x86_64,8 core cpu 2100ghz, ram 16gb, hardisk 500gb	1 (satu)	Dinas Komunikasi, Informatika dan Persandian
2.	Website Poso CSIRT	Ubuntu 22.04 LTS (GNU/Linux 6.2.16-3-pve x86_64,2 core cpu 2100ghz, ram 2gb, hardisk 50gb	1 (satu)	EGOV
3	Komputer OS Ticket	Ubuntu 22.04 LTS (GNU/Linux 6.2.16-3-pve x86_64,2 core cpu 2100ghz, ram 2gb, hardisk 50gb	1 (satu)	EGOV

B. Kematangan Penanganan Insiden Siber

(Penjelasan singkat pengukuran TMPI yang pernah dilaksanakan)

Pemerintah Kabupaten Poso melalui Dinas Komunikasi dan Informatika melaksanakan kegiatan pengukuran tingkat maturitas penanganan insiber siber dengan menggunakan instrumen Tingkat Maturitas Penanganan Insiden Siber (TMPI) sebagai upaya profiling terhadap kematangan Tim Tanggap Insiden Siber dan Organisasi Dinas Komunikasi dan Informatika dalam menerapkan keamanan siber di lingkungan Pemerintah Kabupaten Poso.

TMPI merupakan instrumen yang digunakan untuk mengukur tingkat kematangan tim tanggap insiden siber dalam melakukan pengelolaan insiden siber di internal instansi. Ruang Instrumen TMPI terdiri dari 3 (tiga) fase yaitu Persiapan, Respon dan Tindak Lanjut. Adapun masing-masing ruang lingkup

memberikan gambaran secara nyata atas kondisi TTIS dalam menjalankan proses bisnis pengelolaan insiden siber.

Upaya yang dilakukan oleh TTIS dalam meningkatkan skor TMPI berupa:

1. Penyusunan Kebijakan penanganan insiden siber;
2. Inventarisasi aset dan analisa dampak risiko, bisnis dan hukum;
3. Penyusunan skenario penanganan insiden siber serta mekakukan simulasi;

BAB IV
PENUTUP

Laporan Evaluasi Penyelenggaraan TTIS disusun berdasarkan atas capaian penyelenggaran TTIS selama 1 (satu) tahun. Hasil capaian ini merupakan wujud komitmen pimpinan Pemerintah Kabupaten Poso dalam menjaga keamanan siber terhadap sistem elektronik yang dikelola baik oleh Dinas Komunikasi Informatika dan Statistik maupun Organisasi Perangkat Daerah.

Demikian Laporan Evaluasi Penyelenggaraan TTIS disusun sebagai bahan pertimbangan Bupati Poso dan Kepala Badan Siber dan Sandi Negara dalam menentukan kebijakan dan penguatan TTIS sehingga mampu melakukan pengelolaan insiden siber secara mandiri dan profesional.

Poso, 4 Desember 2024
Kepala Dinas Komunikasi Informatika
Persandian

Ditandatangani secara elektronik oleh :
KEPALA DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KAB.POSO
I WAYAN SUSANTO, S.STP
Pembina Tingkat I / Ivb


Bimbingan Teknis Pengelolaan CSIRT
Tahun 2023
Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Tahun 2023
CYBER
SECURITY
DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN
KABUPATEN POSO
Poso, 29-30 November 2023
dr. Verna G.M Inkiriwang
Bupati Poso


KABUPATEN POSO