BADAN PENANGGULANGAN BENCANA DAERAH KABUPATEN BANTUL	**STANDAR OPERASIONAL PROSEDUR (SOP) MANAJEMEN KEAMANAN INFORMASI**	NOMOR SOP	02/2584
		TGL. PEMBUATAN	05 Februari 2026
		TGL. REVISI	-
		TGL. EFEKTIF	05 Februari 2026
		DISAHKAN OLEH	MUJAHID AMRUDIN, S.IP.,M.E
		NAMA SOP	SOP Manajemen Keamanan Informasi
		HALAMAN	1 dari 3

DASAR HUKUM: 1. Peraturan Menteri PANRB No. 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan. 2. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). 3. Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). 4. Peraturan Badan Siber dan Sandi Negara (BSSN) tentang Standar Keamanan Informasi.	**KUALIFIKASI PELAKSANA:** 1. Memahami konsep CIA Triad (Confidentiality, Integrity, Availability). 2. Memiliki sertifikasi/keahlian di bidang Keamanan Informasi & Jaringan IT. 3. Memahami regulasi dan kebijakan tata kelola teknologi informasi. 4. Mampu melakukan analisis risiko dan penanganan insiden siber.
KETERKAITAN: 1. SOP Pengelolaan Hak Akses Pengguna. 2. SOP Cadangan dan Pemulihan Data (Backup & Recovery). 3. SOP Penanganan Insiden Keamanan Siber. 4. SOP Manajemen Perubahan Sistem (Change Management).	**PERALATAN / PERLENGKAPAN:** 1. Perangkat Server, Firewall, Router, dan Switch. 2. Sistem Antivirus / Antimalware / EDR Enterprise. 3. Media Penyimpanan Backup (Storage/Cloud Backup). 4. Aplikasi Ticketing Incident Response & SIEM.
PERINGATAN: Apabila SOP Manajemen Keamanan Informasi ini tidak dilaksanakan dengan baik, maka berisiko	**PENCATATAN DAN PENYIMPANAN:** 1. Log Aktivitas Sistem & Akses Pengguna

terjadinya kebocoran data rahasia (loss of confidentiality), manipulasi data tak sah (loss of integrity), atau gangguan ketersediaan sistem/layanan (loss of availability) yang dapat melumpuhkan operasional serta merugikan instansi/organisasi.	(Sistem Log). 2. Laporan Audit Keamanan dan Hasil Pentest. 3. Formulir Permohonan & Pencabutan Hak Akses. 4. Dokumen Laporan Kejadian Insiden Siber.

1. TUJUAN

SOP ini bertujuan untuk memberikan panduan standar dalam pengelolaan dan perlindungan aset informasi instansi/organisasi guna memastikan 3 (tiga) prinsip dasar keamanan informasi:

- **Confidentiality (Kerahasiaan):** Memastikan data dan informasi hanya dapat diakses oleh pihak/personel yang berhak dan memiliki wewenang (need-to-know basis).
- **Integrity (Integritas):** Memastikan data yang disimpan dan ditransmisikan dapat diandalkan, akurat, konsisten, serta bebas dari modifikasi, perusakan, atau gangguan yang tidak sah.
- **Availability (Ketersediaan):** Memastikan data, sistem, dan layanan informasi dapat diakses dan digunakan secara optimal saat dibutuhkan, termasuk saat terjadi gangguan operasional maupun bencana.

2. RUANG LINGKUP

SOP ini berlaku untuk seluruh ASN / Karyawan, Penyedia Jasa Pihak Ketiga, serta seluruh pengguna yang mengakses sistem, jaringan, dan aset data/informasi di lingkungan Badan Penanggulangan Bencana Daerah Kabupaten Bantul

3. PROSEDUR DAN ALUR KERJA (FLOWCHART)

No	Kegiatan	Pelaksana / Aktor	Mutu Baku: Kelengkapan	Mutu Baku: Waktu	Mutu Baku: Output
1	**Pengelolaan Kerahasiaan (Confidentiality)** a. Verifikasi hak akses pengguna berdasarkan role (Least Privilege). b. Aktivasi MFA dan penetapan password kompleks. c. Klasifikasi data & Enkripsi transmisi data sensitif. d. Penerapan kebijakan Clean Desk & Clear Screen.	- Pengguna - Admin IT - IT Security Officer	Form Pengajuan Akses, Matriks Hak Akses, Sertifikat Enkripsi/VPN	1 - 2 Hari Kerja	Hak akses terverifikasi, akun terenkripsi & terotorisasi
2	**Pengelolaan Integritas (Integrity)** a. Instalasi & update berkala antivirus/EDR. b. Pelaksanaan Patching OS & aplikasi rutin.	- Admin System - Database Administrator - IT Security Officer	Sistem Patch Management, Antivirus Enterprise, System Log Engine	Rutin (Harian/ Bulanan)	Sistem ter-patch, log terrekam, data tervalidasi bebas manipulasi

No	Kegiatan	Pelaksana / Aktor	Mutu Baku: Kelengkapan	Mutu Baku: Waktu	Mutu Baku: Output
	c. Penerapan Change Management & Digital Signature pada perubahan database. d. Aktivasi & rekapitulasi Log Audit Sistem.				
3	**Pengelolaan Ketersediaan (Availability)** a. Pelaksanaan Backup data rutin (metode 3-2-1). b. Uji coba pemulihan data (Restoration Test) berkala. c. Pemeliharaan sistem redundansi (UPS, Genset, Load Balancer). d. Penanganan insiden & aktivasi BCP/DRP saat gangguan.	- Admin Infrastructure - Tim Incident Response - IT Security Officer	Sistem Backup (Off-site/Cloud), Dokumen DRP/BCP, Network Monitoring Tool	Rutin / Sesuai SLA Insiden	Sistem redundan, data cadangan siap pakai, pemulihan layanan cepat
4	**Monitoring & Evaluasi Keamanan** Melakukan pemantauan berkala, audit internal, serta tinjauan manajemen keamanan informasi.	- CISO / IT Security - Tim Audit Internal	Checklist Audit Keamanan, Tool Vulnerability Assessment	Setiap 3 Bulan / Semester	Laporan Evaluasi Keamanan Informasi & Rekomendasi Perbaikan

Ditetapkan di : Bantul
Pada tanggal : 5 Februari 2026

MUJAHID AMRUDIN, S.IP.,M.E
Pembina Tingkat I, IV/b
NIP. 197005111998031002