LAMPIRAN : KEPUTUSAN KEPALA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KABUPATEN BANTUL
NOMOR: IKMT-PIAK-01-12
TANGGAL: 30 Januari 2023

DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KABUPATEN BANTUL

PROSEDUR BAKU PELAKSANAAN KEGIATAN INSTRUKSI KERJA MANAJEMEN TERINTEGRASI (IKMT)

KEAMANAN INFORMASI

PEMERINTAH KABUPATEN BANTUL

DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL

Nomor IKMT	IKMT-PIAK-01-12
Tanggal Pembuatan	30 Januari 2023
Tanggal Revisi	
Tanggal Efektif	
Disahkan oleh	Kepala Dinas Kependudukan dan Pencatatan Sipil
Nama IKMT	Asesmen Keamanan Informasi untuk Aplikasi Web yang Dihosting Pada Data Center Pemerintah Kabupaten Bantul di Disdukcapil Kabupaten Bantul

DASAR HUKUM

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah
3. Peraturan Daerah Kabupaten Bantul Nomor 8 Tahun 2019 tentang Perubahan Atas Peraturan Daerah Kabupaten Bantul Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Bantul.
4. Peraturan Bupati Bantul Nomor 23 Tahun 2016 tentang Pedoman Penyusunan Standar Operasional Prosedur
5. Peraturan Bupati No. 45 Tahun 2019 Tentang Pelaksanaan Dan Pengelolaan Keamanan Sistem Informasi
6. Peraturan Bupati No. 50 Tahun 2019 Tentang Pengembangan Dan Pengelolaan Aplikasi Sistem Informasi
7. Peraturan Bupati No. 110 Tahun 2019 Kedudukan, Susunan Organisasi, Tugas, Fungsi, Dan Tata Kerja Dinas Komunikasi Dan Informatika Kabupaten Bantul
8. Peraturan Bupati Bantul Nomor 132 Tahun 2020 Tentang Sistem Pemerintahan Berbasis Elektronik Dalam Penyelenggaraan Pemerintahan Daerah.

KUALIFIKASI PELAKSANA

1. Memiliki kemampuan membangun aplikasi web yang sesuai dengan standar keamanan.
2. Memiliki kemampuan analisis terhadap spesifikasi perangkat lunak yang digunakan pada aplikasi web.
3. Memiliki kemampuan untuk melakukan asesmen keamanan informasi pada aplikasi web.
4. Memiliki kemampuan analisis terhadap celah-celah keamanan yang ada pada aplikasi web.

KETERKAITAN

1. SOP Pelayanan Administrasi Surat Masuk
2. SOP Pelayanan Administrasi Surat Keluar
3. SOP Pembangunan dan/atau Pengembangan Aplikasi.

PERALATAN/PERLENGKAPAN

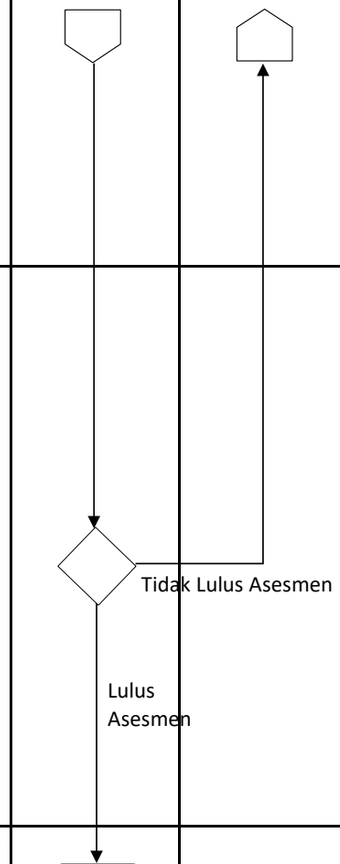
1. Komputer / Laptop dan Jaringan internet
2. Peralatan (tools) asesmen keamanan informasi.
3. Aplikasi web yang akan diasesmen.

PERINGATAN		PENCATATAN DAN PENDATAAN	
1	Apabila prosedur ini dilaksanakan, spesifikasi perangkat lunak pada aplikasi web dapat terpantau dan dapat ditindaklanjuti secara cepat dan tepat untuk menghindari adanya celah keamanan pada aplikasi web.	1	Surat permohonan hosting Dukcapil Kabupaten Bantul dari Perangkat Daerah terkait.
2	Apabila prosedur ini tidak dilaksanakan, aplikasi web berpotensi menjadi sasaran serangan siber sekaligus berpotensi menjadi pintu masuk serangan siber yang mengancam aplikasi-aplikasi lain yang berada dalam satu data center.	2	Lembar Check list asesmen keamanan informasi untuk aplikasi web.
3	Apabila prosedur ini dilaksanakan oleh pihak-pihak atau individu yang tidak memiliki kompetensi yang disebutkan, proses asesmen keamanan informasi pada aplikasi web tidak akan berjalan dengan baik. Sebab seluruh aspek yang mungkin harus dianalisis, dilaporkan, lengkap dan diperbaiki tidak akan terindentifikasi secara lengkap	3	Laporan hasil asesmen keamanan informasi.
		4	Sertifikat lulus asesmen keamanan informasi.

PELAKSANA KEGIATAN		PENCATATAN DAN PENDATAAN
1	Seksi Keamanan Infomrasi dan Persandian Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bantul	
2	Perangkat Daerah penanggung jawab aplikasi web.	

Pelaporan dan Penanganan Insiden Siber

No.	Uraian Prosedur	Pelaksana		Mutu Buku			
		Seksi Keamanan Informasi	Penanggung Jawab Aplikasi	Persyaratan / Kelengkapan	Waktu	Output	Ket
1	Pengumpulan informasi pada aplikasi web yang akan diasesmen.			• Komputer/Laptop	1 hari	-	
2	Pelaksanaan asesmen keamanan informasi pada aplikasi web meliputi kegiatan sebagai berikut: a. Pemeriksaan perangkat lunak yang dipergunakan. b. Pemeriksaan pengaturan hak akses file dan folder pada direktori server (directory listing). c. Pemeriksaan standar keamanan yang digunakan pada fitur pembuatan password. d. Pemeriksaan kerentanan SQL, nosql, OS, dan LDAP Injection pada database. e. Pemeriksaan fitur Captcha. f. Pemeriksaan kerentanan terhadap serangan Cross-Site Scripting (XSS). g. Pemeriksaan implementasi Cross-Site Request Forgery (CSRF) token. h. Pemeriksaan kerentanan fungsi file upload. i. Pemeriksaan implementasi password storage. j. Pemeriksaan penggunaan XML untuk webservice. k. Pemeriksaan konfigurasi pada cookie. l. Pemeriksaan access control. m.Pemeriksaan halaman back end. n. Pemeriksaan error handling. o. Pemeriksaan mode debug. p. Pemeriksaan fungsionalitas menu aplikasi web.			• Komputer/Laptop • Peralatan (tools) asesmen	5 hari	-	a. Perangkat lunak yang digunakan pada aplikasi web merupakan versi terbaru, ter-update, dan masih didukung secara penuh dan resmi oleh upstream provider. b. Memastikan file dan folder sensitif tidak bisa diakses oleh publik. c. Standar keamanan untuk password antara lain: - Berjumlah 8 karakter atau lebih. - Terdiri dari kombinasi huruf besar, huruf kecil, dan angka. - Menggunakan karakter tanda baca Contoh: !@#$%^&*()-=_+<>?”’{} dan sejenisnya. (Apabila tidak menggunakan karakter tanda baca maka jumlah karakter pada password minimal berjumlah 10 karakter.) d. Penyebab kerentanan SQL Injection adalah penulisan coding yang tidak memperhatikan best practice secure coding. e. Direkomendasikan menggunakan Captcha dari Google. f. Kerentanan Cross-Site Scripting (XSS) disebabkan oleh library yang tidak update dan/atau tidak dilakukan sanitasi dan validasi pada input pengguna. g. Cross-Site Request Forgery (CSRF) merupakan bentuk eksploitasi website yang dieksekusi atas wewenang korban, tanpa dikehendakinya h. Pada fungsi file upload tidak terdapat file upload yang executable, mengandung XML atau script yang berpotensi problem. i. Password storage menggunakan strong adaptive dan salted hashing functions / algoritma dengan delay factor, seperti Argon2, scrypt, bcrypt, atau PBKDF2). j. Menghindari penggunaan XML untuk webservice. k. Cookie menggunakan flag HttpOnly.

							l. Pada access control, pengguna hanya dapat mengakses menu, fitur, dan data sesuai dengan kewenangannya. m. Halaman back end menggunakan alamat custom, yaitu tidak menggunakan alamat /admin, /login, dan sejenisnya. n. Pada error handling, apabila aplikasi mengalami error, maka aplikasi memberikan respon terhadap error tersebut, melalui notifikasi pop-up atau redirect ke halaman awal. o. Mode debug harus off atau tidak aktif. p. Seluruh menu pada aplikasi berfungsi sebagaimana mestinya.
3	Analisis dan penyusunan laporan hasil asesmen keamanan informasi. Keterangan: a. Aplikasi web dinyatakan LULUS Analisis dan penyusunan laporan hasil asesmen keamanan informasi. Keterangan: a. Aplikasi web dinyatakan LULUS ASESMEN dengan syarat tidak ditemukan adanya celah keamanan pada aplikasi web atau celah keamanan yang ditemukan merupakan celah keamanan dengan resiko keamanan tingkat rendah dan/atau informasi yang harus segera diperbaiki oleh penanggung jawab aplikasi. b. Aplikasi web dinyatakan TIDAK LULUS ASESMEN apabila ditemukan adanya celah keamanan pada aplikasi web dengan resiko keamanan tingkat sedang dan/atau tinggi sedang dan/atau kritis yang harus segera diperbaiki oleh penanggung jawab aplikasi.			• Hasil analisis • Komputer/Laptop	2 hari	Laporan hasil asesmen keamanan informasi.	
4	Penerbitan sertifikat lulus asesmen keamanan informasi sebagai rekomendasi pemasangan aplikasi web pada Data Center Pemerintah Kabupaten Bantul di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bantul.			• Laporan hasil asesmen • Komputer/Laptop	1 hari	Sertifikat lulus asesmen keamanan informasi.	

Kepala Dinas

PEMERINTAH KABUPATEN BANTUL DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL

Bambang Purwadi Nugroho, S.H.,M.H.
Pembina Utama Muda - IV / c
NIP. 19710506 199603 1 003