KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI

UNIVERSITAS HASANUDDIN

PROSEDUR
KLASIFIKASI KEAMANAN INFORMASI

No. PT/UH/DSITD-18

Status Dokumen	:	☐	Master	☐ Salinan, No.
Nomor Revisi	: 00			
Tanggal Terbit	: 13 Juli 2023			

Dibuat oleh	Diperiksa oleh	Disahkan oleh
Kepala Seksi Teknologi Informasi dan Komunikasi	Direktur Sistem Informasi dan Transformasi Digital	Wakil Rektor Bidang SDM,Alumni dan Sistem Informasi
		
Luqman Hakim, ST	Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.	Prof. Dr. Farida Patittingi, S.H., M.Hum.

DAFTAR REVISI

No. Revisi	Tanggal	Penjelasan Revisi

DAFTAR ISI

TUJUAN	Memberikan panduan dalam klasifikasi informasi di universitas sesuai dengan tingkat sensitivitas dan keamanan yang dibutuhkan untuk melindungi informasi dari akses yang tidak sah, perubahan, atau kerusakan.
RUANG LINGKUP	SOP ini berlaku untuk seluruh informasi yang dihasilkan, disimpan, diproses, atau dikirim oleh universitas, termasuk informasi dalam bentuk fisik dan digital.
DEFINISI	1. **Informasi Sensitif:** Informasi yang jika diakses, diubah, atau dihapus tanpa izin dapat menyebabkan kerugian bagi universitas. 2. **Klasifikasi:** Proses mengkategorikan informasi berdasarkan tingkat kerahasiaan, integritas, dan ketersediaannya. 3. **Kategori Klasifikasi:** Publik, Internal, Terbatas, Rahasia.
KETENTUAN UMUM	1. Semua informasi harus diklasifikasikan sebelum digunakan, disimpan, atau didistribusikan. 2. Klasifikasi dilakukan oleh pemilik informasi atau pihak yang ditunjuk. 3. Setiap kategori informasi memiliki kontrol keamanan yang harus dipatuhi.
REKAMAN /CATATAN	Log Klasifikasi Informasi: Mendokumentasikan informasi yang telah diklasifikasikan beserta kategori dan kontrol keamanannya. Formulir Evaluasi Klasifikasi: Digunakan untuk penilaian klasifikasi awal dan tinjauan berkala.

UNIVERSITAS HASANUDDIN **DIREKTORAT SISTEM INFORMASI DAN TRANSFORMASI DIGITAL**	Nomor SOP	PT/UH/DSITD-18
	Tanggal Pembuatan/Terbit	13 Juli 2023
	Tanggal Revisi	-
	Tanggal Efektif	
	Disahkan Oleh	Wakil Rektor Bidang SDM,Alumni dan Sistem Informasi Prof. Dr. Farida Patittingi, S.H., M.Hum
	NAMA SOP	STANDAR KLASIFIKASI KEAMANAN INFORMASI

DASAR HUKUM / REFERENSI	KUALIFIKASI PELAKSANA
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional 2. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi 3. Undang Undang No.11 Tahun 2008 tentang Informasi & Transaksi Elektronik (ITE) 4. Peraturan Pemerintah RI No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) 5. Permenristekdikti No.75 tahun 2016 tentang Layanan Informasi Publik di Lingkungan Kementerian Riset dan Teknologi dan Pendidikan Tinggi 6. Peraturan Menteri Komunikasi dan Informatika RI No.20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik 7. SNI ISO 27001:2022 Sistem Manajemen Keamanan Informasi - Persyaratan, Annex A.1 Kontrol Keamanan Informasi : 5.12, 5.13	1. Memiliki pemahaman dan pelatihan mengenai keamanan informasi dan klasifikasi. 2. Mengetahui prosedur keamanan yang berlaku di universitas.
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
1. SOP Backup data 2. SOP Peninjauan hak akses 3. SOP Pengendalian hak akses	1. **Sistem Manajemen Keamanan Informasi :** Untuk mengelola dan memantau klasifikasi informasi. 2. **Software Enkripsi:** Untuk mengamankan informasi sensitif.

PERINGATAN	PENCATATAN/PENDATAAN
Ketidakpatuhan terhadap SOP ini dapat menyebabkan pelanggaran keamanan informasi yang serius, berdampak pada reputasi dan operasional universitas.	• Seluruh data klasifikasi harus dicatat dalam sistem yang aman dan hanya dapat diakses oleh pihak yang berwenang. • Data pencatatan harus ditinjau secara berkala untuk memastikan akurasi dan kepatuhan.

PROSEDUR :

1. **Identifikasi Informasi:** Identifikasi informasi yang akan diklasifikasikan.
2. **Penilaian Klasifikasi:** Gunakan Formulir Evaluasi Klasifikasi untuk menentukan kategori informasi (Publik, Internal, Terbatas, Rahasia).
3. **Penetapan Kategori:** Tetapkan kategori berdasarkan penilaian.
4. **Implementasi Kontrol:** Terapkan kontrol keamanan sesuai dengan kategori klasifikasi (misalnya, penggunaan enkripsi untuk informasi Rahasia).
5. **Pendokumentasian:** Catat hasil klasifikasi dalam Log Klasifikasi Informasi.
6. **Tinjauan Berkala:** Lakukan tinjauan berkala terhadap klasifikasi informasi untuk memastikan tetap relevan dan akurat.