
	LAPORAN ONSITE ASSESSMENT INDEKS KAMI	 INDEKS KEAMANAN INFORMASI
Instansi/Perusahaan: PEMERINTAH PROVINSI NUSA TENGGARA BARAT	Pimpinan Unit Kerja : Baiq Nelly Yuniarti, AP., M.Si 19750615 199412 2 001	
Unit Kerja: DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK	Narasumber Instansi : 1. Lalu Amjad, S.H., M.H. 19691231 199203 1 099 2. Yasrul, S.Kom., M.Eng 19740203 199903 1 001 3. Lalu Arief Gunawan, S.E., M.Si 19761021 201001 1 002 4. Ni Made Febrie Arisandi Ak, SE., ST 19760213 200801 2 014 5. Robert Silas Kabanga, S.Kom., M.Eng 19860513 201101 1 015 6. R. Ronald Ommy Y., S.T., M.T 19830717 200901 1 008 7. Yosafat Parulian D. -	
Alamat: Jl. Udayana No.14, Kota Mataram, Nusa Tenggara Barat 83122		
Email: kominfotik@ntbprov.go.id	Asesor : 1. Lukman Nul Hakim, S.E., M.M 19701116 199110 1 001 2. Irma Nurfitri Handayani, S.ST 19850303 200501 2 001 3. Arif Fachru Rozi, S.ST 19860423 200501 1 002 4. Carissa Mega Yulianingrum, S.Tr.TP 19930720 201611 2 001	
Tel/ Fax: Tel: (0370) 644264		

A. Ruang Lingkup:

1. Instansi / Unit Kerja:

Dinas Komunikasi, Informatika dan Statistik Provinsi Nusa Tenggara Barat.

2. Fungsi Kerja:

Dinas Komunikasi, Informatika dan Statistik Provinsi Nusa Tenggara Barat menyelenggarakan Urusan Pemerintahan Bidang Komunikasi dan Informatika, Urusan Pemerintahan Bidang Statistik serta Urusan Pemerintahan Bidang Persandian yang menjadi kewenangan Daerah Provinsi dan Tugas Pembantuan yang ditugaskan kepada Daerah Provinsi, salah satu bagian dari Diskominfo adalah bidang Persandian dan Keamanan Informasi. Bidang Persandian dan Keamanan Informasi bertugas melaksanakan pengelolaan persandian dan keamanan informasi, diantaranya adalah penyediaan/pembangunan infrastruktur dan sarana prasarana teknologi keamanan informasi serta penerapan sertifikat sistem manajemen pengamanan informasi pada setiap sistem elektronik berbasis komputer di perangkat daerah lingkungan pemerintah Provinsi NTB

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Udayana No.14, Kota Mataram, Nusa Tenggara Barat 83122
2	Data Center	Jl. Pejanggalik no.12 Mataram, Nusa Tenggara Barat 83122
3	Disaster Recovery Center (DRC)	Jl. Pejanggalik no.12 Mataram, Nusa Tenggara Barat 83122

B. Nama /Jenis Layanan Publik:

Pendaftaran *Online* Rumah Sakit Jiwa Mutiara Sukma Pelayanan Perijinan Penelitian yang dikelola oleh Diskominfo Provinsi Nusa Tenggara Barat

C. Aset TI yang kritikal:

1. Informasi:

- Data Rekam Medis Pasien
- Data Penelitian

2. Aplikasi:

- SiPenter
- Pendaftaran Online RSJMS

3. Server :

- Server baremetal di Data Center
- Cloud-dedicated VPS di Jakarta dan PDN

4. Infrastruktur Jaringan/Network:

- Intranet
- Internet

D. DATA CENTER (DC):

- ☒ ADA, dalam ruangan khusus (Ruang server dikelola internal).
- ☐ ADA, jadi satu dengan ruang kerja
- ☐ TIDAK ADA

E. DISASTER RECOVERY CENTER (DRC):

- ☒ ADA ☐ Dikelola Internal ☐ Dikelola Vendor :
- ☐ TIDAK ADA

Status Ketersediaan Dokumen Kerangka Kerja**Sistem Manajemen Keamanan Informasi (SMKI)**

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	Kebijakan, Sasaran, Rencana, Standar			
1	Kebijakan Keamanan Informasi		Tdk	

2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	Ya		
3	Sasaran TI / Keamanan Informasi	Ya		
4	Organisasi TI / Keamanan Informasi (IT <i>Steering Committee</i> , Fungsi Keamanan TI)	Ya		
5	Metodologi Manajemen Risiko TI		Tdk	
6	<i>Business Continuity Plan</i>		Tdk	
7	Klasifikasi Informasi	Ya		
8	<i>Standar software desktop</i>		Tdk	
9	Metode Pengukuran Efektivitas Kontrol		Tdk	
10	<i>Non Disclosure Agreement</i> (NDA)		Tdk	
	Prosedur/ Pedoman:			
1	Pengendalian Dokumen	Ya		
2	Pengendalian Rekaman/Catatan	Ya		
3	Tindakan Perbaikan & Pencegahan		Tdk	
4	Audit Internal			
5	Penanganan (<i>Handling</i>) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran			
6	Pengelolaan <i>Media Removable & Disposal</i>		Tdk	
7	Pengelolaan Perubahan Sistem TI (<i>Change Control</i> Sistem TI)		Tdk	
8	Pengelolaan Hak Akses (<i>User Access Management</i>)		Tdk	
9	<i>Teleworking</i> (Akses Remote)		Tdk	
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	Ya		

11	Pemantauan (<i>Monitoring</i>) Sumber Daya TI: a. Monitoring Kapasitas b. Log Penggunaan User		Tdk	
12	Instalasi & Pengendalian Software		Tdk	
13	<i>Back-up & restore</i> (prosedur/jadwal)		Tdk	

Tabel 1. *Check-list* Ketersediaan Dokumen SMKI (Indeks KAMI)**Dokumen yang diperiksa:**

1. Peraturan Gubernur Nusa Tenggara Barat nomor 35 tahun 2012 tentang Pedoman Pengelolaan Informasi dan Dokumentasi di Lingkungan Pemerintah Provinsi Nusa Tenggara Barat
2. Peraturan Gubernur Nusa Tenggara Barat nomor 55 tahun 2019 tentang Rencana Induk Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Nusa Tenggara Barat
3. Peraturan Gubernur Nusa Tenggara Barat nomor 11 tahun 2020 tentang Pedoman Uji Konsekuensi Informasi Publik
4. SOP : Pengajuan Email Dinas
5. SOP Pengembangan Aplikasi
6. SOP BCP
7. SOP Kirim terima berita rahasia
8. SOP Pengiriman naskah dinas yang dikecualikan
9. SOP Pengiriman naskah
10. SOP Penerimaan
11. SOP Pengiriman naskah berita email sanapati
12. SOP Back up data elektronik internal naskah biasa dan dikecualikan
13. SOP Pendokumentasian Informasi Publik
14. SOP Pengelolaan Insiden Keamanan Informasi
15. SOP Pemutakhiran masa kerja pegawai pengelola informasi berklasifikasi
16. SOP Penanganan Gangguan Pusat Data
17. SOP Masuk Pusat Data
18. SOP Back up data elektronik eksternal naskah dinas
19. SOP Penempatan Server
20. Rancangan Peraturan Gubernur tNTB entang SK Tim Audit Internal SPBE
21. Rancangan Peraturan Gubernur NTB tentang SMKI

22. Laporan Kegiatan Literasi Keamanan Informasi
23. NDA Trial Platform Satu Data Indonesia
24. Laporan Pengembangan Portal NTBProv
25. Laporan ITSA BSSN pada 3 (Tiga) Sistem Elektronik
26. Daftar Aset Perangkat Keras dan Perangkat Lunak Diskominfo Provinsi NTB
27. Dokumen Riwayat Pengembangan NTB Care
28. Laporan Penanganan Insiden Siber Aplikasi e-kinerja
29. Dokumen Pelaporan Insiden Siber
30. SK NTBProv-CSIRT
31. Renstra Diskominfo 2019-2023
32. DPAA-Belanja SKPD Diksominfo NTB 2022 nomor DPPA/A.2/2.16.2.20.2.21.04.0000/001/2022
33. Dokumen Analisis jabatan Diskominfo Provinsi NTB 2021
34. Laporan Hasil Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian Pemerintah Provinsi NTB
35. Laporan Seksi Keamanan Informasi 2021
36. Perjanjian Kinerja Tahun 2021
37. Rancangan Manajemen Risiko

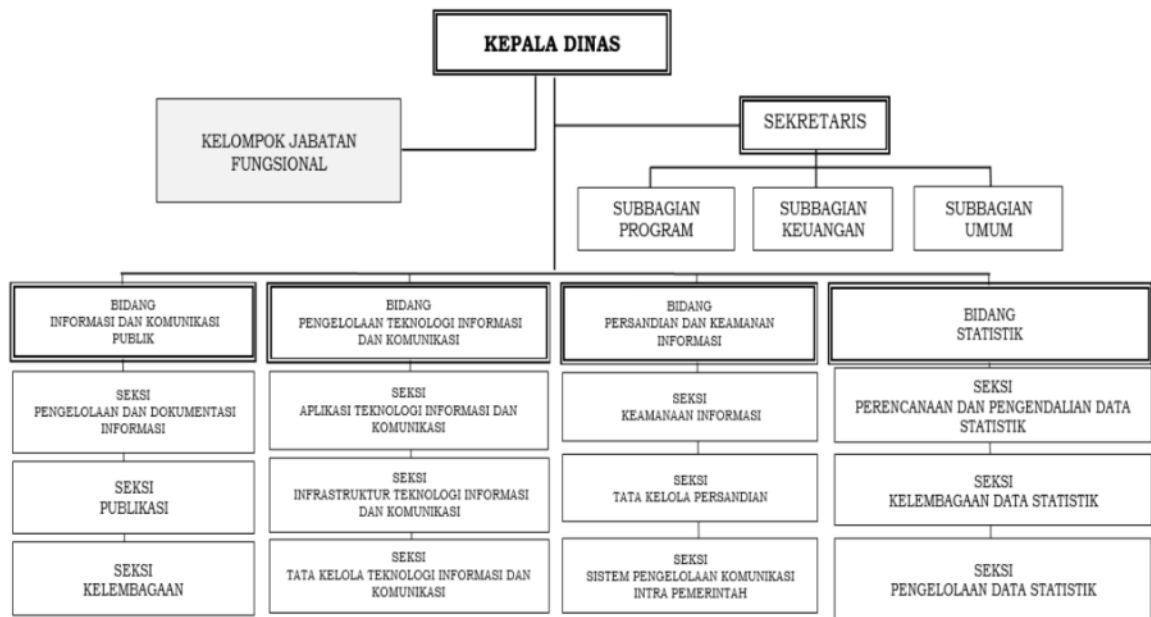
Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Tangkapan Layar Tampilan Webpanel
2. Tangkapan Layar SSL aplikasi web dan algoritma otentikasi

Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber instansi/lembaga disimpulkan sebagai berikut :

I. KONDISI UMUM:

1. Struktur Diskominfo Provinsi Nusa Tenggara Barat adalah sebagai berikut:



Gambar 1. Struktur Organisasi Dinas Komunikasi, Informatika dan Statistik Provinsi Nusa Tenggara Barat

2. Sumber Daya Manusia Dinas Komunikasi, Informatika Provinsi Nusa Tenggara Barat terdiri dari:

No	Unit Kerja/ Bidang	ASN	NON-ASN	Jumlah
1	Sekretariat	20	40	60
2	Informasi & Komunikasi Publik	9	17	26
3	Pengelolaan Teknologi Informasi dan Komunikasi	7	9	16
4	Persandian dan Keamanan Informasi	7	3	10
5	Statistik	9	6	15
Jumlah				

Tabel 2. SDM Diskominfotik Provinsi Nusa Tenggara Barat

3. Berdasarkan verifikasi terhadap hasil *Self Assessment* isian file Indeks KAMI diperoleh hasil sebagai berikut:

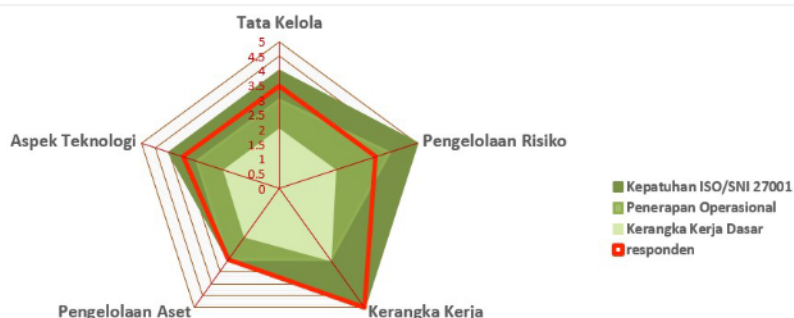
Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 ini dengan ruang lingkup Diskominfo Provinsi Nusa Tenggara Barat, Server dan Sistem Informasi yang dikelola dan dilakukan verifikasi oleh Tim BSSN dengan kategori **TINGGI** dan hasil evaluasi akhir **Pemenuhan Kerangka Kerja Dasar** dengan total nilai **286**.

Pada tahun 2022 ini merupakan penilaian pertama bagi Diskominfo Provinsi Nusa Tenggara Barat dilakukan verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI dengan melakukan pengecekan keseluruhan kelengkapan kebijakan dan/atau prosedur dan penerapan dokumen kebijakan dan/atau prosedur pada area Kategori, Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi.

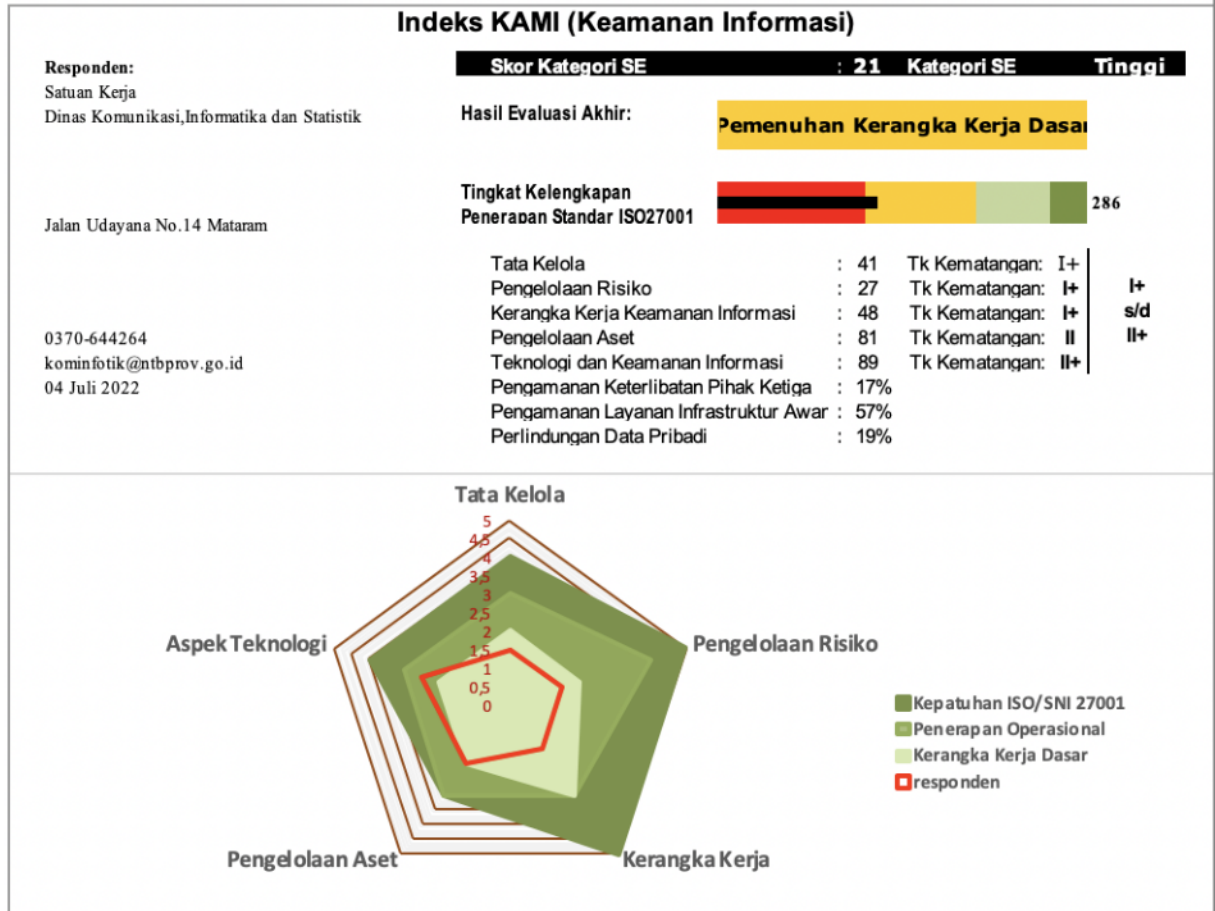
Penilaian tahun 2022 berfokus kepada satu Sistem Elektronik yang dikelola oleh Diskominfo Provinsi Nusa Tenggara Barat dengan kategori tinggi yaitu: SiPenter.

Total Score Sebelum Verifikasi: 645 (ref. File Indeks KAMI Pra Verifikasi)

Indeks KAMI (Keamanan Informasi)			
Responden: Dinas Komunikasi dan Informatika Provinsi Jawa Tengah, Bidang Persandian dan Keamanan Informasi	Skor Kategori SE	: 44	Kategori SE Strategis
	Hasil Evaluasi Akhir:	Baik	
	Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kateori	634	
Jl. Menteri Supeno I/2 Mugassari, Kota Semarang, Jawa Tengah Data Center (Jl. Taman Menteri Supeno no. 2B, Kota Semarang, Belakang Masjid At-Taqwa)	Tata Kelola	: 123	Tk Kematangan: III+
(024) 8319140 diskominfo@jatengprov.go.id 18/05/2022	Pengelolaan Risiko	: 67	Tk Kematangan: III+
	Kerangka Kerja Keamanan Informasi	: 159	Tk Kematangan: V
	Pengelolaan Aset	: 167	Tk Kematangan: III
	Teknologi dan Keamanan Informasi	: 118	Tk Kematangan: III+
	Pengamanan Keterlibatan Pihak Ketiga	: 58%	
	Pengamanan Layanan Infrastruktur Awan	: 67%	
	Perlindungan Data Pribadi	: 31%	



Total Score Setelah Verifikasi: 286 (ref. file Indeks KAMI Pasca Verifikasi)



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Pimpinan dari Diskominfotik Provinsi NTB sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah adanya penetapan kebijakan keamanan informasi. Salah satu hal ini adalah dengan dibuktikan terkait program keamanan informasi dalam pembentukan CSIRT Provinsi NTB
2. Diskominfotik Provinsi NTB sudah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memastikan kepatuhannya
3. Pejabat/petugas pelaksana pengamanan informasi sudah ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang akan dilaksanakan

4. Alokasi sumber daya terkait pelaksanaan program keamanan informasi sudah direncanakan dan disediakan dalam rangka memastikan pengelolaan keamanan informasi telah memadai dan dipastikan kepatuhannya
5. Diskominfotik Provinsi NTB sudah mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi
6. Diskominfotik Provinsi NTB sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi dengan merencanakan secara berkala minimal setiap tahun dalam rangka memastikan kebutuhan penerapan kontrol keamanan informasi telah terpenuhi
7. Pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait dan pihak eksternal yang berkepentingan untuk menerapkan dan menjamin kepatuhan pengamanan informasi kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak.gram keamanan informasi kepada pimpinan
8. Penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektivitas kepada pimpinan
9. Kondisi dan permasalahan keamanan informasi menjadi konsiderans atau bagian dari sebagian proses pengambilan keputusan
10. Diskominfotik telah mendefinisikan parameter dan pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaan, pemantauan dan eskalasi pelaporan
11. Diskominfotik telah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi pegawai
12. Diskominfotik telah menetapkan target sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin

B. Kelemahan/Kekurangan

1. Peran fungsi pelaksana pengamanan informasi sedang proses pemetaan terkait pengelolaan program keamanan informasi secara lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan

2. Semua pelaksana pengamanan informasi yang terlibat di Diskominfo Provinsi NTB belum memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi
3. Manajemen Diskominfo Provinsi NTB dan fungsi pengelola keamanan informasi sudah merencanakan namun tidak menerapkan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi melalui beberapa media (seperti email, poster, training, dll) dan dievaluasi hasil penerapannya untuk memastikan kepatuhannya bagi semua pihak yang terkait. Hal ini dikarenakan program kerja tersebut dikenakan *refocusing*
4. Diskominfo Provinsi NTB dalam proses perencanaan pengintegrasian persyaratan keamanan informasi dalam proses kerja
5. Data pribadi yang digunakan dalam proses kerja belum diidentifikasi dan belum dilakukan penerapan pengamanan sesuai peraturan perundangan yang berlaku
6. Tanggungjawab pengelolaan keamanan informasi belum mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak yang berkepentingan untuk mengidentifikasi persyaratan/kebutuhan pengamanan
7. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK belum didefinisikan dan dialokasikan
8. Pimpinan Diskominfo Provinsi NTB belum menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi khususnya mencakup aset informasi yang menjadi tanggungjawabnya
9. Manajemen Diskominfo Provinsi NTB belum mendelegasikan pihak terkait / unit kerja / fungsi pengelola keamanan informasi pada internal Diskominfo Provinsi NTB untuk mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisa tingkat kepatuhannya
10. Diskominfo Provinsi NTB belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)

III. ASPEK RISIKO:**A. Kekuatan/Kematangan**

1. Diskominfotik Provinsi Nusa Tenggara Barat memiliki CSIRT yang bertugas dalam melakukan penanganan insiden siber serta melakukan mitigasi insiden siber maupun risiko gangguan keamanan informasi
2. Diskominfotik Provinsi Nusa Tenggara Barat telah memiliki Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik yang dijadikan sebagai acuan dalam pelaksanaan manajemen risiko terhadap aset yang dikelola
3. Ambang batas tingkat risiko telah ditentukan serta dampak kerugian telah terdefiniskan pada Dokumen Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik

B. Kelemahan/Kekurangan

1. Program kerja pengelolaan risiko keamanan informasi belum dilakukan
2. Kerangka kerja pengelolaan risiko telah ditetapkan namun belum diterapkan pada aset utama
3. Penetapan penanggungjawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko kepada pimpinan belum dilakukan
4. Identifikasi ancaman dan kelemahan pada aset informasi belum dilakukan
5. Analisa dampak kerugian akibat hilangnya atau terganggunya fungsi aset utama serta analisis/kajian risiko keamanan informasi masih dalam perencanaan
6. Pemantauan status penyelesaian langkah mitigasi risiko masih dalam perencanaan
7. Evaluasi kerangka kerja pengelolaan risiko secara berkala masih dalam perencanaan
8. Implementasi pengelolaan risiko belum sepenuhnya menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan.
9. Prosedur tinjauan manajemen dalam hal pengelolaan risiko belum dilaksanakan

IV. ASPEK KERANGKA KERJA:**A. Kekuatan/Kematangan**

1. Mekanisme kerja pengkomunikasian kebijakan keamanan informasi kepada semua pihak terkait tersedia
2. Mekanisme kerja pelaksanaan identifikasi atas kondisi yang membahayakan keamanan informasi dan penetapannya menjadi sebuah insiden keamanan informasi tersedia
3. Aspek keamanan informasi yang meliputi kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam dokumen kontrak
4. Konsekuensi atas tindakan pelanggaran kebijakan keamanan informasi telah didefinisikan, dikomunikasikan serta diterapkan
5. Pengembangan sistem telah menerapkan *Secure SDLC* serta pembahasan aspek keamanan informasi dalam manajemen proyek telah diterapkan
6. Mekanisme penanggulangan atas munculnya risiko baru atas ketidakpatuhan terhadap kebijakan keamanan informasi telah tersedia
7. Strategi penggunaan, penerapan dan pemutakhiran teknologi keamanan informasi yang disesuaikan dengan kebutuhan dan perubahan profil risiko tersedia

B. Kelemahan/Kekurangan

1. Dokumen Kebijakan keamanan informasi sedang disusun sehingga belum dapat diterapkan kepada seluruh pegawai
2. Mekanisme pengelolaan dokumen kebijakan dan prosedur keamanan informasi yang meliputi penggunaan daftar induk, distribusi, penarikan dari peredaran hingga penarikan tidak tersedia
3. Prosedur untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi tidak tersedia
4. Implementasi *security patch* diterapkan namun kebijakan yang mewajibkan penerapan *security patch* belum disusun
5. *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) belum disusun
6. Uji coba dan evaluasi hasil uji coba DRP belum dilakukan
7. Kebijakan dan prosedur keamanan informasi belum dilakukan evaluasi secara berkala
8. Strategi penerapan keamanan informasi atas hasil analisa risiko tidak tersedia

9. Hasil audit internal belum diterapkan untuk mengevaluasi kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi
10. Hasil audit internal belum diterapkan untuk perbaikan atau peningkatan kinerja keamanan informasi
11. Analisa penilaian aspek finansial sebagai data dukung dalam melakukan revisi kebijakan dan prosedur tidak diterapkan
12. Mekanisme pengujian dan evaluasi terhadap tingkat atau status kepatuhan program keamanan informasi tidak diterapkan

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

1. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap tersedia
2. Tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya
3. Diskominfotik Provinsi Nusa Tenggara Barat memiliki proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi)
4. Tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi dalam kebijakan pengelolaan barang
5. Masa retensi data, prosedur *back-up*, restore telah ditetapkan
6. Mekanisme penyelidikan/investigasi terkait kegagalan keamanan informasi dan pelaporan insiden keamanan informasi tersedia
7. Mekanisme pengamanan fisik Aset diterapkan
8. Mekanisme Pengecekan latar belakang SDM dan prosedur pengelolaan akun user bagi pegawai yang mutasi/keluar atau pegawai kontrak yang telah habis masa kerja diterapkan
9. Daftar data yang harus di *back up* dan laporan analisa kepatuhan terhadap prosedur *back up* serta daftar rekaman penerapan keamanan informasi tersedia
10. Mekanisme pengelolaan hak akses diterapkan
11. Infrastruktur komputasi terlindungi dari dampak lingkungan (kebakaran) dan pasokan listrik atau dampak petir
12. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sesuai persyaratan konstruksi bangunan yang aman
13. Peraturan yang mengatur pengamanan lokasi kerja tersedia

B. Kelemahan/Kekurangan

1. Pendefinisian tingkatan akses atas setiap klasifikasi aset informasi tidak tersedia
2. Tata tertib penggunaan komputer, email, internet serta intranet, aset instansi belum tersedia
3. Peraturan terkait instalasi piranti lunak pada aset TI milik instansi, mekanisme pemberian akses atau ijin penggunaan data pribadi tidak tersedia
4. Prosedur pengelolaan hak akses, mekanisme otentikasi pengguna dan otorisasi penggunaan aset informasi tidak tersedia
5. Mekanisme pengamanan pertukaran data dengan pihak eksternal tidak tersedia
6. Mekanisme sanitasi digital tidak tersedia
7. Prosedur kajian penggunaan akses dan hak akses serta mekanisme pembenahan atas ketidaksesuaian terhadap kebijakan keamanan informasi tidak tersedia
8. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga tidak tersedia
9. Peraturan pengamanan terhadap pengaksesan perangkat komputasi instansi secara *remote* tidak tersedia
10. Mekanisme pengamanan fisik lingkungan kerja atas kehadiran pihak ketiga tidak tersedia

VI. ASPEK TEKNOLOGI:**A. Kekuatan/Kematangan**

1. Pengamanan pada layanan TIK yang menggunakan internet sudah dilakukan lebih dari satu lapis. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll). Hal ini dapat dilihat dari topologi jaringan pada DiskominfoProvinsi Nusa Tenggara Barat
2. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dipantau untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada
3. Setiap perubahan dalam sistem informasi dan upaya akses oleh yang tidak berhak secara otomatis terekam di dalam *log*
4. Mekanisme enkripsi untuk melindungi aset informasi penting telah diterapkan
5. Mekanisme pembatasan waktu akses dan penanganan kegagalan *login* telah diterapkan
6. Sistem Pendeteksian intrusi dan monitoring aset penting DiskominfoProvinsi Nusa Tenggara Barat telah diterapkan

7. Sistem Operasi Server dan klien dimutakhirkan dan terlindungi dari virus atau *malware*

B. Kelemahan/Kekurangan

1. Analisa kepatuhan penerapan konfigurasi standar pada sistem elektronik dilakukan tidak berkala
2. Pembatasan masa berlaku kredensial pengguna tidak diterapkan dan mekanisme penggantian *password* tidak terotomatisasi
3. Audit keamanan sistem elektronik tidak dilakukan secara keseluruhan dan dilaksanakan oleh tim pengembang sistem elektronik

VII. REKOMENDASI

1. Pimpinan untuk berkomitmen dalam memberikan dukungan program dan anggaran dalam penyelenggaraan keamanan informasi di Provinsi Nusa Tenggara Barat
2. Menyelenggarakan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi kepada seluruh pegawai dilaksanakan secara rutin
3. Melaksanakan pemenuhan kompetensi dan keahlian pegawai Diskominfo Provinsi Nusa Tenggara Barat sesuai dengan standar kompetensi keamanan informasi melalui pelatihan, *workshop*, *cyber drill* dan bimbingan teknis keamanan informasi dilakukan setiap tahun
4. Melakukan pendefinisian kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)
5. Melakukan penyusunan Kebijakan Sistem Manajemen Keamanan Informasi
6. Menerapkan penilaian risiko terhadap aset instansi
7. Menyusun *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP)
8. Menyusun mekanisme sanitasi digital aman
9. Melakukan penyusunan mekanisme pengamanan data, aset dan lingkungan kerja terhadap pihak ketiga
10. Menyusun prosedur mengenai pengelolaan implementasi *security patch* untuk memonitor adanya *update* kedalam sistem yang diperlukan, dengan alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya
11. Merumuskan kebijakan dan prosedur terkait perlindungan data pribadi untuk menjadi pedoman tertulis dalam implementasi yang telah diterapkan saat ini

12. Merumuskan kebijakan dan prosedur pengamanan layanan infrastruktur *cloud service* sebagai pedoman implementasi penyelenggaraan layanan *cloud* di Provinsi Nusa Tenggara Barat.
13. Melaksanakan kajian keamanan terhadap penggunaan akses dan hak akses serta kajian keamanan atas implementasi pengelolaan data pribadi pada sistem elektronik
14. Menyusun peraturan pengamanan terhadap pengaksesan perangkat komputasi instansi secara *remote*
15. Menyusun Tata tertib penggunaan komputer, email, internet, intranet dan aset instansi
16. Kebijakan dan prosedur tentang pengujian aplikasi sebaiknya dibuatkan terpisah dengan kebijakan dan prosedur pengelolaan dan pelaporan insiden keamanan informasi.
17. Melakukan analisa kepatuhan penerapan konfigurasi standar pada sistem elektronik dilakukan secara berkala
18. Melakukan pembatasan masa berlaku kredensial pengguna diterapkan dan mekanisme penggantian *password* dilakukan secara otomatis
19. Melakukan audit keamanan sistem elektronik dilakukan secara keseluruhan serta berkala dan dilaksanakan oleh pihak independen

VIII. PENUTUP

Demikian Laporan *Onsite Assessment* Indeks KAMI Pemerintah Daerah Provinsi Nusa Tenggara Barat T.A. 2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Provinsi Nusa Tenggara Barat.

Laporan *Onsite Assessment* Indeks KAMI Pemerintah Daerah Provinsi Nusa Tenggara Barat T.A. 2022 ini disampaikan kepada :

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Nusa Tenggara Barat; dan
3. Sekretaris Daerah Provinsi Nusa Tenggara Barat

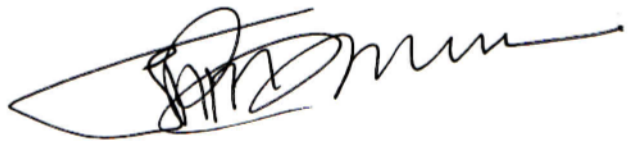
Mataram, 14 Juli 2022

Kepala Bidang Persandian dan
Keamanan Informasi



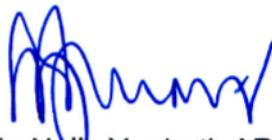
Lalu Amjad, S.H., M.H
19691231 199203 1 099

Sandiman Ahli Madya pada
Direktorat Keamanan Siber dan Sandi
Pemerintah Daerah selaku Lead Asesor:



Lukman Nul Hakim, S.E., M.M
19701116 199110 1 001

Mengetahui,
Plt. Kepala Dinas Komunikasi, Informatika dan Statistik
Provinsi Nusa Tenggara Barat



Baiq Nelly Yuniarti, AP., M.Si
19750615 199412 2 001