Altha
spbe

Ceklis Keamanan Sistem Penghubung Layanan

Standar Teknis Keamanan Sistem Penghubung Layanan
Nama Instansi:
Nama Aplikasi:
Tanggal Asesmen:

Fungsi		Prosedur	Ya	Tidak	Keterangan
Keamanan interoperabilitas data dan informasi	1.1	Menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik			
Keamanan interoperabilitas data dan informasi	1.2	Menerapkan sistem enkripsi data			
Keamanan interoperabilitas data dan informasi	1.3	Memastikan data dan informasi selalu dapat diakses sesuai otoritasnya			
Keamanan interoperabilitas data dan informasi	1.4	Menerapkan sistem hash function pada file			
Kontrol sistem integrasi	2.1	Menerapkan protokol secure socket layer atau protokol transport layer security versi terkini pada sesi pengiriman data dan informasi			
Kontrol sistem integrasi	2.2	Menerapkan internet protocol security untuk mengamankan transmisi data dalam jaringan berbasis transmission control protocol/internet protocol			
Kontrol sistem integrasi	2.3	Menerapkan sistem anti distributed denial of service			
Kontrol sistem integrasi	2.4	Menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung			
Kontrol sistem integrasi	2.5	Menerapkan manajemen keamanan sesi			
Kontrol sistem integrasi	2.6	Menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan			
Kontrol sistem integrasi	2.7	Menerapkan validasi input			
Kontrol sistem integrasi	2.8	Menerapkan kriptografi pada verifikasi statis			
Kontrol sistem integrasi	2.9	Menerapkan sertifikat elektronik pada web authentication			
Kontrol sistem integrasi	2.10	Menerapkan penanganan eror dan pencatatan log			
Kontrol sistem integrasi	2.11	Menerapkan proteksi data dan jalur komunikasi			
Kontrol sistem integrasi	2.12	Menerapkan pendeteksi virus untuk memeriksa beberapa konten file			
Kontrol sistem integrasi	2.13	Menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus)			
Kontrol sistem integrasi	2.14	Memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi			
Kontrol perangkat integrator	3.1	Menggunakan sistem operasi dan perangkat lunak dengan security patches terkini			
Kontrol perangkat	3.2	Menggunakan anti virus dan anti-spyware terkini			
Kontrol perangkat	3.3	Mengaktifkan fitur keamanan pada peramban web			
Kontrol perangkat	3.4	Menerapkan firewall dan host-based intrusion detection systems			
Kontrol perangkat	3.5	Mencegah instalasi perangkat lunak yang belum terverifikasi			
Kontrol perangkat	3.6	Mencegah akses terhadap situs yang tidak sah			
Kontrol perangkat	3.7	Mengaktifkan sistem recovery dan restore pada perangkat integrator			
Keamanan API dan Web Service	4.1	Menerapkan protokol secure socket layer atau protokol transport layer security diantara pengirim dan penerima API			
Keamanan API dan Web Service	4.2	Menerapkan protokol open authorization versi terkini untuk menjembatani interaksi antara resource owner, resource server dan/atau third party			
Keamanan API dan Web Service	4.3	Menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid			
Keamanan API dan Web Service	4.4	Melindungi layanan web RESTful yang menggunakan cookie dari cross-site request forgery			
Keamanan API dan Web Service	4.5	Memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.			
Keamanan migrasi data	5.1	Memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem			
Keamanan migrasi data	5.2	Memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal			
Keamanan migrasi data	5.3	Mendokumentasikan format sistem basis data lama secara rinci			
Keamanan migrasi data	5.4	Melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data			
Keamanan migrasi data	5.5	Menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data			
Keamanan migrasi data	5.6	Melakukan validasi data ketika proses migrasi data selesai			

Nama Personil:	
Jabatan Personil:	