



KEBIJAKAN RESET PASSWORD

Classification: **Internal**

Nomor Dokumen	Judul	Versi	Tanggal Berlaku	Pemilik Dokumen
033.R00/LTSI/SMKI/RESET-PASSWORD/IX/2025	Kebijakan Reset Password	1.0		Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI)

Contents

1. Pendahuluan	3
2. Tujuan.....	3
3. Ruang Lingkup	3
4. Kebijakan / Prinsip Inti	3
6. Peran & Tanggung Jawab	4
7. Acuan Dokumen Lain.....	4
8. Peninjauan & Persetujuan	4

1. Pendahuluan

Permintaan Reset Password memiliki risiko tinggi terhadap keamanan informasi apabila tidak diatur dengan baik. Oleh karena itu, diperlukan kebijakan yang mengatur proses reset password untuk memastikan bahwa proses dilakukan dengan benar, aman, terkendali, dan sesuai dengan prinsip keamanan informasi dan prosedur yang berlaku.

2. Tujuan

Kebijakan ini bertujuan untuk menetapkan prosedur dan kontrol keamanan dalam proses reset password untuk memastikan bahwa hanya pengguna yang sah dapat melakukan pemulihan akses, serta mencegah potensi penyalahgunaan atau akses tidak sah.

3. Ruang Lingkup

Kebijakan ini berlaku untuk:

1. Tim Layanan TSI DPTSI
2. Seluruh aplikasi dan layanan yang terintegrasi dalam myITS Portal
3. Seluruh pengguna yang membutuhkan bantuan dalam reset password untuk mengakses aplikasi dan layanan sistem di ITS.

4. Kebijakan / Prinsip Inti

Dalam proses permohonan dan melakukan reset password, terdapat sejumlah prinsip yang perlu dipatuhi serta larangan yang harus dihindari. Adapun ketentuan tersebut adalah sebagai berikut:

1. Permohonan reset password hanya dapat dilakukan oleh pengguna yang terverifikasi bahwa pengguna tidak bisa melakukannya secara mandiri dikarenakan email alternatif dan nomor telepon di myITS Portal belum diverifikasi.
2. Setiap permohonan harus diajukan melalui tiket di servicedesk, myITS Office, atau datang langsung ke DPTSI dengan melampirkan identitas pengguna, KTM/KTP/SIM, dan alasan permohonan dilakukan.
3. Tim Layanan TSI DPTSI melakukan verifikasi terhadap kesesuaian identitas pengguna dengan basis data di Microsoft Azure AD sebelum melakukan reset password.
4. Pembuatan password baru harus memenuhi standar kompleksitas:
 - a. Tidak boleh sama dengan password sebelumnya.
 - b. Minimal 8 karakter.
 - c. Menggunakan kombinasi huruf kapital, huruf kecil, dan angka
 - d. Penggunaan simbol seperti (!@#&\$%^&*) bersifat opsional namun dianjurkan untuk meningkatkan keamanan.
 - e. Tidak mengandung username/myITS ID atau bagian apapun dari nama pribadi mahasiswa.
 - f. Hindari password yang umum seperti: 12345, admin123, semangat, abcde.
 - g. Hindari password yang mengandung unsur tanggal lahir atau identitas mahasiswa.
 - h. Tidak boleh menggunakan spasi dalam password.
 - i. Contoh password yang benar: 4Nt4its%

5. Tim layanan LTSl harus mendokumentasikan semua permohonan reset password dalam sistem logbook atau sistem tiket resmi untuk kebutuhan operasional serta keperluan keamanan dan kepatuhan.

6. Peran & Tanggung Jawab

1. **Kasubdit LTSl**, bertanggung jawab untuk memastikan bahwa seluruh proses permohonan reset password berjalan sesuai dengan kebijakan dan prosedur yang telah ditetapkan.
2. **Tim Layanan TSl**, bertanggung jawab untuk melakukan verifikasi data permohonan serta melakukan reset password sesuai dengan prosedur yang telah ditetapkan.

7. Acuan Dokumen Lain

- ISO/IEC 27001:2022– Information Security Management System (ISMS).
- Prosedur Permohonan Reset Password.

8. Peninjauan & Persetujuan

Kebijakan ini harus ditinjau minimal setiap 1 (satu) tahun sekali atau setiap kali terjadi perubahan sistem, struktur organisasi, maupun peraturan keamanan informasi yang relevan.

Peran	Nama	Jabatan	Tanggal	Tanda Tangan
Disusun oleh	Vania Meilani Taqiyyah	Tim Layanan TSl DPTSl	30/09/2025	_____
Direview oleh	[Nama]	Direktur DPTSl	_____	_____
Disetujui oleh	[Nama]	Wakil Rektor III ITS	_____	_____