백오피스포탈 메뉴 정책서

작성자	@피닉스(조윤기)
검토자	@현즈(홍현종)
상태	완료
이 페이지에서 다루는 내용	문서 히스토리 개요 정책 1. 기본 정책 1.1 권한 처리 순서 2. 백오피스포탈 운영 정책 2.1 백오피스 클라이언트, Role 및 권한 그룹 관리 2.1.1 백오피스 클라이언트 관리 2.1.2 Role 관리 2.1.3 권한 그룹(Group) 관리 Role / Policy / Permission 관계도 2.2 Resource 및 Permission 관리 2.2.1 Resource 관리 2.2.2 Permission 관리 2.3 메뉴 관리 2.3.1 메뉴 관리 2.3.2 메뉴 제공 2.3.4 권한 체크 2.4 개인정보/위치정보 관리 2.5 권한 변경 반영 및 캐시 정책 2.5.1 권한 변경 반영 2.5.2 캐시 정책 2.6 전체 요약

문서 히스토리

No	작성자	날짜	내용	비고
1	@피닉스(조윤기)	2025년 11월 11일	백오피스포탈 메뉴 정책 초안 작성	
2				

개요

본 정책서는 [백오피스 메뉴 기능 설계]의 **하위 상세 정책 문서**입니다.

- **상위 문서 참조**: 시스템 개요, 요구사항, 구성도, 데이터 구조
- **본 문서 내용**: 운영 정책 및 사용 정책 상세

구분	설명
목적	백오피스포탈 메뉴/권한/리소스/Role/Permission 관리의 운영·사용 기준 제공
대상	사용자(어드민), 운영자, 개발자(Keycloak·백오피스포탈)
핵심 구성요소	Client, Role, Group, User, Resource, Scope, Permission, Menu
권한 모델 기준	Keycloak 기반 (Role → Policy → Permission → Resource(Scope) 연계), Menu는 포탈 내부 DB 관리

정책

1. 기본 정책

1.1 권한 처리 순서

순서	내용	실행 주체	실행 방법	비고
1	Client-Id (백오피스 클라이언트) 생성	백오피스 포탈	백오피스 포탈 → 백오피스 클라이언트 관리 화면에서 생성	Keycloak Admin API 호출로 Client 등록 및 menu_group 테이블에 기본 메뉴 그룹 정보 생성
2	Client-Role 생성	백오피스 포탈	백오피스 포탈 → 백오피스 클라이언트 별 Role 관리 화면에서 생성	Keycloak Admin API를 통해 Role 생성 및 Policy 자동 생성
3	권한 그룹 생성	백오피스 포탈	백오피스 포탈 → 백오피스 클라이언트 별 권한그룹 관리 화면에서 생성	Keycloak Admin API로 Group 등록
4	USER ↔ 권한 그룹 매핑	전자결재 → 백오피스 포탈	전자결재 승인 완료 → 자동 반영	승인 시 Keycloak Admin API 호출로 Group 매핑 반영

5	API Resource 등록/수정 (Scope 포함)	백오피스 포탈	백오피스 포탈 → 백오피스 클라이언트 별 Resource 관리 화면에서 등록/수정	Keycloak Admin API를 통해 Resource 및 Scope 등록/수정
6	Permission 자동 생성	백오피스 포탈	Role과 Resource 매핑 시 자동 생성 → 리소스 생성시	Role과 Resource 매핑 시 Keycloak Admin API를 통해 Permission 자동 생성
7	메뉴 생성	백오피스 포탈	백오피스 포탈 → 백오피스 클라이언트 별 메뉴 관리 화면에서 생성	내부 DB에서 메뉴 관리
8	메뉴-Resource 매핑	백오피스 포탈	백오피스 포탈 → 백오피스 클라이언트 별 메뉴 관리 화면에서 메뉴 선택 → 리소스 매핑	메뉴는 ResourceId와 매핑해서 관리

---

2. 백오피스포탈 운영 정책

2.1 백오피스 클라이언트, Role 및 권한 그룹 관리

2.1.1 백오피스 클라이언트 관리

항목	내용
생성 위치	백오피스 포탈 UI
네이밍 규칙(ClientId)	영문 소문자, ‘-’, ‘_’ (단어 사전 기반 권장)
변경 제약	Update 미제공 → 변경 시 신규 생성(Create) 방식
Keycloak 연동	Create: “Keycloak 등록” 클릭 시 ClientID 생성
활성화 조건	Keycloak 등록 후 Role/Group/Resource 관리 가능
Client-ID 획득	Read: 백오피스 포탈 내 화면에서만 확인 가능 (API 미제공)

2.1.2 Role 관리

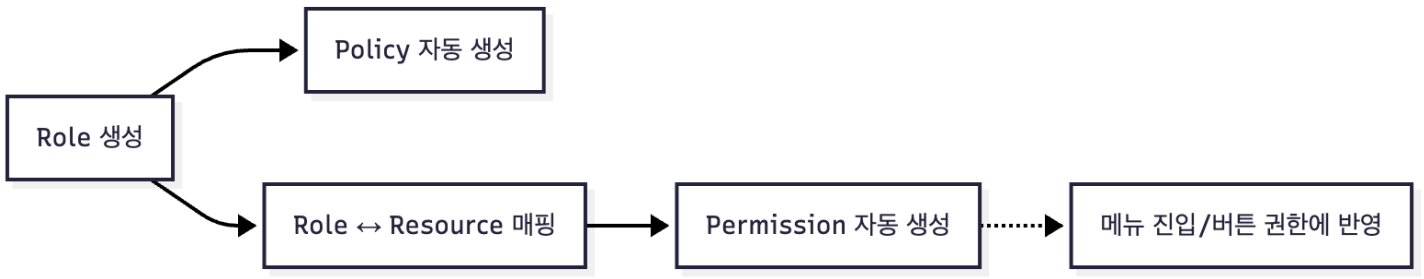
항목	내용
생성 위치	클라이언트 상세 화면

생성	신규 Role 생성 시 Policy 자동 생성(키클락 등록 필수)
수정	이름 수정 가능
삭제	삭제 시 관련 Policy 자동 삭제
네이밍 규칙	영문 소문자, '-', '_', 숫자
제약	Role 명 중복 불가, 예약어 금지 (예: `default-roles-*`, `offline_access`)

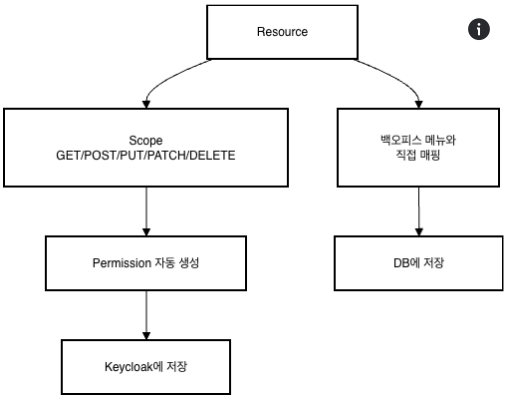
2.1.3 권한 그룹(Group) 관리

항목	내용
생성 위치	클라이언트 개요 화면
생성	그룹 네임은 중복될 수 없음
수정	그룹명 및 구성 변경 가능
삭제	삭제 가능
USER 매핑	전자결재 승인 시 자동 매핑
USER 매핑 실패 처리	운영자 수동 처리 가능 (담당자: 피닉스)

Role / Policy / Permission 관계도



2.2 Resource 및 Permission 관리



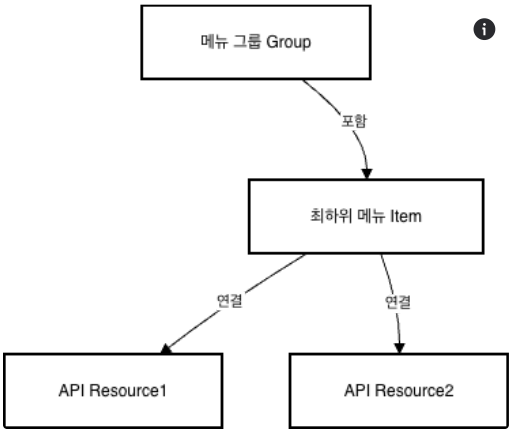
2.2.1 Resource 관리

항목	내용
생성 / 수정	포탈 UI에서 등록 및 수정 가능
조회	API 리소스 리스트 및 상세 조회 가능
삭제	Resource 삭제 시 관련 Permission 자동 삭제
Scope 구성	CRUD 기반 HTTP Method 기준 → GET, POST, PUT, DELETE
역할	API 접근 제어 핵심 요소
개인정보/위치정보	Keycloak Resource Attribute에 저장

2.2.2 Permission 관리

항목	내용
생성	Create: Role ↔ Resource 매핑 시 자동 생성
삭제	Delete: Resource 또는 Role 연결 해제 시 Permission 자동 삭제
Scope 구성	해당 Resource의 모든 Scope 포함
메뉴와 영향	메뉴는 Permission이 아닌 **Resource 기반으로 연결**

2.3 메뉴 관리

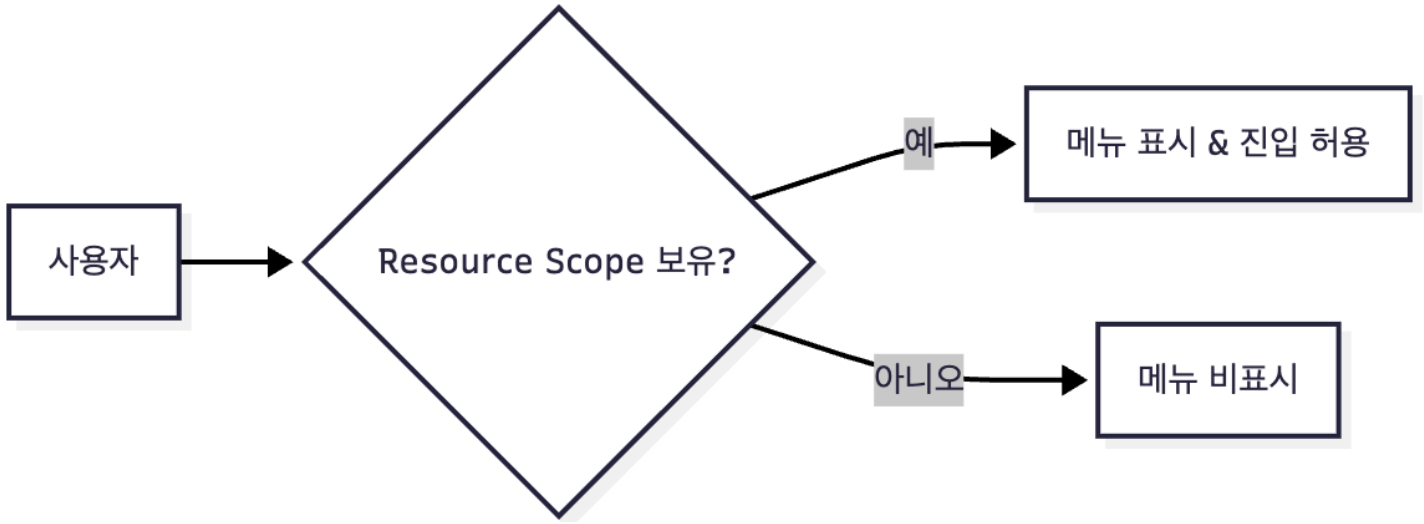


2.3.1 메뉴 관리

항목	내용
생성	메뉴는 백오피스 포탈 메뉴 관리 화면에서 생성 가능 *최대 2 Depth 구조까지만 생성 가능*. 최하위 메뉴(Item) 기준으로 실제 화면과 연결됨
조회	Client-ID 기준 • 트리 구조 제공 • 트리 구조에서 GROUP/ITEM 선택시 상세 제공
수정	Client-ID 기준 • 트리 구조 제공 • 트리 구조에서 GROUP/ITEM 선택시 상세 제공
삭제	GROUP 삭제시 하위 ITEM 및 GROUP 동시 삭제
메뉴 구조	최대 2 Depth 구조까지 생성 가능 (GROUP → ITEM)
메뉴 그룹(GROUP)	하위 메뉴를 묶는 폴더 역할, API 리소스 매핑 불필요
최하위 메뉴(ITEM)	실제 화면으로 연결되는 메뉴, **최소 1개 이상의 API 리소스 필수**
관리 권한	메뉴 관리자 권한이 있는 사용자만 생성, 수정, 삭제 가능
저장 위치	메뉴 정보는 백오피스 포탈 내부 DB에서 관리됨

메뉴 등록 절차	API 리소스 선 등록 필수 • 메뉴 구조에 따라 **메뉴 그룹** 또는 **최하위 메뉴** 메뉴 생성 • 1개 메뉴에 여러 API 리소스 등록 가능 • 메뉴 노출 순서 조정
메뉴-Resource 매핑	mismatching 시 메뉴 미노출
권한 보유 사용자	Role 보유자 기준 메뉴 표시/진입 확인
권한 미보유 사용자	메뉴 노출 안됨 확인

2.3.2 메뉴 제공



조건	설명
메뉴 표시	매핑된 Resource가 하나라도 존재
메뉴 진입	1개 이상의 Scope 권한 필요
다중 Resource 매핑	OR 조건 기반 처리

2.3.4 권한 체크

종류	내용	비고
메뉴 권한 체크	메뉴 - API 리소스 - Role 에 부여된 사용자 확인	백오피스 메뉴 기능 설계 | 메뉴 조회

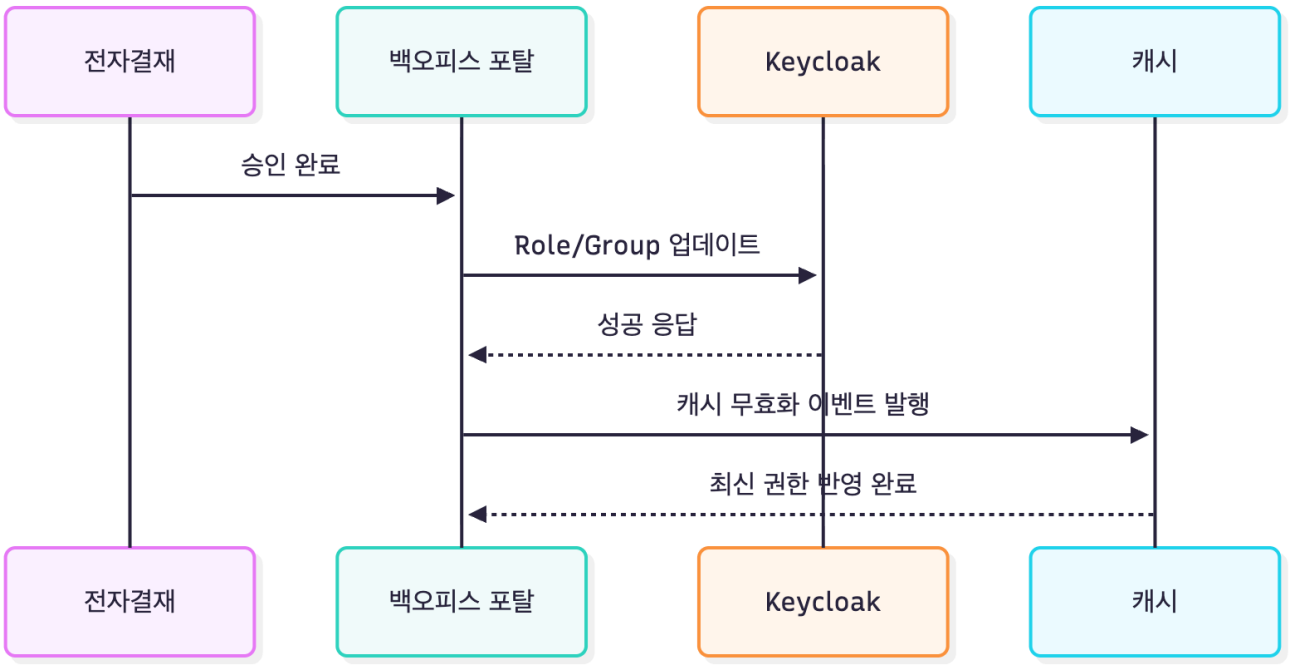
	• Request ◦ Header Authorization: Bearer JWT ◦ Param : path	
기능 권한 체크	API 리소스 - Role 에 부여된 사용자 확인 • Request ◦ Header Authorization: Bearer JWT	

2.4 개인정보/위치정보 관리

항목	내용
관리 위치	API Resource
체크 방식	“개인/위치 정보 포함 여부” 플래그 설정
개인정보 종류	위치정보는 true/false로 관리 이름, 생년월일, 주소, 전화번호, 면허정보 등 개인정보 내역 비밀번호 서류(운전경력확인서, 해지계약서, 임대차계약서) 면허번호 CI 주민등록번호 이력서 카드번호 유효기간(카드번호+유효기간) Bill key 계좌번호 블랙박스 이름 생년월일 성별(이름+생년월일+성별) 이메일주소

	주소 전화번호 서류(카쉐어링, 쏘카마이존 계약서류) 면허발급일(면허증번호+발급일) 단말 앱 접속위치 예약정보 차량위치 본인사진 녹취 회원번호 연령 영수증 사망여부 직장정보
비고	개인정보 포함 시 반드시 개인정보 내역 체크(필수) • 체크되지 않을시 메뉴에 개인정보 취급 내역이 포함되지 않은 것으로 간주

2.5 권한 변경 반영 및 캐시 정책



2.5.1 권한 변경 반영

항목	내용

변경 시점		전자결재 승인 또는 관리자 변경시 수행
관리위치	기존 서비스 어드민	DB
	신규 서비스 어드민	키클락
토큰	기존 서비스 어드민	백오피스 클라이언트에서 JWT 토큰정보의 Role 정보 사용 시 발급 필요
	신규 서비스 어드민	

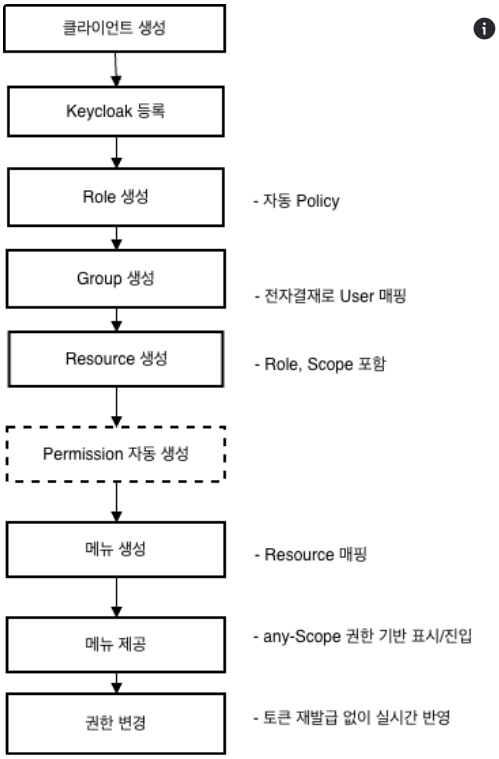
2.5.2 캐시 정책

동작	조건	처리 내용	반영 시점
캐시 데이터 생성	사용자 최초 권한 요청 시	Role, Group, Menu, Resource 정보를 캐시에 저장	즉시
캐시 데이터 조회	사용자 권한 확인 요청 시	캐시된 권한 정보를 조회하여 응답	즉시
캐시 데이터 갱신	Role, Group, Menu, Resource 변경 시	기존 캐시 삭제 후 다음 요청 시 재생성	변경 즉시
캐시 데이터 삭제	• Role 생성/수정/삭제 • Group 생성/수정/삭제 • Menu 생성/수정/삭제 • Resource 생성/수정/삭제 • Permission 변경	해당 Client-ID 관련 모든 캐시 즉시 무효화	변경 즉시

2.5.3 캐시 라이프사이클 특징

항목	내용
TTL (Time To Live)	8시간 (업무시간 기준)
무효화 정책	데이터 변경 시 즉시 무효화 (Invalidate on Write)
재생성 시점	TTL 만료 후 첫 요청 시 재생성
실시간성 보장	변경 즉시 반영, 이후 조회 시 최신 데이터 제공

2.6 전체 요약


클라이언트 생성
Keycloak 등록
Role 생성
- 자동 Policy
Group 생성
- 전자결재로 User 매핑
Resource 생성
- Role, Scope 포함
Permission 자동 생성
메뉴 생성
- Resource 매핑
메뉴 제공
- any-Scope 권한 기반 표시/진입
권한 변경
- 토큰 재발급 없이 실시간 반영