PEMERINTAH KABUPATEN PESISIR SELATAN
DINAS KOMUNIKASI DAN INFORMATIKA
JL. H. AGUS SALIM - PAINAN
KODE POS : 25611
TELP / FAX : (0756) 231 2227
eMAIL : kominfo@pesisirselatankab.go.id

RESUME

LAPORAN AKHIR KEGIATAN

Nama Program	:	Program Peningkatan akses Informasi dan Komunikasi
Nama Kegiatan	:	Penyelenggaraan Persandian dan Keamanan Informasi Daerah
Nomor Rekening Kegiatan	:	1.02.10.1.02.10.01.19.15.
Anggaran Kegiatan	:	Rp 112.997.000,-

A. Realisasi Anggaran

Pelaksanaan Penyelenggaraan Persandian dan Keamanan Informasi Daerah ini dianggarkan sebesar Rp 112.997.000,- dengan realisasi kegiatan fisik tercapai 100%, dan anggaran terealisasi Rp 104.704.969,- atau sebesar 92,66%. Dari anggaran yang direncanakan tersebut tersisa sebesar Rp 8.292.031,-. Untuk lebih jelasnya dapat dilihat pada tabel berikut ini.

Pagu Anggaran Awal	Pagu Anggaran Setelah Perubahan	Realisasi Anggaran	Sisa Anggaran	Persentase Anggaran
Rp 72.817.000,-	**Rp 112.997.000,-**	**Rp. 104,927,669,-**	**Rp. 8,069,331,-**	**92,86 %**

B. Tolak Ukur Kinerja

Tolak Ukur Kinerja merupakan capaian *income* dan *outcome* dari sebuah kegiatan yang dilaksanakan. Pada Kegiatan Penyelenggaraan Persandian dan Keamanan Informasi Daerah pada Tahun 2019 ini realisasi hasilnya melebihi dari target yang ditetapkan, Untuk lebih jelasnya dapat dilihat pada tabel berikut ini.

Indikator		Target	Realisasi
Capaian Program	: - Terselenggaranya pengamanan dan verifikasi informasi perangkat daerah - Tersedianya sertifikasi elektronik (Tanda Tangan Digital) - Bimtek 4 ASN tentang Persandian dan Keamanan Informasi	-100% -45 OPD -4 ASN Bimtek Persandian/Keamanan Informasi	-100% -45 OPD -3 ASN Bimtek Persandian/Keamanan Informasi, 2 ASN Bimtek SiMAYA, 3 ASN Bimtek Penyusunan Laporan Keuangan Satuan Kerja Perangkat Daerah (SKPD)
Masukan	: Jumlah Dana Yang Dibutuhkan	Rp 112.997.000,-	Rp 104.704.969,- (92,66%)

Keluaran :	Terkendalinya keamanan informasi Pemerintah Kabupaten Pesisir Selatan	45 OPD	45 OPD
Hasil :	- Terlaksananya pengamanan dan terverifikasinya data informasi - Tersedianya Buku Meningkatkan kesadaran Keamanan Informasi	- 22 Aplikasi - 45 Buku	- 35 Aplikasi - 49 Buku

C. Hasil Dari Kegiatan

1. Bertanggung jawab sebagai admin email Sanapati. Email Sanapati merupakan salah satu peralatan sandi yang berfungsi sebagai jaring komunikasi Sandi antara pusat dan daerah.
2. Melakukan koordinasi dan konsultasi mengenai tugas-tugas yang perlu dilakukan oleh persandian di daerah ke Dinas Kominfo Provinsi Sumbar, pada tanggal 25 Februari 2019.
3. Sharing informasi mengenai tata cara pengamanan data informasi dan praktek pengamanan sistem serta peralatan persandian ke Dinas Komunikasi dan Informatika Kota Bukittinggi, pada tanggal 11 – 12 Maret 2019. Hasil kegiatan ini adalah:
    a. Terdapat 3 pembagian kerja pada bidang persandian, yaitu Operator Sandi, Pengamanan Siber, dan Pengamanan Sistem.
    b. Tugas seorang Sandiman tidak hanya berperan dalam pengamanan informasi data rahasia saja akan tetapi juga melakukan pengamanan terhadap seluruh data dan informasi termasuk pengamanan aplikasi, pengamanan server, dan pengamanan sistemnya.
4. Mengikuti upgrade aplikasi siMaya dan aplikasi SPJ Online Pesisir Selatan ke Dinas Kominfo Provinsi Sumatera Barat, pada tanggal 15 Maret 2019. Hasil kegiatan ini adalah:
    a. Aplikasi siMaya telah selesai di upgrade dan sudah bisa digunakan untuk aplikasi tanda tangan digital P12 secara keseluruhan.

b. Aplikasi SPJ Online telah selesai di upgrade dan sudah bisa digunakan untuk aplikasi tanda tangan digital P12, namun hanya pada proses Nota Dinas saja, untuk proses SPT dan seterusnya masih dalam tahap pengembangan.

c. Aplikasi siMaya dan SPJ online perlu di assessment oleh BSrE jika terdapat perubahan fitur dan perubahan lain pada aplikasi tersebut. Assessment dilakukan setelah PKS.

5. Menghadiri undangan Analisis Kebutuhan dan Asistensi Teknis Layanan Sertifikat elektronik oleh Tim BSrE di Badan Siber dan Sandi Negara (BSSN) Jakarta, pada tanggal 26 – 28 Maret 2019. Hasil kegiatan ini adalah:

   a. Aplikasi yang akan digunakan untuk menerapkan tanda tangan elektronik telah diassessment oleh BSSN.

   b. Melakukan penandatanganan kerja sama untuk tanda tangan elektronik atau sertifikat elektronik antara Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan dengan Badan Siber dan Sandi Negara (BSSN).

6. Rapat koordinasi Persandian se-Sumatra Barat tentang upaya pemerintah untuk memproteksi dan menanggulangi insiden serangan siber dalam rangka penanganan keamanan informasi, pada tanggal 25 April 2019. Hasil kegiatan ini adalah:

   a. Bentuk ancaman serangan siber dilihat dari segi dimensinya adalah berupa Fisik, Logika, dan Konten Sosial-Budaya.

   b. Ruang lingkup keamanan siber yaitu keamanan aplikasi, keamanan informasi, keamanan jaringan, dan penanganan insiden.

   c. Tugas bidang Persandian pada saat ini bukan hanya untuk kepentingan data rahasia saja, tetapi untuk keamanan informasi secara keseluruhan seperti mengelola email sanapati, sertifikat elektronik, hp/ht bersandi sca, file enkripsi dan lainnya. Penanganan insiden keamanan siber merupakan sebuah usaha untuk mendeteksi, melaporkan, menilai, menangani, dan merespons serta mempelajari insiden keamanan siber.

7. Monitoring, Evaluasi, dan Pengarahan Tata Cara meningkatkan Keamanan Informasi berupa *Hardware* dan *Software* ke beberapa Kecamatan se-Kabupaten Pesisir Selatan, pada tanggal 3, 4, dan 14 Mei 2019. Hasil kegiatan ini adalah:
    a. Penyerahan Surat Keputusan Kepala Diskominfo tentang Tim Teknis Pendamping Organisasi Perangkat Daerah dalam penanganan Keamanan Informasi.
    b. Mengarahkan langkah-langkah pengamanan informasi baik *software* maupun *hardware* serta tata cara penggunaan aplikasi kepada pihak Kecamatan.
8. Koordinasi dan konsultasi Jabatan Fungsional Sandiman ke Dinas Komunikasi dan Informatika Provinsi Sumatra Barat di Padang, pada tanggal 16 Mei 2019. Hasil kegiatan ini adalah:
    a. Jabatan Fungsional Sandiman mempunyai agenda dan kegiatan-kegiatan untuk mengikuti diklat persandian ataupun sertifikasi yang diadakan langsung oleh BSSN untuk meningkatkan kemampuan SDM tenaga ahli yang telah ada di Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan khususnya bagian persandian.
9. Sosialisasi SK Tim Teknis Pendamping OPD dalam PPemanfaatan Teknologi Informasi dan Komunikasi di Kecamatan Koto XI Tarusan, pada tanggal 19 Juni 2019. Hasil kegiatan ini adalah:
    a. Mengarahkan langkah-langkah pengamanan informasi baik *software* maupun *hardware* serta tata cara penggunaan aplikasi kepada pihak Kecamatan.
    b. Tercapainya maksud sosialisasi ke pihak kecamatan terkait SK Tim Teknis Pendamping OPD sekaligus penyerahan SK Tim Teknis Pendamping OPD.
10. Asistensi Pembentukan CSIRT (*Computer Security Incident Response Team*) Sektoral di Lingkungan Pemerintah Daerah, pada tanggal 17 – 18 Juni 2019. Hasil kegiatan ini adalah:
    a. CSIRT merupakan organisasi atau tim yang bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas insiden keamanan siber.

b. Pembentukan CSIRT membutuhkan staf yang ahli di bidangnya, salah satu kompetensi dasar staf yang dibutuhkan adalah CSIRT Koordinasi (membutuhkan personal skills) dan CSIRT Penanganan Insiden (membutuhkan Technical skills).

11. Lanjutan proses kerja sama Pemerintah Kabupaten Pesisir Selatan melalui Dinas Kominfo Bersama BSSN terkait Sertifikat Elektronik, dengan membuat/mendaftarkan Tanda Tangan Digital kepada setiap Kepala OPD, Camat dan Direktur Rumah Sakit. Hasil kegiatan ini adalah:

    a. Data-data yang diperlukan untuk pembuatan Sertifikat Elektronik setiap Kepala OPD, Camat, dan Direktur Rumah Sakit sudah lengkap.

    b. Telah selesainya pembuatan Sertifikat Elektronik untuk Setiap Kepala OPD, Camat, dan Direktur Rumah Sakit.

    c. Penggunaan Sertifikat Elektronik telah di tambahkan pada aplikasi siMAYA dan e-SPPD.

12. Sosialisasi Sertifikat Elektronik oleh Narasumber dari Badan Siber dan Sandi Negara dan demo dalam penerapan sertifikat elektronik langsung ke Aplikasi siMAYA kepada Kepala OPD, Camat, dan Direktur Rumah Sakit di Lingkup Kabupaten Pesisir Selatan, pada tanggal 30 Juli 2019. Hasil kegiatan ini adalah:

    a. Pembuatan passphrase/PIN Sertifikat Elektronik dari setiap Kepala OPD, Camat, dan Direktur Rumah Sakit sudah dilakukan.

    b. Tercapainya maksud dari sosialisasi kepada peserta.

    c. Peserta mampu menerapkan Sertifikat Elektronik yang telah dimiliki ke aplikasi siMAYA dan e-SPPD.

13. Sosialisasi tentang kegiatan standardisasi dan sertifikasi keamanan modul sandi, pengecekan/validasi dan pendataan produk keamanan siber dan sandi yang digunakan di Pemerintahan Daerah serta evaluasi pemanfaatan penggunaan peralatan sandi yang didistribusi oleh BSSN, pada tanggal 08 Agustus 2019. Hasil kegiatan ini adalah:

    a. Pengguna perangkat teknologi informasi sudah menjadi keharusan dan kebutuhan bagi seluruh OPD, untuk itu sangat diperlukan produk keamanan

sandi dalam melakukan keamanan di setiap perangkat yang digunakan, baik berupa *software* maupun *hardware*.

b. Apabila ada pengadaan aplikasi harus disertifikasi ke Deputi 1 dan jika ada permasalahan diajukan ke Deputi 2.

c. Setiap barang aplikasi harus disertifikasi menurut RUU yang akan diterbitkan.

d. Standar Keamanan TIK:

- SNI ISO/IEC 19790–Persyaratan Keamanan untuk Modul Kriptografi
- SNI ISO/IEC 24759–Persyaratan Uji untuk Modul Kriptografi
- SNI ISO/IEC 15408–Kriteria Evaluasi Keamanan Teknologi Informasi
- SNI ISO/IEC 18045–Metodologi untuk Evaluasi Keamanan TI
- SNI ISO/IEC 27001–Sistem Manajemen Keamanan Informasi

e. Langkah dalam pengamananan perangkat TIK adalah:

- Setiap perangkat yang diadakan harus menampilkan spesifikasi yang sesuai dan menerapkan standar SNI.
- Melakukan evaluasi keamanan produk sandi seperti pentest.
- Minimal menggunakan satu fungsi kriptografi (modul kriptografi).
- Aplikasi yang digunakan harus memiliki fungsi keamanannya, terutama pada aplikasi yang bersifat private.

14. Membuat buku keamanan informasi dengan berbagai macam cara pengamanan informasi, kebijakan-kebijakan dalam mengamankan informasi serta beberapa tip komputer sederhana yang membuka wawasan pembaca.

15. Sosialisasi *webmail* server Pemda Pessel dan buku Keamanan Informasi ke beberapa kecamatan di Kabupaten Pesisir Selatan, pada tanggal 22 – 23 Agustus 2019. Hasil kegiatan ini adalah:

    a. Sosialisasi ini dilakukan untuk memanfaatkan email khusus pada lingkup Pemerintah Kabupaten Pesisir Selatan dalam mengamankan data transaksi elektronik. Sosialisasi dilakukan pada Kecamatan Silaut berjalan lancar.

b. Penyerahan buku Keamanan Informasi dan SK Tim Teknis Pendamping OPD dalam Pemanfaatan Teknologi Informasi dan Komunikasi. SK ini bertujuan untuk penanganan masalah IT yang ada di Kecamatan.

16. Melakukan monitoring dan evaluasi dalam pengamanan *website* Pemerintah Daerah. Kegiatan ini dilakukan dalam waktu lebih kurang 1 bulan. Hasil kegiatan ini adalah:

    a. Terdapatnya beberapa *website* Pemda yang masih kurang dalam pengamanannya.

    b. SSL expires soon: Sertifikat keamanan website akan kadaluarsa, seharusnya SSL segera diperpanjang.

    c. HTTP still accessible: protokol HTTP masih bisa diakses, kondisi seharusnya adalah semua akses HTTP langsung diarahkan ke protocol yang lebih aman yaitu HTTPS.

    d. HTTP Strict Transport Security (HSTS) not enforced: HSTS tidak diperkuat. HSTS merupakan fitur untuk meningkatkan keamanan informasi pada website seperti username/password. Seharusnya HSTS diaktifkan dan diperkuat pada website.

    e. Secure cookies not used: Keamanan cookie tidak digunakan. Cookie merupakan informasi kecil yang disimpan suatu website di komputer pengguna. Seharusnya keamanan cookies perlu digunakan agar tidak terjadi pencurian informasi melalui website.

    f. Unnecessary open ports: port-port yang tidak diperlukan terbuka sehingga memudahkan *attacker* memasukkan file/informasi berupa virus atau link yang tidak aman. Seharusnya port yang tidak ada gunanya pada website harus ditutup.

17. Pelatihan *IT Security Assessment* di Dinas Komunikasi dan Informatika Provinsi Sumatra Barat oleh Badan Siber dan Sandi Negara (BSSN), pada tanggal 21 Agustus 2019. Hasil kegiatan ini adalah:

a. Sumber ancaman teknologi informasi berasal dari *General Hacking Community, Careless/Untrained Insiders, Foreign Government, Hacktivists, Terrorist Halicious Insiders*.

b. Jenis ancaman keamanan siber teknologi informasi berupa *External Hacking, Malware, Social Engineering, Spam, Insider Data Leakage/Thieft.*

18. Pendampingan dan pembuatan phrase/PIN Tanda Tangan Digital ke Kecamatan Linggo Sari Baganti dan Kecamatan Lunang, pada tanggal 15 dan 16 Agustus 2019. Kegiatan ini bertujuan untuk memudahkan Camat dalam menandatangani dokumen-dokumen penting secara daring.

19. Mengikuti Workshop Upaya Pemerintah Daerah dalam Rangka Peningkatan Kapasitas dan Kualitas SDM Pengelola Persandian dan Keamanan Siber Melalui Program Pengembangan Serta Pendidikan & Pelatihan di Dinas Kominfo Provinsi Sumatera Barat, pada tanggal 16 Oktober 2019. Hasil kegiatan ini adalah:

    a. Untuk mewujudkan SDM unggul berkarakter yang siap menghadapi ancaman terhadap keamanan dan ketahanan siber, BSSN bertanggung jawab dalam mengadakan Pendidikan dan Pelatihan Keamanan Siber.

    b. Jabatan Fungsional Sandiman merupakan jabatan yang mempunyai ruang lingkup, tugas, tanggung jawab dan wewenang untuk melakukan pengamanan informasi, pengamanan siber dan persandian.

    c. Sandiman berkedudukan sebagai pelaksana teknis di bidang keamanan informasi, keamanan siber dan persandian pada Instansi Pemerintah. Berkedudukan di bawah dan bertanggung jawab secara langsung kepada Pejabat Pimpinan Tinggi Pertama, Pejabat Administrator, atau Pejabat Pengawas yang memiliki keterkaitan dengan pelaksanaan tugas Jabatan Fungsional Sandiman, ditetapkan dalam peta jabatan sesuai dengan ketentuan peraturan perundang-undangan.

20. Mengikuti bimbingan teknis khusus persandian dan keamanan informasi oleh PT Inixindo di Yogyakarta, dengan materi *Web Application Penetration Testing* dan Pengelolaan Keamanan Informasi Pemda, pada tanggal 30 Oktober – 2 November 2019. Hasil kegiatan ini adalah:

a. Beberapa poin penting dalam mengikuti bimbingan teknis Web App Penetration Testing, terutama yg diujikan pada Website Pesisir Selatan sendiri adalah :

- Dalam proses *scanning*, dikarenakan *website* Pesisir Selatan pada saat testing belum dilengkapi *firewall* karena sedang proses migrasi dari server lama ke server yang baru menggunakan WAF/IDS/IPS pada *website*, sehingga memudahkan celah kami untuk masuk ke dalam sistem.
- Beberapa celah keamanan yang rentan banyak kemungkinan untuk dideteksi dengan mudah oleh tester ataupun orang yang ingin melakukan *hacking*, seperti XSS, BRUTEFORCE, dan SQL *injection* terutama pada halaman *login*.
- *Website* Pesisir Selatan terdeteksi mudahnya tester ataupun orang yang ingin melakukan *hacking* dengan SQL *injection* pada semua *website* Pesisir Selatan, sehingga dalam pelatihan ini kami dapat mengetahui dengan detail isi *database* yang terdapat pada *website* Pesisir Selatan, baik *username* maupun *password* admin *website*.
- Kategori celah keamanan : *Host Threats, Application Threats dan Network Threats.*
- Karna bahayanya SQL *injection* ini bagi *website*, diperlukan untuk perbaikan *coding*.
- Pentingnya pengelolaan keamanan informasi dalam lingkup Pemerintah Daerah.

b. Kegiatan Bimtek dengan Materi LSP Pengelolaan Keamanan Informasi di Inixindo Training For IT Professional. Beberapa poin penting dalam pembelajaran bimtek ini adalah sebagai berikut:

- Konsep Keamanan Informasi adalah:
- Confidentiality (kerahasiaan) bahwa keamanan informasi terjamin kerahasiaannya kepada mereka yang berhak untuk menerimanya dalam artian mencegah orang yang tidak berhak untuk mengakses informasi tersebut.

- Integrity (keutuhan) bahwa informasi yang diterima oleh penerima terjaga keutuhannya, tidak berubah dari aslinya.
- Avaibility (ketersediaan) bahwa informasi yang kita butuhkan bisa didapatkan kapan saja bisa jadi manusia ataupun komputer.
- Hal tersebut tidak akan berjalan dengan baik, Apabila Instansi/ Pemerintahan Daerah tidak mempunyai assessmen/kebijakan yang mengatur punishment/reward dan tenaga TIK maupun user IT yg professional dalam mengelola TIK tersebut.
- Komponen yang perlu diamakan adalah Network (jaringan) dan Application (aplikasi), tetapi yang terlebih penting untuk Pemerintah Daerah adalah aplikasi karena pada saat sekarang ancaman seperti hacking lebih banyak menyerang aplikasi.

21. Mengumpulkan dan merekap dokumen email Sanapati yang ditujukan ke Pemerintah Daerah Kabupaten Pesisir Selatan.
22. Melakukan serah terima peralatan sandi *Smart Jammer* PBJ630 dari Badan Siber dan Sandi Negara (BSSN), sekaligus bimbingan teknis dalam prosedur penggunaan *Smart Jammer* PBJ630 kepada operator yang akan bertanggung jawab mengoperasikan alat tersebut, pada tanggal 11 November 2019 di Dinas Kominfo Provinsi Sumatra Barat.

Diketahui Oleh:
KPA
Kepala Bidang Penyelenggaraan
e-Government dan Persandian

SYAFRUDIN, S.H., M.Si
NIP. 19650613 199703 1 001

Painan, Desember 2019
Disusun Oleh:
PPTK

NANANG SYUFRIADI, ST
NIP. 19850520 201001 1 028

DOKUMENTASI KEGIATAN

- Bimbingan teknis dalam prosedur penggunaan *Smart Jammer* PBJ630




- Workshop Upaya Pemerintah Daerah dalam Rangka Peningkatan Kapasitas dan Kualitas SDM Pengelola Persandian dan Keamanan Siber Melalui Program Pengembangan Serta Pendidikan & Pelatihan


- Pelatihan *IT Security Assessment* di Dinas Komunikasi dan Informatika Provinsi Sumatra Barat oleh Badan Siber dan Sandi Negara (BSSN)




- Sosialisasi tentang kegiatan standardisasi dan sertifikasi keamanan modul sandi, pengecekan/validasi dan pendataan produk keamanan siber dan sandi yang digunakan di Pemerintahan Daerah serta evaluasi pemanfaatan penggunaan peralatan sandi yang didistribusi oleh BSSN.



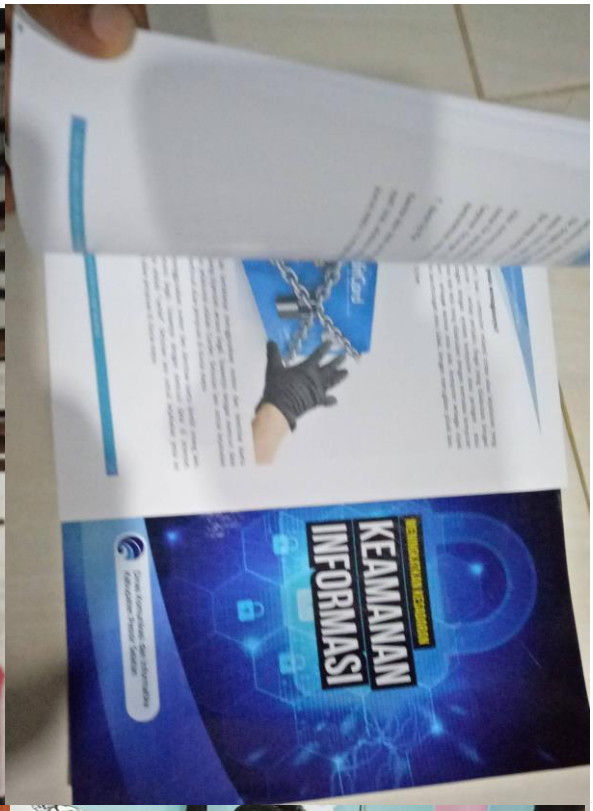

- Sosialisasi Sertifikat Elektronik oleh Narasumber dari Badan Siber dan Sandi Negara dan demo dalam penerapan sertifikat elektronik langsung ke Aplikasi siMAYA kepada Kepala OPD, Camat, dan Direktur Rumah Sakit di Lingkup Kabupaten Pesisir Selatan.




- Asistensi Pembentukan *CSIRT* (*Computer Security Incident Response Team*) Sektoral di Lingkungan Pemerintah Daerah.




- Mengikuti bimbingan teknis khusus persandian dan keamanan informasi oleh PT Inixindo di Yogyakarta, dengan materi Web Application Penetration Testing dan Pengelolaan Keamanan Informasi Pemda.


KEAMANAN
INFORMASI


PELAYANAN ADMINISTRASI TERPADU KECAMATAN
(PATEN)
BAYANG UTARA


PATEN
KECAMATAN SILAU


(PATEN)
BAYANG UTARA


LOKASI TPS KEC. SUTERA