Autorisasi Pengguna

Panduan Modul: Autorisasi Pengguna

Lokasi Modul
Pengaturan > Autorisasi Fungsi > Autorisasi Pengguna

Tujuan Modul
Modul **Autorisasi Pengguna** adalah pusat kendali keamanan sistem, di mana Administrator mendefinisikan "peran" atau "jabatan fungsional" dalam bentuk **Kelompok Otorisasi**. Setiap kelompok ini merepresentasikan sekumpulan hak akses ke berbagai menu, tombol, dan fungsi di seluruh sistem. Ini adalah inti dari mekanisme *Role-Based Access Control* (RBAC), yang menentukan "siapa boleh melakukan apa".

1. Tampilan Utama (Daftar Kelompok Otorisasi)

Halaman utama menampilkan daftar semua peran atau kelompok otorisasi yang telah dibuat.

Penjelasan Tampilan

- **Filter**: Memungkinkan pencarian kelompok berdasarkan **ID Kelompok**.
- **Tambah Kelompok**: Link untuk membuat kelompok otorisasi baru.

- **Tabel Kelompok**:
  - **ID Kelompok**: ID unik untuk setiap kelompok.
  - **Nama Kelompok**: Nama peran fungsional (contoh: `1_MANAGING_DIRECTOR`, `2_MANAGER_ACCOUNTING`).
  - **Deskripsi**: Penjelasan singkat mengenai peran kelompok tersebut.
  - **Status**: Menunjukkan apakah kelompok tersebut aktif (`Aktif`) atau tidak.
- **Aksi**: Mengklik salah satu baris akan membawa pengguna ke halaman **Ubah** untuk mengelola kelompok tersebut.

2. Halaman Ubah (Detail Kelompok Otorisasi)

Halaman ini adalah form untuk mengedit detail sebuah kelompok dan menjadi gerbang untuk mengatur hak akses spesifiknya.

Penjelasan Tampilan

- **Informasi Dasar**:
  - **Nama Kelompok & Deskripsi**: Field untuk mengubah nama dan deskripsi peran.
  - **Status**: Kotak centang "Aktif" untuk mengaktifkan/menonaktifkan kelompok.
- **Tombol Aksi Lanjutan**:

- **Ubah**: Menyimpan perubahan pada nama, deskripsi, atau status.

- **Kelompok Admin**: Kemungkinan digunakan untuk menunjuk pengguna mana yang dapat mengelola keanggotaan kelompok ini.

- **Autorisasi Pengguna**: Ini adalah tombol paling penting. Mengkliknya kemungkinan besar akan membuka halaman matriks keamanan, di mana administrator dapat mencentang setiap menu, sub-menu, dan fungsi (misalnya, Buat, Ubah, Hapus) yang boleh diakses oleh kelompok ini.

- **Hapus**: Untuk menghapus kelompok otorisasi.

3. Langkah-langkah Mengatur Hak Akses

1. **Buat Kelompok Baru**: Dari halaman utama, klik **Tambah Kelompok**, beri nama dan deskripsi (misalnya, "Staf Pembelian"), lalu simpan.

2. **Atur Hak Akses**: Klik pada kelompok yang baru dibuat, lalu klik tombol **Autorisasi Pengguna**.

3. **Tetapkan Izin**: Di halaman matriks keamanan yang muncul (tidak ditampilkan), centang semua menu dan fungsi yang boleh diakses oleh "Staf Pembelian" (misalnya, bisa 'melihat' dan 'membuat' *Purchase Requisition*, tapi tidak bisa 'menghapus' *Purchase Order*). Simpan matriks izin tersebut.

4. **Tetapkan Pengguna ke Kelompok**: Terakhir, buka modul **Data Pegawai**, cari pegawai yang relevan, dan di bagian "Otorisasi Fungsi", masukkan pegawai tersebut ke dalam kelompok "Staf Pembelian".

4. Alur Kerja & Proses Bisnis Terintegrasi

- **Penerapan RBAC**: Alur di atas adalah implementasi penuh dari *Role-Based Access Control*. Hak akses tidak diberikan ke individu, melainkan ke peran (kelompok). Individu kemudian dimasukkan ke dalam peran tersebut.

- **Keamanan Dinamis**: Saat seorang pegawai ("Staf Pembelian") login, sistem akan memeriksa kelompoknya. Sistem kemudian hanya akan menampilkan menu dan mengaktifkan tombol yang telah diizinkan untuk kelompok tersebut di modul ini. Semua fungsi lain akan disembunyikan atau dinonaktifkan.

- **Pusat Keamanan**: Modul ini, bersama dengan **Data Pegawai**, adalah pusat dari seluruh kerangka keamanan sistem. Pengaturan di sini menentukan batas wewenang setiap pengguna di seluruh aplikasi.

5. Tips & Catatan Penting

- Struktur kelompok harus dirancang dengan hati-hati untuk mencerminkan peran fungsional nyata di perusahaan. Hindari membuat terlalu banyak kelompok yang tumpang tindih.

- Terapkan prinsip *Least Privilege*: Selalu berikan hak akses seminimal mungkin yang dibutuhkan oleh sebuah peran

untuk menjalankan tugasnya.

- Tombol "Autorisasi Pengguna" adalah area yang paling sensitif. Kesalahan konfigurasi di sini dapat memberikan hak akses yang berlebihan atau justru menghalangi pengguna untuk bekerja.

- Pengelolaan modul ini adalah tugas eksklusif dari Administrator Sistem atau peran setingkat yang bertanggung jawab penuh atas keamanan aplikasi.

Revision #2
Created 19 October 2025 10:13:05 by Sayu
Updated 23 October 2025 08:18:43 by Sayu