# **Functional Requirement: FR.022 - Manajemen Pengguna & Hak Akses**

## **1. Pendahuluan**

Dokumen ini merinci persyaratan fungsional untuk FR.022 - Manajemen Pengguna & Hak Akses dalam proyek Mini Bank Digital. Fungsionalitas ini adalah inti dari keamanan sistem, memungkinkan Administrator (Operator Officer) untuk mengelola akun pengguna, menetapkan peran, dan mengelola hak akses, memastikan bahwa setiap pengguna hanya memiliki akses ke fungsionalitas dan data yang sesuai dengan tanggung jawab mereka.

## **2. Deskripsi Fungsional**

Sistem harus menyediakan antarmuka yang memungkinkan Operator Officer (OO) untuk:

* **Membuat Pengguna Baru:** Memasukkan detail pengguna (nama, *username*, *email*, peran).
* **Mengelola Pengguna yang Ada:** Mengubah detail pengguna, mengatur ulang kata sandi, mengaktifkan/menonaktifkan akun.
* **Mengelola Peran:** Membuat, mengubah, atau menghapus peran (misalnya, Customer Service, Teller, Kepala Cabang, Operator Officer).
* **Mengelola Hak Akses:** Menetapkan izin spesifik untuk setiap peran terkait fungsionalitas dan data (misalnya, Teller dapat memproses setoran, tetapi tidak dapat melihat laporan keuangan Kepala Cabang).
* **Melihat Log Aktivitas Pengguna:** Melacak perubahan yang dilakukan pada konfigurasi pengguna dan hak akses.

Semua perubahan pada manajemen pengguna dan hak akses harus dicatat dalam *audit trail*.

## **3. User Stories**

* **OO-005:** Sebagai Operator Officer, saya ingin dapat membuat akun pengguna baru untuk staf bank, sehingga mereka dapat mengakses sistem sesuai dengan peran mereka.
  + **Acceptance Criteria (Contoh Utama):**
    - Diberikan saya mengakses modul manajemen pengguna, ketika saya mengklik "Tambah Pengguna Baru" dan mengisi semua detail yang diperlukan (nama, *username*, *email*, peran), maka sistem membuat akun baru dan mengirimkan kredensial awal kepada pengguna.
    - Diberikan saya mencoba membuat *username* yang sudah ada, ketika saya menyimpan, maka sistem menampilkan pesan kesalahan bahwa *username* sudah digunakan.
* **OO-006:** Sebagai Operator Officer, saya ingin dapat mengubah peran atau menonaktifkan akun pengguna yang ada, sehingga saya dapat menyesuaikan hak akses atau mencabut akses jika diperlukan.
  + **Acceptance Criteria (Contoh Utama):**
    - Diberikan saya mencari pengguna tertentu, ketika saya memilih pengguna tersebut dan mengubah perannya dari "Teller" menjadi "Kepala Cabang", maka hak akses pengguna tersebut diperbarui secara otomatis sesuai dengan peran baru.
    - Diberikan seorang karyawan telah mengundurkan diri, ketika saya menonaktifkan akunnya, maka pengguna tersebut tidak dapat lagi masuk ke sistem.
    - Diberikan saya mengubah detail pengguna atau status akun, ketika saya menyimpannya, maka perubahan tersebut dicatat dalam *audit trail*.

## **4. Tampilan Antarmuka Pengguna (UI)**

### **Manajemen Pengguna & Hak Akses:**

* **Fungsionalitas Utama:** Membuat, mengelola pengguna, peran, dan hak akses.
* **Peran Pengguna:** Operator Officer (OO).
* **Fitur Kunci/Catatan:**
  + **Daftar Pengguna:** Menampilkan semua pengguna dengan status dan peran mereka.
  + **Formulir Tambah/Edit Pengguna:** Untuk memasukkan dan mengubah detail pengguna.
  + **Manajemen Peran:** Antarmuka untuk mendefinisikan peran dan izinnya.
  + **Pencarian & Filter:** Untuk menemukan pengguna dengan mudah.

### **Tabel: Field List & Komponen UI untuk Modul Manajemen Pengguna & Hak Akses**

| **Seksi** | **Field / Komponen** | **Tipe / Control** |
| --- | --- | --- |
| **Daftar Pengguna** | Tabel Pengguna | Data Table (Kolom: Nama, Username, Email, Peran, Status, Aksi) |
|  | Tombol "Tambah Pengguna Baru" | Button |
|  | Input Pencarian | Text Input |
|  | Filter Peran | Dropdown |
| **Formulir Pengguna** | Nama Lengkap | Text Input |
|  | Username | Text Input |
|  | Email | Text Input |
|  | Kata Sandi (untuk reset/buat baru) | Password Input |
|  | Konfirmasi Kata Sandi | Password Input |
|  | Peran | Dropdown (CS, Teller, KC, OO, dll.) |
|  | Status Akun | Toggle Switch / Radio Button (Aktif, Nonaktif) |
|  | Tombol "Simpan" | Button |
|  | Tombol "Batal" | Button |
| **Manajemen Peran & Hak Akses** | Daftar Peran | List / Table (Kolom: Nama Peran, Deskripsi, Aksi) |
|  | Tombol "Tambah Peran Baru" | Button |
|  | Nama Peran | Text Input |
|  | Deskripsi Peran | Textarea |
|  | Daftar Izin/Hak Akses | Checkbox List (misal: "Proses Setoran", "Lihat Laporan Harian", "Kelola Produk Bank") |
|  | Tombol "Simpan Peran" | Button |
|  | Tombol "Batal" | Button |
| **Pesan Sistem** | Area Notifikasi/Pesan | Display Area |

## **5. Aturan Bisnis**

* Setiap pengguna harus memiliki *username* yang unik.
* Kata sandi harus memenuhi kebijakan keamanan yang ditetapkan (misalnya, panjang minimum, kombinasi karakter).
* Hanya Operator Officer (OO) yang memiliki hak untuk mengelola pengguna dan hak akses.
* Peran "Operator Officer" tidak dapat dinonaktifkan atau dihapus kecuali ada peran OO lain yang aktif.
* Setiap perubahan pada detail pengguna, peran, atau hak akses harus dicatat dalam *audit trail* (FR.009).
* Ketika peran pengguna diubah, hak akses mereka harus segera diperbarui sesuai dengan peran baru.
* Sistem harus mencegah pengguna memberikan hak akses yang melebihi hak akses mereka sendiri.

## **6. Persyaratan Non-Fungsional (NFRs)**

* **NFR.001 – Keamanan:** Modul ini harus sangat aman, dengan otentikasi yang kuat untuk Operator Officer dan perlindungan terhadap akses tidak sah. Semua data sensitif (misalnya, kata sandi) harus dienkripsi.
* **NFR.002 – Akurasi:** Informasi pengguna dan konfigurasi hak akses harus akurat dan konsisten.
* **NFR.003 – Kemudahan Penggunaan:** Antarmuka harus intuitif dan mudah digunakan untuk mengelola pengguna dan izin.
* **NFR.006 – Kinerja:** Operasi manajemen pengguna (misalnya, pencarian, penyimpanan perubahan) harus responsif.
* **NFR.007 – Kepatuhan:** Sistem harus mematuhi regulasi terkait manajemen akses dan pencatatan aktivitas pengguna.
* **NFR.008 – Skalabilitas:** Sistem harus mampu mengelola sejumlah besar pengguna dan peran tanpa penurunan kinerja yang signifikan.

## **7. Ketergantungan**

* Modul Otentikasi dan Otorisasi Pengguna (FR.001) sebagai dasar untuk verifikasi identitas.
* Modul Audit Trail (FR.009) untuk pencatatan semua perubahan.
* Basis data pengguna dan peran.

## **8. Asumsi**

* Ada kebijakan yang jelas mengenai siapa yang dapat menjadi Operator Officer dan tanggung jawab mereka.
* Proses *onboarding* dan *offboarding* karyawan di luar sistem telah ditentukan untuk memicu tindakan manajemen pengguna.

## **9. Isu Terbuka**

* Bagaimana penanganan jika seorang Operator Officer mengunci diri sendiri dari sistem secara tidak sengaja?
* Apakah ada mekanisme untuk otorisasi ganda untuk perubahan hak akses yang sangat sensitif?

## **10. Pertimbangan Masa Depan**

* Integrasi dengan sistem *Human Resources Information System* (HRIS) untuk otomatisasi pembuatan/penonaktifan akun.
* Implementasi *Single Sign-On* (SSO) untuk otentikasi yang lebih efisien.
* Fitur pelaporan kepatuhan terkait hak akses dan audit.
* Pemberitahuan otomatis kepada Operator Officer tentang aktivitas akun yang mencurigakan (misalnya, upaya login yang gagal berulang).

## 11. Test Scenario

### 1) Matriks Traceability FR → Test Scenario

| **FR Area** | **Deskripsi Singkat** | **TS ID yang Mencakup** | **Keterangan** |
| --- | --- | --- | --- |
| Akses Modul | OO dapat mengakses modul Manajemen Pengguna & Hak Akses | TS-UA-001 | Validasi hak akses peran |
| Tambah Pengguna Baru | Membuat akun pengguna baru dengan detail lengkap | TS-UA-002 | Validasi input, username unik, dan pembuatan akun |
| Validasi Username | Menolak username duplikat | TS-UA-003 | Validasi sistem terhadap username yang sudah ada |
| Edit Pengguna | Mengubah detail, peran, atau status akun | TS-UA-004 | Update data & hak akses otomatis |
| Nonaktifkan Akun | Menonaktifkan akun pengguna yang keluar | TS-UA-005 | Pengguna tidak dapat login lagi |
| Reset Password | Mengatur ulang kata sandi pengguna | TS-UA-006 | Kebijakan password diterapkan |
| Manajemen Peran | Membuat, mengedit, dan menghapus peran | TS-UA-007 | Validasi nama unik & daftar izin |
| Hak Akses Peran | Menetapkan izin akses berdasarkan peran | TS-UA-008 | Cek otorisasi & pembatasan izin |
| Audit Trail | Catat semua perubahan pengguna/peran | TS-UA-009 | Verifikasi pencatatan log |
| NFR – Keamanan & Kepatuhan | Akses, enkripsi, dan kepatuhan audit | TS-UA-010 | Pengujian keamanan & kepatuhan regulasi |

### 2) Daftar Test Scenario (Ringkas)

* **TS-UA-001** – Akses modul hanya untuk OO (High)
* **TS-UA-002** – Membuat pengguna baru dengan detail lengkap (High)
* **TS-UA-003** – Validasi username duplikat (High)
* **TS-UA-004** – Mengubah data & peran pengguna (High)
* **TS-UA-005** – Menonaktifkan akun pengguna (High)
* **TS-UA-006** – Reset kata sandi pengguna (Medium)
* **TS-UA-007** – Membuat dan mengedit peran baru (High)
* **TS-UA-008** – Menetapkan hak akses sesuai peran (High)
* **TS-UA-009** – Audit trail semua aktivitas pengguna (High)
* **TS-UA-010** – Pengujian keamanan, enkripsi, dan kepatuhan (Medium)

### 3) Detail Test Scenario

TS-UA-001 – Akses Modul oleh Operator Officer

**Tujuan:** Memastikan hanya Operator Officer (OO) yang dapat membuka dan mengelola modul manajemen pengguna.  
 **Pra-kondisi:** Ada akun OO dan akun non-OO (CS/Teller).  
 **Langkah:**

1. Login sebagai OO → buka *Modul Manajemen Pengguna & Hak Akses*.
2. Login sebagai CS → coba akses modul yang sama.  
    **Expected Result:**

* OO dapat mengakses modul.
* CS tidak bisa mengakses, muncul pesan *“Akses ditolak”*.

TS-UA-002 – Menambahkan Pengguna Baru

**Tujuan:** Memastikan sistem dapat membuat akun baru dengan detail yang lengkap dan valid.  
 **Langkah:**

1. OO klik “Tambah Pengguna Baru”.
2. Isi Nama, Username, Email, Kata Sandi, Peran (mis. Teller).
3. Klik “Simpan”.  
    **Expected:**

* Sistem membuat akun baru.
* Pesan sukses “Pengguna berhasil ditambahkan”.
* Audit trail mencatat aksi dengan ID pengguna & waktu.

TS-UA-003 – Validasi Username Duplikat

**Tujuan:** Memastikan username unik dan tidak boleh ganda.  
 **Data Uji:** Username “teller01” sudah digunakan.  
 **Langkah:**

1. Tambahkan pengguna baru dengan username “teller01”.
2. Klik “Simpan”.  
    **Expected:**

* Pesan error “Username sudah digunakan”.
* Data tidak tersimpan.

TS-UA-004 – Mengedit Data & Peran Pengguna

**Tujuan:** OO dapat mengubah detail atau peran pengguna, dan hak akses diperbarui otomatis.  
 **Langkah:**

1. Pilih pengguna → klik “Edit”.
2. Ubah peran dari “Teller” ke “Kepala Cabang”.
3. Klik “Simpan”.  
    **Expected:**

* Peran pengguna berubah.
* Hak akses mengikuti peran baru.
* Audit trail mencatat perubahan peran.

TS-UA-005 – Menonaktifkan Akun Pengguna

**Tujuan:** Memastikan pengguna nonaktif tidak dapat login.  
 **Langkah:**

1. OO pilih akun “CS01” → ubah status menjadi *Nonaktif*.
2. Logout dan login sebagai CS01.  
    **Expected:**

* Login ditolak dengan pesan *“Akun dinonaktifkan”*.
* Audit log mencatat penonaktifan akun.

TS-UA-006 – Reset Kata Sandi Pengguna

**Tujuan:** Menguji fitur reset password sesuai kebijakan keamanan.  
 **Langkah:**

1. Pilih pengguna → klik “Reset Password”.
2. Masukkan password baru dan konfirmasi.
3. Klik “Simpan”.  
    **Expected:**

* Password baru disimpan.
* Pengguna wajib login ulang dengan password baru.
* Password memenuhi kebijakan keamanan (min 8 karakter, kombinasi huruf, angka, simbol).

TS-UA-007 – Membuat dan Mengedit Peran Baru

**Tujuan:** OO dapat menambah atau mengedit peran sistem.  
 **Langkah:**

1. Klik tab “Manajemen Peran” → “Tambah Peran Baru”.
2. Isi nama peran (mis. “Reviewer”), pilih izin terkait.
3. Klik “Simpan Peran”.  
    **Expected:**

* Peran baru tersimpan.
* Nama peran unik.
* Audit trail mencatat pembuatan peran.

TS-UA-008 – Menetapkan Hak Akses Berdasarkan Peran

**Tujuan:** Memastikan hak akses sesuai dengan izin yang ditetapkan.  
 **Langkah:**

1. Login sebagai pengguna dengan peran baru (mis. Reviewer).
2. Akses fitur yang seharusnya diizinkan (mis. lihat laporan).
3. Akses fitur yang tidak diizinkan (mis. kelola transaksi).  
    **Expected:**

* Fitur diizinkan dapat diakses.
* Fitur lain diblokir dengan pesan *“Tidak memiliki izin”*.

TS-UA-009 – Audit Trail Aktivitas Manajemen Pengguna

**Tujuan:** Semua aktivitas manajemen pengguna dicatat dalam audit trail.  
 **Langkah:**

1. OO menambah, mengedit, dan menonaktifkan pengguna.
2. Buka modul audit trail (FR.009).  
    **Expected:**

* Audit log mencatat semua aktivitas (tambah/edit/nonaktif).
* Termasuk ID user, waktu, dan nilai sebelum/sesudah.

TS-UA-010 – Uji Keamanan & Kepatuhan

**Tujuan:** Pastikan data sensitif terenkripsi & sesuai regulasi keamanan.  
 **Langkah:**

1. Buka database & periksa penyimpanan password (hash/enkripsi).
2. Coba akses modul tanpa login.  
    **Expected:**

* Password tidak tampil dalam teks asli.
* Akses tanpa otorisasi ditolak (HTTP 403).
* Sistem mematuhi kebijakan keamanan & logging.

## **1**2**. Alur Kerja/Flowchart**

graph TD  
 A[Mulai] --> B(OO Ingin Mengelola Pengguna/Hak Akses);  
 B --> C[OO Akses Modul Manajemen Pengguna & Hak Akses];  
 C --> D{Pilih Tindakan?};  
 D -- Tambah Pengguna --> E[OO Input Detail Pengguna Baru & Peran];  
 E --> F{Detail Valid & Unik?};  
 F -- Tidak --> G[Sistem Tampilkan Pesan Kesalahan];  
 G --> E;  
 F -- Ya --> H[Sistem Buat Akun Pengguna Baru];  
 H --> I[Sistem Catat di Audit Trail];  
 I --> Z(Selesai);  
  
 D -- Edit Pengguna --> J[OO Pilih Pengguna untuk Diedit];  
 J --> K[OO Ubah Detail/Peran/Status Akun];  
 K --> L{Perubahan Valid & Diizinkan?};  
 L -- Tidak --> M[Sistem Tampilkan Pesan Kesalahan];  
 M --> K;  
 L -- Ya --> N[Sistem Update Akun Pengguna];  
 N --> O[Sistem Catat di Audit Trail];  
 O --> Z;  
  
 D -- Kelola Peran --> P[OO Akses Manajemen Peran];  
 P --> Q{Pilih Tindakan Peran?};  
 Q -- Tambah Peran --> R[OO Input Nama Peran & Pilih Izin];  
 R --> S{Nama Peran Unik & Izin Valid?};  
 S -- Tidak --> T[Sistem Tampilkan Pesan Kesalahan];  
 T --> R;  
 S -- Ya --> U[Sistem Buat Peran Baru];  
 U --> V[Sistem Catat di Audit Trail];  
 V --> Z;  
  
 Q -- Edit Peran --> W[OO Pilih Peran untuk Diedit];  
 W --> X[OO Ubah Izin Peran];  
 X --> Y{Perubahan Izin Valid?};  
 Y -- Tidak --> AA[Sistem Tampilkan Pesan Kesalahan];  
 AA --> X;  
 Y -- Ya --> BB[Sistem Update Izin Peran];  
 BB --> CC[Sistem Catat di Audit Trail];  
 CC --> Z;

