SIGNFLOW - QUY TRÌNH QUẢN LÝ NGƯỜI DÙNG & SSO

Module: User Management & Authentication **Integrations:** Google Workspace (OAuth 2.0) **Role:** Product Owner **Version:** 1.0 **Status:** Draft

1. TỔNG QUAN (OVERVIEW)

Module này giải quyết bài toán xác thực (Authentication) và phân quyền (Authorization) mà không cần xây dựng hệ thống quản lý mật khẩu nội bộ.

- **Cơ chế:** Sử dụng Google SSO (Single Sign-On).
- **Mục tiêu:** Tự động hóa việc đăng ký (Auto-Registration), phát hiện Admin qua cấu hình (Auto-Admin Promotion) và thu thập thông tin người dùng mới (Onboarding Flow).
- **Default Role:** Người dùng mới mặc định là **SENDER**.

2. DATA MODEL: USER PROFILE

Cấu trúc dữ liệu người dùng trong Database (NoSQL/SQL):

```
{
  "userId": "UUID (System generated)",
  "googleUid": "String (From Google)",
  "email": "user@company.com",
  "avatarUrl": "URL",
  "role": "SENDER | CHECKER | MANAGER | ADMIN",
  "status": "ACTIVE | INACTIVE | BANNED",
  "isProfileComplete": false, // Cờ đánh dấu đã điền thông tin bổ sung chưa
  "profile": {
    "fullName": "Nguyen Van A",
    "departmentId": "DEPT_01",
    "jobTitle": "Chuyên viên",
    "contactEmail": "user.work@company.com" // Email nhận thông báo (có thể khác email
  },
  "metadata": {
    "createdAt": "Timestamp",
    "lastLoginAt": "Timestamp",
    "createdBy": "SYSTEM_SSO"
  }
}
```

3. QUY TRÌNH ĐĂNG NHẬP & ONBOARDING (LOGIN FLOW)

3.1. Sơ đồ luồng (Workflow Diagram)

```
flowchart TD
    A[User truy cập SignFlow] --> B{Đã đăng nhập?}
    B -- Yes --> C[Dashboard]
    B -- No --> D[Click 'Login with Google']

    D --> E[Google OAuth Consent Screen]
```

```
E --> F{Google Auth Success?}

F -- No --> G[Hiển thị lỗi đăng nhập]
F -- Yes --> H[Hệ thống nhận Token & User Info]

H --> I{Email tồn tại trong DB?}

I -- Yes (Cũ) --> J[Cập nhật LastLogin]
J --> K{Profile Complete?}

I -- No (Mới) --> L[Tạo User mới (Auto-Register)]
L --> M{Email in Admin Whitelist?}

M -- Yes --> N[Set Role = ADMIN]
M -- No --> O[Set Role = SENDER]

N --> P[Lưu DB]
O --> P
P --> Q[Redirect: Onboarding Page]

Q --> R[User điền thông tin: Phòng ban, Tên...]
R --> S[Submit Form]
S --> T[Update DB: isProfileComplete = true]
T --> C[Dashboard]

K -- Yes --> C
K -- No --> Q
```

3.2. Chi tiết các bước xử lý logic

Bước 1: Google Authentication

- Client gọi Google OAuth API.
- Google trả về `id_token` và thông tin cơ bản (`email` , `name` , `picture` , `sub` - googleUid).

Bước 2: System User Verification (Server-side)

- Backend verify `id_token` để đảm bảo tính hợp lệ.
- Query DB tìm User theo `email` .

Bước 3: Xử lý phân nhánh (Existing vs New User)

A. Nếu User ĐÃ tồn tại:

- Kiểm tra trạng thái `status` . Nếu `INACTIVE` -> Chặn đăng nhập.
- Nếu `ACTIVE` -> Cập nhật `lastLoginAt` .
- Kiểm tra cờ `isProfileComplete` :
  - Nếu `true` -> Cấp Session Token (JWT) -> Vào Dashboard.
  - Nếu `false` -> Redirect sang trang **Onboarding**.

B. Nếu User CHƯA tồn tại (Lần đầu đăng nhập):

- Hệ thống thực hiện **Auto-Registration**:
- **Logic Auto-Admin:**

- Hệ thống load danh sách `ADMIN_WHITELIST` từ biến môi trường (ENV) hoặc Config File (VD: `admin@signflow.com, it_manager@company.com`).
- Nếu `email` khớp danh sách -> Gán Role = **ADMIN**.
- Nếu không khớp -> Gán Role = **SENDER** (Mặc định).

- Lưu User vào DB với `isProfileComplete = false`.
- Redirect sang trang **Onboarding**.

4. QUY TRÌNH ONBOARDING (CẬP NHẬT THÔNG TIN)

Đây là form bắt buộc sau khi đăng ký thành công lần đầu.

Các trường thông tin cần thu thập:

1. **Họ và Tên (Full Name):** Prefill từ Google, cho phép sửa.
2. **Mã Nhân Viên (Employee ID):** (Optional/Required tùy policy).
3. **Phòng Ban (Department):** Dropdown list (Lấy từ danh mục phòng ban trong hệ thống).
   - *Mục đích:* Để sau này routing văn bản (VD: Chỉ Manager phòng IT mới ký được văn bản của Sender phòng IT).
4. **Chức vụ (Job Title):** Text input.
5. **Email nhận thông báo:** Prefill từ Google Email. User có thể đổi nếu muốn nhận noti qua email khác.

Hành động sau Submit:

- Validate dữ liệu.
- Update User Profile vào DB.
- Set `isProfileComplete = true`.
- Chuyển hướng về trang chủ tương ứng với Role.

5. CHỨC NĂNG QUẢN TRỊ VIÊN (ADMIN PORTAL)

Admin (được tạo từ whitelist hoặc do Admin khác cấp quyền) sẽ có menu "Quản lý người dùng".

5.1. Danh sách người dùng

Hiển thị bảng:

- Avatar / Tên / Email.
- Phòng ban / Chức vụ.
- Role hiện tại (Sender/Checker/Manager).
- Trạng thái (Active/Inactive).
- Ngày đăng nhập cuối.

5.2. Cấp quyền (Promote/Demote)

Admin bấm "Edit Role" cho một User:

- **SENDER -> CHECKER:** Người dùng được phép truy cập menu "Duyệt tài liệu".
- **CHECKER -> MANAGER:** Người dùng được phép cấu hình Chữ ký số & Ký pháp lý.
    - *Lưu ý:* Khi cấp quyền Manager, hệ thống có thể yêu cầu Manager upload Chứng thư số (Public Certificate) để lưu vào hồ sơ (nếu dùng ký USB Token).

5.3. Khóa tài khoản (Deactivate)

- Dùng khi nhân viên nghỉ việc.
- Admin chuyển Status sang `INACTIVE`.
- Token hiện tại của User (nếu đang login) sẽ bị vô hiệu hóa (Blacklist JWT) hoặc chờ hết hạn.

6. CÁC QUY TẮC BẢO MẬT (SECURITY RULES)

1. **Domain Restriction (Optional):**
    - Chỉ cho phép email có đuôi `@congty.com` đăng nhập. Các email `@gmail.com` cá nhân sẽ bị chặn ngay bước SSO Callback.
2. **Session Management:**
    - Sử dụng JWT (JSON Web Token) cho session của ứng dụng.
    - Token hết hạn sau 24h (hoặc tùy cấu hình).
3. **Role Guard:**
    - API Backend phải check Role ở mọi endpoint (VD: Endpoint `approveDocument` bắt buộc Role phải là `CHECKER` hoặc `MANAGER`).

End of User Management Specification