SOP
Manajemen Keamanan Informasi
(08.01.001/AMI/D.1/SOP-SEKRE/2025)

PT AMI

PENGESAHAN DOKUMEN		
Disusun Oleh:	**Diperiksa Oleh:**	**Disahkan Oleh:**
Dian Ike Putri	Suryo Albar	Priyatno Bambang Hernowo
Supervisor Sekretariat	Direktur Operasional	Direktur Utama
Tgl. 1 Agustus 2025	Tgl. 6 Agustus 2025	Tgl. 11 Agustus 2025

Alamat: Jl. Janti KM. 4, Gedongkuning, Banguntapan, Bantul, D.I. Yogyakarta-Indonesia
Telp: +62 274 451034/+62 274 451035; Fax: +62 274 451034
E-mail: pt.anindya@gmail.com

1. TUJUAN

Melindungi informasi dari ancaman, menjaga agar data tetap rahasia, akurat, dan selalu tersedia, serta memastikan pengelolaannya sesuai hukum dan bersifat terbuka.

2. RUANG LINGKUP

SOP ini berlaku untuk semua karyawan PT Anindya Mitra Internasional dan pihak eksternal yang bekerjasama di PT Anindya Mitra Internasional.

3. ISTILAH DAN DEFINISI

3.1. **Keamanan Informasi**: Menjaga data dari ancaman agar tetap rahasia, utuh (akurat), dan siap digunakan.

3.2. **Insiden Keamanan**: Kejadian yang membahayakan keamanan informasi, seperti peretasan atau kebocoran data.

4. REFERENSI (ACUAN)

4.1. Undang-Undang Nomor 14 Tahun 2008: Tentang Keterbukaan Informasi Publik.

4.2. Undang-Undang Nomor 11 Tahun 2008: Tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016.

5. PENANGGUNG JAWAB

5.1. Direktur Utama

5.2. Kepala Sekretariat

5.3. Tim IT

5.4. Tim PPID

6. PROSEDUR MANAJEMEN KEAMANAN INFORMASI

6.1. Tim IT menerima laporan insiden keamanan informasi, melakukan validasi awal bersama tim PPID, dan meneruskan laporan ke Kepala Sekretariat.

6.2. Kepala Sekretariat melakukan analisis mendalam, identifikasi penyebab, dan investigasi terhadap insiden yang dilaporkan dengan Tim terkait dan Direktur Utama.

6.3. Melakukan tindakan yang diperlukan untuk menangani insiden, termasuk perbaikan teknis atau pemulihan aset informasi yang terdampak sesuai instruksi Direktur Utama.

6.4. Mendokumentasikan seluruh proses penanganan insiden, mulai dari awal hingga penyelesaian, sebagai bahan evaluasi dan arsip.

6.5. Melakukan evaluasi pasca-insiden untuk mengidentifikasi celah keamanan, dan merumuskan langkah-langkah perbaikan untuk mencegah kejadian serupa di masa mendatang.

7. FLOWCHART

7.1. Flowchart Manajemen Keamanan Informasi