별첨 #2. 접근통제 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 6 조(계정 및 접근통제), 제 7 조(네트워크 보호), 제 11 조(결제 보안)에 따라 시스템·네트워크·애플리케이션에 대한 접근을 안전하게 통제하기 위한 절차 및 기준을 규정함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 영역 전체에 적용한다.

1. 서버·DB·네트워크 장비·보안장비(WAF/UTM)
2. 운영자 페이지, 관리 콘솔, 내부 업무 시스템
3. 결제 시스템 및 PG 사 연동 구간
4. VPN, 원격 접속, 외부 개발사 접근

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 접근통제 정책 승인
   - 예외 승인 및 위험평가
2. 정보보안담당자
   - 접근 정책 검토
   - 모니터링 및 이상행위 분석
3. 시스템/네트워크 관리자
   - 접근통제 설정 반영
   - 방화벽/ACL 정책 운영
   - 접근 로그 관리
4. 사용자(임직원 및 협력업체 포함)
   - 승인된 방식으로만 시스템 접근
   - 권한 오·남용 금지

제 2 장 접근통제 원칙

제 4 조(최소권한 원칙)

1. 모든 접근은 업무 수행에 필요한 최소한 권한만 부여한다.
2. 특히 다음 영역은 최소권한 + 별도 승인 원칙을 적용한다.

- 루트/관리자 접근
- DB 직접 접속
- 결제·로그·고객정보 관련 접속
- 보안장비 설정 변경

제 5 조(허용 기반 정책)

1. 기본 정책은 Default Deny(기본 차단) 으로 운영한다.
2. 모든 허용은 다음 절차를 따른다.
    - 사유 및 위험 분석 포함
    - 승인 요청 후 적용
3. 외부 연동은 반드시 IP·포트·프로토콜 기반 화이트리스트 방식으로만 허용한다.

제 3 장 시스템 접근통제

제 6 조(서버 접근 통제)

1. 서버 접근은 반드시 VPN 이후 허용한다.
2. SSH 접근 요구사항:
    - 패스워드 로그인 금지
    - 공개키 기반 인증 또는 MFA 가능
    - Root 직접 로그인 금지(sudo 방식 사용)
3. 운영환경 서버는 운영자 PC(또는 Jump Server) 에서만 접근 가능하도록 제약할 수 있다.

제 7 조(DB 접근 통제)

1. DB 는 로컬 또는 지정된 중간 레이어(WAS)에서만 접근을 허용한다.
2. 운영환경 DB 에 대한 직접 SQL Client 로 접속하는 행위는 원칙적으로 금지한다.
3. DBA 계정은 최소 인원으로 제한하며, 모든 작업은 로그로 남긴다.
4. 결제·고객정보 DB 접근 시
    - 접속 로그 필수
    - 비식별화 후 조회 원칙
    - 대량 조회 또는 다운로드 제한 가능

제 8 조(관리자 페이지 접근 통제)

1. 관리자 페이지는 접근 요구사항:
    - 내부망 또는 VPN 에서만 접근
    - 접근 IP 화이트리스트 운영
    - MFA 적용 가능
    - 세션 타임아웃: 10 분
2. 관리자 페이지 URL 경로는 외부 노출을 금지한다.

제 4 장 네트워크 접근통제

제 9 조(망/존 간 접근통제)

1. 네트워크는 DMZ → 서버존 → 내부망 순으로 단계적 분리한다.
2. 존 간 통신 허용 시 반드시 정보보호책임자(CISO) 승인 후 가능하다.
3. 불필요한 포트·프로토콜은 즉시 차단한다.
4. Outbound 트래픽도 최소권한 정책을 적용한다.

제 10 조(방화벽 및 ACL 운영)

1. Allow by Exception 원칙 적용
2. 신규 룰 적용 절차
    - 요청서 제출
    - 사유·업무 필요성·위험분석 포함
    - 정보보호책임자(CISO) 승인
    - 설정 적용 및 기록 보관
3. 임시 허용 룰은 만료일 설정 필수
4. 방화벽 룰은 분기 1 회 전체 검토한다.

제 11 조(보안장비 접근통제-WAF/UTM)

1. WAF 운영 기준
    - 웹·API·결제·관리자 페이지 보호
    - SQL Injection, XSS, File Upload 우회, RCE 차단 룰 적용
    - 서비스 변경 시 정책 재검토
2. UTM 운영 기준
    - DMZ·내부망·서버존 트래픽 전 구간 트래픽 감시
    - IPS 활성화(Injection, Brute Force, Port Scan 탐지 가능)
    - Port Scan·Brute Force 탐지 가능
3. 정책 변경 승인 기준
    - 보안장비 정책 변경 시
        1. 사유
        2. 영향 범위
        3. 위험 분석
    - 포함해 정보보호책임자(CISO) 승인 후 반영

제 5 장 결제 시스템 접근통제

제 12 조(결제 데이터 접근 제한)

1. 카드번호·CVC·유효기간 등 민감결제정보 저장 및 열람 금지
2. 결제 API Key·Secret Key 접근은 최소 인원만 보유
3. Secret Key 는 HSM, Key Vault 등 보안 저장소에서만 조회 가능

제 13 조(PG 연동 접근 통제)

1. PG Callback/Webhook 호출은 반드시 서명값(Signature) 또는 Token 검증을 거쳐 처리한다.
2. PG 연동 서버 IP 는 화이트리스트 기반으로 제한한다.
3. 비인가 IP 의 요청은 즉시 차단한다.
4. 결제 오류 발생 시 거래 로그, API 요청·응답 로그 기반으로 원인 분석을 수행한다.

제 6 장 사용자 세션 및 인증

제 14 조(세션 보안)

1. 관리자 페이지 세션 타임아웃: 10 분
2. Session Fixation 방지 설정 적용
3. Session ID 는 Secure·HttpOnly 적용

제 15 조(인증 강화)

1. MFA 적용 가능 영역:
    - 관리자 페이지
    - 서버/DB 접근
    - 결게 관련 내부 콘솔
2. 로그인 실패 5 회 이상 시 계정 잠금
3. 비밀번호 정책은 계정 관리 지침과 동일하게 적용한다.

제 7 장 접근 모니터링 및 점검

제 16 조(접근 로그 수집)

다음 로그는 중앙 로그 서버로 전송한다.

- SSH/RDP 접속

- 관리자 페이지 로그인 로그
- DB 접근 로그
- 방화벽·WAF·UTM 탐지 로그
- 결제 요청/응답 로그

보관 기간은 1 년 이상이며, 결제 관련 로그는 5 년 이상 보관한다.

제 17 조(이상행위 탐지)

아래와 같은 행위 발생 시 즉시 정보보호책임자(CISO)에 보고:

1. 동일 계정에서 반복적인 로그인 실패
2. 해외·비인가 IP 접근
3. 비정상 관리자 페이지 접근
4. 대량 결제 요청 시도
5. WAF·IPS 의 고위험 공격 탐지

제 18 조(정기 점검)

1. 접근권한 점검: 월 1 회
2. 네트워크 ACL/방화벽 룰 점검: 분기 1 회
3. 관리자 페이지 접근기록 점검: 월 1 회
4. 점검 결과는 문서화하여 1 년 이상 보관한다.

제 8 장 예외관리

제 19 조(예외 승인)

1. 접근통제 정책 완화 필요 시 다음 항목을 포함하여 CISO 승인 후 진행한다.
    - 사유
    - 기간
    - 위험 분석
    - 대체 통제
2. 예외는 만료 즉시 원복한다.

제 9 장 부칙

제 20 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 21 조(개정)

본 지침은 정보보보호책임자(CISO)의 검토 후 개정한다.