KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI

UNIVERSITAS HASANUDDIN

PROSEDUR
PEMBUATAN PASSWORD

No. PT/UH/DSITD-15

Status Dokumen	:	☐	Master	☐ Salinan, No.
Nomor Revisi	: 00			
Tanggal Terbit	: 4 September 2024			

Dibuat oleh	Diperiksa oleh	Disahkan oleh
Kasubdit Teknologi Informasi dan Komunikasi	Direktur Sistem Informasi dan Transformasi Digital	Wakil Rektor Bidang SDM,Alumni dan Sistem Informasi
		
Muh. Yusni Ismail, S.T., M.T.	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

HALAMAN JUDUL 1
DAFTAR REVISI 2
DAFTAR ISI 3
TUJUAN 4
RUANG LINGKUP 4
DEFINISI 4
KETENTUAN UMUM 4
REKAMAN / CATATAN 4
PENGESAHAN 5
DASAR HUKUM / REFERENSI 5
KUALIFIKASI PELAKSANA 5
KETERKAITAN 5
PERLENGKAPAN/PERALATAN 5
PERINGATAN 6
PENCATATAN / PENDATAAN 6
PROSEDUR (DIAGRAM ALUR) 7

TUJUAN	Menetapkan prosedur standar untuk pembuatan, penggunaan, dan manajemen kata sandi guna melindungi akses ke sistem dan data penting sesuai dengan standar keamanan informasi ISO 27001:2022
RUANG LINGKUP	SOP ini berlaku untuk seluruh pengguna sistem informasi yang dikelola oleh Universitas, termasuk staf, dosen, mahasiswa, dan kontraktor.
DEFINISI	1. **Kata Sandi**: Kombinasi karakter yang digunakan untuk memverifikasi identitas pengguna dan memberikan akses ke sistem atau data. 2. **Multi-Factor Authentication (MFA)**: Proses autentikasi yang memerlukan lebih dari satu metode verifikasi dari kategori kredensial independen.
KETENTUAN UMUM	**1.** Semua kata sandi yang digunakan untuk akses ke sistem universitas harus memenuhi standar keamanan yang ditetapkan dalam SOP ini. **2.** Pengguna wajib menjaga kerahasiaan kata sandi dan tidak membagikannya kepada pihak lain. **3.** Kata sandi yang tidak lagi digunakan harus segera dinonaktifkan atau dihapus.
REKAMAN /CATATAN	List akun sistem informasi

UNIVERSITAS HASANUDDIN **DIREKTORAT SISTEM INDORMASI DAN TRANSFORMASI DIGITAL**	Nomor SOP	PT/UH/DSITD-15
	Tanggal Pembuatan/Terbit	4 September 2024
	Tanggal Revisi	-
	Tanggal Efektif	
	Disahkan Oleh	Wakil Rektor Bidang SDM,Alumni dan Sistem Informasi Prof. Dr. Farida Patittingi, S.H., M.Hum
	NAMA SOP	PEMBUATAN PASSWORD

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 Kementrian Riset dan Teknologi dan Pendidikan Tinggi 6. Peraturan Menteri Komunikasi dan Informatika RI No.20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistim Elektronik 7. SNI ISO 27001:2022 Sistem Manajemen Keamanan Informasi – Lampiran A, Kontorl Organisasi : 5.15, 5.18, Kontrol Teknologi : 8.2, 8.3, 8.5	1. Pengguna yang diizinkan untuk mengelola atau mengakses sistem harus telah mengikuti pelatihan keamanan informasi. 2. Pengguna harus memahami dan mematuhi kebijakan keamanan informasi yang berlaku di universitas.
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
• SOP Peninjauan Hak Akses • SOP Pengendalian Hak Akses • SOP Manajemen Insiden Keamanan Informasi	1. Laptop 2. Akses Internet

PERINGATAN	PENCATATAN/PENDATAAN
• **Pelanggaran Hak Akses:** Setiap pelanggaran hak akses, termasuk akses yang tidak sah atau penggunaan akses di luar wewenang, akan dianggap sebagai pelanggaran serius dan dapat berujung pada tindakan disipliner hingga pemutusan hubungan kerja. • **Audit Berkala:** Kegagalan dalam melaksanakan audit berkala dapat mengakibatkan ketidaksesuaian dengan persyaratan ISO 27001 dan meningkatkan risiko kebocoran informasi. • **Tanggung Jawab Hukum:** Penyalahgunaan hak akses yang menyebabkan kebocoran informasi atau kerugian pada universitas dapat berakibat pada tuntutan hukum terhadap individu terkait.	Disimpan sebagai data elektronik

PROSEDUR :

1. **Kriteria Pembuatan Kata Sandi**
    a. Kata sandi minimal terdiri dari 12 karakter.
    b. Harus mengandung kombinasi huruf besar, huruf kecil, angka, dan simbol.
    c. Tidak boleh menggunakan informasi pribadi yang mudah ditebak (misalnya, nama, tanggal lahir, atau kata umum).
    d. Kata sandi harus unik dan tidak boleh sama dengan kata sandi yang digunakan pada sistem lain.
2. **Penyimpanan dan Pengelolaan Kata Sandi**
    a. Kata sandi tidak boleh dicatat dalam bentuk teks biasa (plain text) atau dibagikan dengan orang lain.
    b. Penggunaan aplikasi pengelola kata sandi (password manager) direkomendasikan untuk menyimpan dan mengelola kata sandi dengan aman.
    c. Perubahan kata sandi harus dilakukan secara berkala, minimal setiap 90 hari.
3. **Penggunaan Multi-Factor Authentication (MFA)**
    a. Untuk sistem kritis atau akses ke data sensitif, penggunaan MFA diwajibkan.
    b. MFA dapat berupa kombinasi kata sandi dengan otentikasi tambahan seperti token, biometrik, atau kode verifikasi.
4. **Pelaporan dan Penanganan Insiden**
    a. Pengguna harus segera melaporkan jika ada indikasi pelanggaran keamanan kata sandi atau jika kata sandi dicurigai telah diketahui pihak yang tidak berwenang.
    b. Setelah pelaporan, pengguna wajib segera mengganti kata sandi yang terdampak.