



**PEMERINTAH KOTA BATAM
DINAS KOMUNIKASI DAN INFORMATIKA**

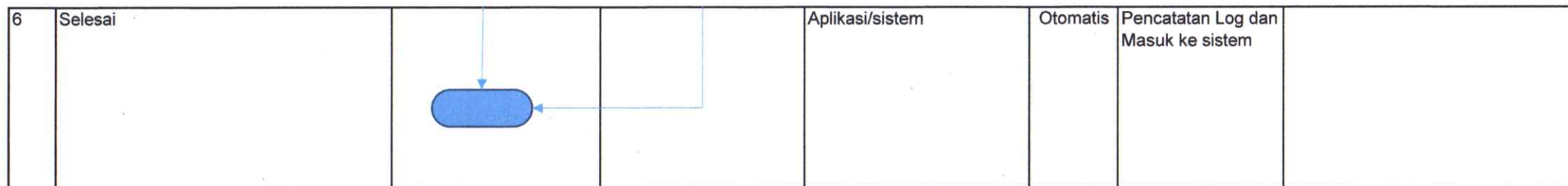
Bidang Pengelolaan Informasi Publik, Informatika, dan Persandian

Nomor SOP	07 /SOP/KOMINFO-PIPIP/II/2026
Tanggal Pembuatan	06 Maret 2026
Tanggal Revisi	
Tanggal Efektif	06 Maret 2026
Disahkan Oleh	Kepala Dinas Komunikasi dan Informatika Kota Batam  Rudi Panjaitan, S.STP., M.Si Pembina Utama Muda / IVC NIP. 19761123 199511 1 002
Nama SOP	AUTENTIKASI

Dasar Hukum	Kualifikasi Pelaksana
1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik; 2. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia 3. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik. 4. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah 5. Peraturan Menteri PANRB Nomor 59 Tahun 2020 Tentang Pemantauan dan Evaluasi SPBE. 6. Peraturan Menteri PANRB Nomor 7 Tahun 2022 Tentang Arsitektur SPBE Nasional 7. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541); 9. Peraturan Wali Kota Batam Nomor 65 Tahun 2022 tentang Penyelenggaraan Manajemen Keamanan Informasi Sistem Pemerintah Berbasis Elektronik di Lingkungan Pemerintah Kota Batam;	1. Memahami prosedur autentikasi yang berlaku 2. Mampu mengoperasikan sistem atau alat autentikasi 3. Mengerti standar keamanan data/informasi 4. Memahami risiko dan cara pencegahan kecurangan

10. Peraturan Wali Kota Batam Nomor 67 Tahun 2023 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam; 11. Peraturan Wali Kota Batam Nomor 37 Tahun 2024 tentang Tugas Pokok, Fungsi, Uraian Tugas, dan Sistem Kerja di lingkungan Dinas Komunikasi dan Informatika.	
Keterkaitan	Peralatan / Perlengkapan
1. SOP Manajemen Sesi 2. SOP Kontrol Akses Aplikasi 3. SOP Validasi Input 4. SOP Kriptografi 5. SOP Error Handling	1. Perangkat Komputer 2. Perangkat Printer 3. Kertas 4. Jaringan Internet 5. SSL/TLS Certificate 6. Database Terenkripsi 7. Koneksi Jalur Komunikasi Aman 8. Server Autentikasi
Peringatan	Pencatatan dan Pendataan
1. Pencatatan log yang tidak lengkap akan mengakibatkan kegagalan dalam pengawasan dan investigasi 2. Sistem wajib mengamankan penyimpanan kata sandi menggunakan mekanisme hash	1. Pencatatan dan Pendataan dilaksanakan secara elektronik

Autentikasi							
No	Kegiatan	Pelaksana		Mutu Baku			Ket
		Pengguna	Sistem	Kelengkapan	Waktu	Output	
1	Memasukkan nama pengguna, kata sandi dan informasi lainnya melalui jalur komunikasi aman (HTTPS/TLS)	<pre> graph TD subgraph Pengguna U([User]) P1[] end subgraph Sistem S1[] D{ } S2[] end U --> S1 S1 --> D D -- Diterima --> P1 D -- Ditolak --> S2 </pre>		Peramban/SSL	1 Menit	Data Login Terkirim	
2	Menyaring permintaan bot dan mesin			Server Auth	Otomatis	Hasil penyaringan	
3	Melakukan verifikasi nama pengguna dan kata sandi pada sisi server secara terenkripsi			Server Auth	Otomatis	Validitas Kredensial	
4	Autentikasi ditolak dan sistem mencatat insiden dan membatasi akses jika perlu			Server Auth dan Kebijakan Password	Otomatis	Pencatatan Log	
5	Autentikasi diterima			Aplikasi/sistem	Otomatis	Pencatatan Log dan Masuk ke sistem	



Keterangan :



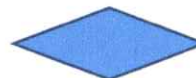
Terminator

Simbol yang menyatakan awal atau akhir suatu program



Process

Simbol yang menyatakan suatu proses yang dilakukan komputer



Decision

Simbol yang menunjukkan kondisi tertentu yang akan menghasilkan dua kemungkinan jawaban, iya atau tidak