별첨 #1. 계정 관리 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 6 조(계정 및 접근통제) 중 계정 관리에 해당하는 실행 절차를 규정하여, 정보시스템 내 계정의 생성·변경·삭제 및 운영 방식에 대한 통일된 기준을 확립함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 계정 유형에 적용한다.

1. 밥세권 서비스 운영 서버·DB·네트워크·보안장비의 관리계정
2. 내부 운영 시스템의 사용자계정
3. 개발·운영·유지보수 과정에서 사용되는 업무계정 및 기술계정
4. 외부 개발/협력업체 인력에게 발급되는 계정

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 계정 정책 총괄 승인
   - 계정 권한 계정 승인
2. 보안관리자
   - 계정 발급 절차 운영 및 점검
   - 계정 현황 정기 검토
3. 정보보안 담당자
   - 계정 권한 검토 및 최소권한 점검
   - 비정상 계정 사용 행위 탐지
4. 시스템관리자
   - 계정 생성·변경·비활성화 수행
5. 사용자(임직원 및 협력업체)
   - 계정 공유 금지
   - 비밀번호 정책 준수
   - 불필요한 권한 반납

제 2 장 용어 정의

1. 사용자 계정: 시스템 접속을 위해 개인에게 부여되는 고유 계정으로 업무 수행을 위한 일반 권한을 가짐
2. 관리자 계정: 설정 변경·시스템 운영을 수행할 수 있는 고급 권한 계정
3. 시스템 계정(서비스 계정): 배치·연동·자동화 기능 수행 목적의 계정
4. 임시 계정: 외부 개발자 또는 장애 대응 시 한시적으로 사용되는 계정
5. 권한: 계정이 시스템 내에서 수행할 수 있는 행위 또는 접근범위(RBAC 기반)

제 3 장 계정 생성

제 4 조(계정 생성 절차)

계정 생성은 다음 절차로 수행한다.

1. 사용자 또는 부서장 신청서 제출
    - 신청 사유
    - 접근 대상 시스템
    - 필요 권한
    - 사용 기간(임시계정 필수)
2. 부서장 승인
3. 정보보안담당자 검토
    - 최소권한 원칙 충족 여부
    - Role 기반(Role-Based Access Control, RBAC) 권한 적용 여부
    - 권한 매트릭스 기준 부합 여부(부서/직무별 권한 범위)
    - 중복 계정 존재 여부
    - 외부 인력 여부 확인
4. 정보보호책임자(CISO) 승인
5. 시스템관리자 계정 생성
6. 계정 발급 알림 및 초기 접속 안내
7. 계정 발급 기록 보관(1 년 이상)

제 5 조(임시계정 생성)

1. 외부 개발사·점검 인력 계정에는 반드시 기간 제한을 포함한다.
2. 임시계정의 기본 사용 기간은 30 일이며, 연장 시 재승인 필요
3. 임시계정 생성·활성·비활성화·삭제 이력은 별도 관리한다.

제 4 장 계정 변경·이동

제 6 조(직무 변경 시 권한 조정)

1. 부서 변경 또는 업무 변경 발생 시
    - 기존 권한 회수
    - 신규 직무에 따른 권한 재부여
2. 사용자는 불필요해진 권한을 즉시 반납 요청해야 한다.
3. 권한 조정 이력은 1 년 이상 보관한다.

제 7 조(개인정보·결제 관련 계정 관리)

(정책 제 11 조 반영)

1. 결제 시스템 접근 계정은 별도 식별 및 관리한다.
2. 결제 운영·로그 조회·설정 변경 계정은 개인별 발급 원칙
3. API Key/Secret 관리 계정은 최소 인원만 보유
4. 결제계정 권한 변경은 반드시 정보보호책임자(CISO) 승인을 득해야 한다.

제 5 장 비활성화·삭제

제 8 조(비활성화)

1. 90 일 이상 미사용 계정은 자동 잠금한다.
2. 임시계정은 목적 종료 즉시 비활성화 또는 삭제한다.
3. 보안 이상행위 발생 시 즉시 잠금 처리할 수 있다.

제 9 조(퇴사·계약 종료 계정)

1. 퇴사자 계정은 퇴사 당일 1 시간 이내 비활성화한다.
2. 협력업체 계약 종료 시 계정도 동일 기준 적용
3. 비활성·삭제 내역은 1 년 이상 보관한다.

제 6 장 계정 점검 및 감사

제 10 조(정기 점검)

1. 시스템관리자: 월 1 회
    - 미사용 계정
    - 임시 계정
    - 과도 권한 계정
2. 정보보안담당자: 분기 1 회 전체 계정 목록 점검
3. 점검 결과는 정보보호책임자(CISO)에 보고한다.

제 11 조(로그 관리)

아래 항목은 중앙 로그 서버로 전송하며 1 년 이상 보관한다.

1. 계정 생성·변경·삭제 로그
2. 관리자 계정 로그인 로그
3. 비정상적 로그인 시도(Brute Force 등)

제 7 장 계정 보안 요구사항

제 12 조(금지 사항)

1. 계정 공유 금지
2. 동일인 다계정 사용 금지(업무계정·서비스계정 제외)
3. 테스트용 계정 운영환경 사용 금지
4. 기본값(default) 계정 사용 금지

제 13 조(비밀번호 관리)

비밀번호 정책은 접근통제 지침과 동일하게 적용되며 다음을 포함한다.

1. 최소 10 자 이상
2. 영문·숫자·특수문자 조합
3. 90 일 마다 변경
4. 최근 3 개 이상 비밀번호 재사용 금지

제 8 장 부칙

제 14 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 15 조(개정)

본 지침은 정보보호책임자(CISO)의 검토 후 개정한다.