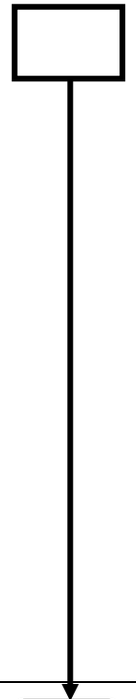
Nomor SOP	B/000.8.3.3/00493/INFRA/2026
Tanggal Pembuatan	16 Agustus 2021
Tanggal Revisi	30 Juni 2026
Tanggal Pengesahan	30 Juni 2026
Disahkan oleh	Kepala Dinas Komunikasi dan Informatika Kabupaten Bantul **BOBOT ARIFFI` AIDIN, S.T., M.T.** Pembina Utama Muda, IV/c NIP. 196906191996031003
Nama SOP	Asesmen Keamanan Informasi untuk Aplikasi Web Pada Pusat Data Pemerintah Kabupaten Bantul

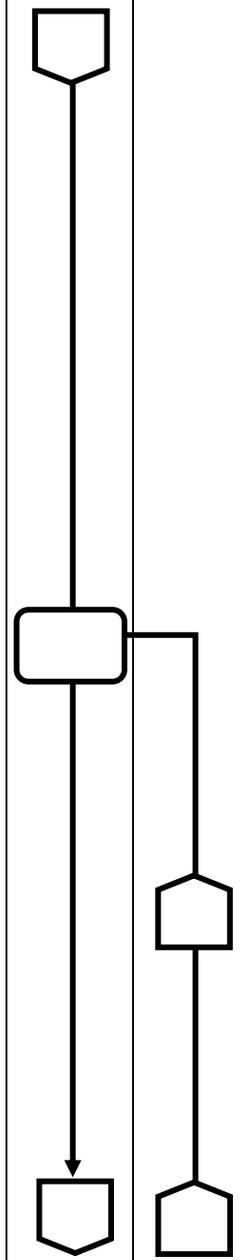
PEMERINTAH KABUPATEN BANTUL

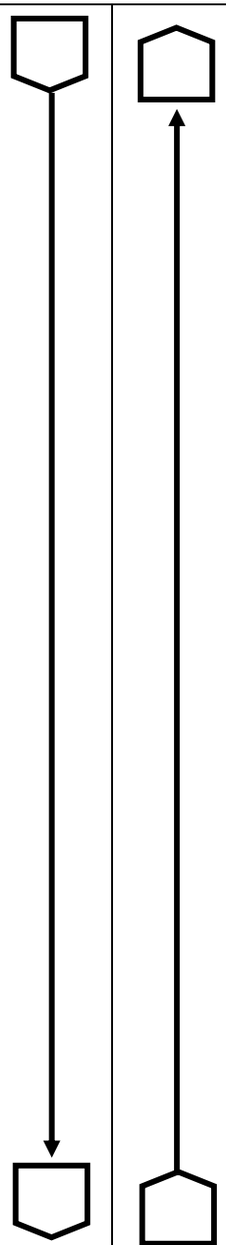
DINAS KOMUNIKASI DAN INFORMATIKA

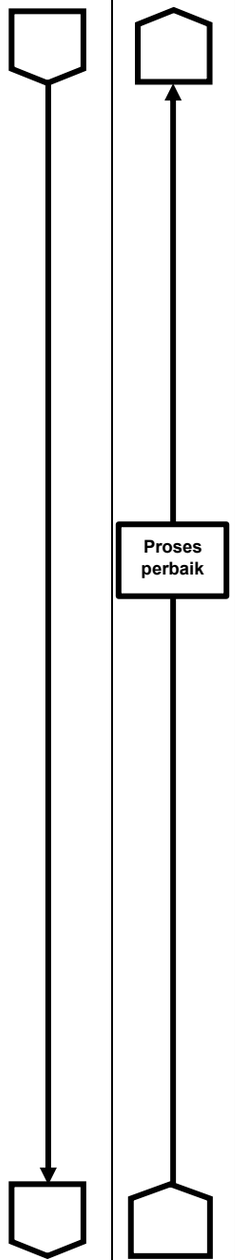
Dasar Hukum	Kualifikasi Pelaksana
1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. 2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah. 3. Peraturan Daerah Kabupaten Bantul 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 Nomor 45 Tahun 2019 tentang Pelaksanaan dan Pengelolaan Keamanan Sistem Informasi.	1. Memiliki kemampuan membangun aplikasi web sesuai standar keamanan. 2. Memiliki kemampuan melakukan instalasi aplikasi web pada server. 3. Memiliki kemampuan melakukan asesmen keamanan informasi pada aplikasi web.

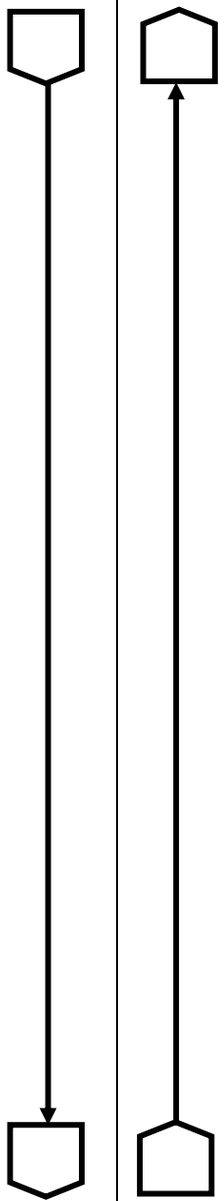
6. Peraturan Bupati Nomor 50 Tahun 2019 tentang Pengembangan dan Pengelolaan Aplikasi Sistem Informasi. 7. Peraturan Bupati Bantul Nomor 50 Tahun 2023 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Pada Pemerintah Kabupaten Bantul. 8. Peraturan Bupati Bantul Nomor 30 Tahun 2023 tentang Pembangunan dan Pengembangan Aplikasi Sistem Pemerintahan Berbasis Elektronik. 9. Peraturan Bupati Bantul Nomor 35 Tahun 2023 tentang Sistem Manajemen Keamanan Informasi.	
Keterkaitan	**Peralatan / Perlengkapan**
1. SOP Pelayanan Administrasi Surat Masuk. 2. SOP Pelayanan Administrasi Surat Keluar. 3. SOP Layanan Hosting. 4. SOP Pembangunan dan/atau Pengembangan Aplikasi.	1. Komputer / Laptop. 2. Server. 3. Aplikasi web yang akan diasesmen. 4. Peralatan (tools) asesmen keamanan informasi.
Peringatan	**Pencatatan dan Pendataan**
1. Jika prosedur ini dilaksanakan, spesifikasi perangkat lunak aplikasi web dapat terpantau dan ditindaklanjuti secara cepat untuk mencegah celah keamanan. 2. Jika prosedur ini tidak dilaksanakan, aplikasi web berpotensi menjadi sasaran serangan siber dan dapat mengancam aplikasi lain yang berada dalam satu server atau data center. 3. Jika prosedur ini dilaksanakan oleh pihak yang tidak kompeten, proses asesmen keamanan informasi tidak akan berjalan efektif, sehingga seluruh aspek yang harus dianalisis, dilaporkan, dan diperbaiki tidak teridentifikasi secara lengkap.	1. Surat permohonan hosting / subdomain / asesmen keamanan informasi aplikasi. 2. Surat Rekomendasi Rencana dan Anggaran SPBE. 3. Dokumen Software Requirement Specification (SRS). 4. Dokumen Application Deployment. 5. Dokumen User Acceptance Testing (UAT). 6. Dokumen User Manual / petunjuk penggunaan aplikasi. 7. Dokumen Application Programming Interface (API). 8. Berita Acara Serah Terima (BAST) aplikasi. 9. Laporan hasil asesmen keamanan informasi. 10. Lembar pengesahan asesmen keamanan informasi.
Pelaksana Kegiatan	
1. Tim kerja yang membidangi Keamanan Informasi dan Persandian Dinas Komunikasi dan Informatika Kabupaten Bantul. 2. Tim kerja yang membidangi Infrastruktur Teknologi Informasi Pemerintah Dinas Komunikasi dan Informatika Kabupaten Bantul. 3. Perangkat Daerah penanggung jawab aplikasi web dan/atau pengembang aplikasi.	

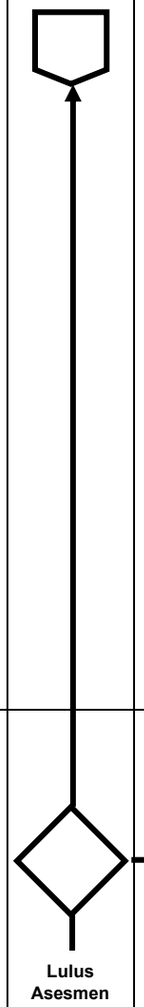
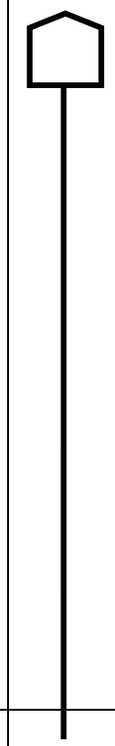
No.	Uraian Kegiatan	Pelaksana			Mutu Baku			Keterangan
		1	2	3	Perlengkapan	Waktu	Output	
1.	Pemenuhan kelengkapan dokumen pengembangan aplikasi.				-	7 hari	-	Dokumen pengembangan aplikasi yang dilengkapi antara lain: a. Surat permohonan hosting / subdomain / asesmen. b. Surat Rekomendasi Rencana dan Anggaran SPBE. c. Dokumen Software Requirement Specification (SRS). d. Dokumen Application Deployment. e. Dokumen User Acceptance Testing (UAT). f. Dokumen User Manual / petunjuk penggunaan aplikasi. g. Dokumen Application Programming Interface (API) apabila aplikasi menggunakan web service. h. Berita Acara Serah Terima (BAST) apabila aplikasi merupakan hibah dari pihak ketiga.
2.	Pengunggahan kode sumber (source code) aplikasi ke repository.				Komputer/ Laptop	3 hari	-	Alamat *repository*: https://vhessel.bantulkab.go.id
3.	Pemasangan aplikasi di server development.				Komputer/ Laptop	3 hari	-	Alamat domain: https://kab-bantul.id

4.	Pelaksanaan asesmen keamanan informasi meliputi pemeriksaan terhadap: a. Keamanan perangkat lunak. b. Kekuatan dan kebijakan kata sandi. c. Kerentanan Injection. d. Implementasi CAPTCHA. e. Kerentanan file upload. f. Implementasi password storage. g. Keamanan API/Web Service. h. Konfigurasi cookie. i. Access control. j. Kerentanan Cross-Site Scripting (XSS). k. Pembatasan percobaan login. l. Implementasi CSRF token. m. Hak akses file dan folder (directory listing). n. Keamanan halaman backend. o. Auto sign-out (session timeout). p. Penggunaan mode debug. q. Masa berlaku cookie (cookie expiration). r. Implementasi Multi-Factor Authentication (MFA).				- Komputer / Laptop - Peralatan (*tools)* asesmen	14 hari	-	**a. Keamanan Perangkat Lunak** Perangkat lunak, framework, library, dan komponen pendukung yang digunakan dalam aplikasi web harus menggunakan versi yang masih didukung oleh pengembang, diperbarui secara berkala, serta dipastikan tidak menggunakan komponen yang telah mencapai akhir masa dukungan (end of life). **b. Kekuatan dan kebijakan Kata Sandi** Sistem harus menerapkan kebijakan kata sandi yang memenuhi standar keamanan, yaitu minimal terdiri dari 8 karakter dengan kombinasi huruf besar, huruf kecil, dan angka, serta dianjurkan menggunakan karakter khusus. Apabila tidak menggunakan karakter khusus, maka panjang kata sandi minimal 10 karakter. Sistem harus memaksa penggantian kata sandi secara otomatis setiap 90 hari atau sesuai kebijakan keamanan yang berlaku. **c. Kerentanan Injection** Pengembangan aplikasi harus menerapkan prinsip secure coding untuk mencegah kerentanan injection terhadap SQL, NoSQL, OS, dan LDAP, termasuk memastikan bahwa setiap input dari pengguna divalidasi dan tidak dapat digunakan untuk mengeksekusi perintah atau query berbahaya pada sistem atau basis data.

								**d. Implementasi CAPTCHA** Sistem dianjurkan menerapkan mekanisme CAPTCHA sebagai langkah pencegahan terhadap akses otomatis oleh bot atau program otomatis. Penggunaan layanan CAPTCHA dari Google atau layanan sejenis direkomendasikan. **e. Keamanan Fungsi Unggah Berkas** Fungsi unggah berkas harus dilengkapi dengan mekanisme validasi tipe file dan isi file untuk memastikan bahwa file yang diunggah tidak bersifat executable, tidak mengandung XML, maupun script yang berpotensi menimbulkan kerentanan keamanan. **f. Keamanan Penyimpanan Kata Sandi** Penyimpanan kata sandi harus menggunakan algoritma hashing yang kuat dengan mekanisme adaptive dan salted hashing functions, seperti Argon2, scrypt, bcrypt, atau PBKDF2, sehingga kata sandi tidak tersimpan dalam bentuk teks biasa (plaintext). **g. Keamanan API atau Web Service** Implementasi API atau web service harus memperhatikan aspek keamanan komunikasi dan pertukaran data, termasuk menghindari penggunaan format XML yang berpotensi menimbulkan kerentanan keamanan serta memastikan mekanisme autentikasi

								dan validasi data diterapkan dengan baik. **h. Konfigurasi Cookie** Cookie yang digunakan oleh aplikasi harus dikonfigurasi dengan atribut keamanan seperti flag Secure dan HttpOnly guna mengurangi risiko pencurian cookie melalui koneksi tidak aman maupun serangan berbasis script. **i. Pengendalian Akses (Access Control)** Sistem harus menerapkan mekanisme pengendalian akses yang memastikan setiap pengguna hanya dapat mengakses menu, fitur, dan data sesuai dengan hak akses atau kewenangan yang dimilikinya berdasarkan peran atau otorisasi yang telah ditetapkan. **j. Kerentanan Cross-Site Scripting (XSS)** Sistem harus memastikan bahwa seluruh input dari pengguna telah melalui proses validasi dan sanitasi yang memadai serta menggunakan library yang selalu diperbarui guna mencegah potensi kerentanan Cross-Site Scripting (XSS). **k. Pembatasan Percobaan Login** Sistem harus menerapkan pembatasan jumlah percobaan login dalam periode waktu tertentu guna mencegah serangan brute force terhadap akun pengguna.

								l. **Implementasi Token CSRF** Sistem harus menerapkan mekanisme token Cross-Site Request Forgery (CSRF) untuk memverifikasi setiap permintaan yang dikirimkan oleh pengguna sehingga mencegah eksploitasi yang dapat menjalankan perintah atas nama pengguna tanpa sepengetahuannya. m. **Hak Akses File dan Folder** Pengaturan hak akses pada file dan folder di server harus memastikan bahwa file atau direktori yang bersifat sensitif tidak dapat diakses oleh publik serta fitur directory listing pada server tidak diaktifkan. n. **Keamanan Halaman Backend** Halaman backend atau panel administrasi harus menggunakan alamat khusus (custom path) dan tidak menggunakan alamat umum seperti /admin, /login, atau sejenisnya untuk mengurangi potensi percobaan akses tidak sah. o. **Implementasi Auto Sign-Out** Sistem harus menerapkan mekanisme auto sign-out atau session timeout yang secara otomatis mengakhiri sesi pengguna setelah periode tertentu tanpa aktivitas guna mencegah penyalahgunaan akses. p. **Penggunaan Mode Debug** Mode debug pada aplikasi harus dinonaktifkan pada lingkungan produksi untuk mencegah terbukanya informasi teknis sistem yang dapat

								dimanfaatkan oleh pihak yang tidak berwenang. q. **Masa Berlaku Cookie (Cookie Expiration)** Cookie sesi login harus dikonfigurasi dengan masa berlaku (Max-Age/Expires) paling lama 1 (satu) hari sejak diterbitkan, agar otomatis terhapus oleh browser. Ketentuan ini melengkapi atribut Secure dan HttpOnly pada konfigurasi cookie serta mekanisme auto sign-out, guna membatasi masa pakai cookie r. **Implementasi Multi-Factor Authentication (MFA)** Sistem harus menerapkan autentikasi multi-faktor sebagai lapisan tambahan selain kata sandi, guna mencegah penyalahgunaan akun yang kredensialnya bocor.
5.	Penyusunan laporan asesmen keamanan informasi dan lembar pengesahannya.			-	- Komputer/ Laptop	3 hari	- Laporan asesmen keamanan informasi - Lembar pengesah-an	a. Aplikasi web dinyatakan LULUS asesmen keamanan informasi jika memenuhi standar keamanan yang tercantum pada SOP ini. b. Untuk aplikasi baru akan disusun lembar pengesahan sedangkan untuk aplikasi lama hanya laporan asesmen keamanan informasi saja.
6.	Penyampaian laporan asesmen keamanan informasi dan lembar pengesahannya.			-	- Komputer/ Laptop	1 hari	-	Laporan asesmen keamanan informasi dan lembar pengesahan akan dikirimkan melalui aplikasi persuratan (SURBAN) ke perangkat daerah terkait.