별첨 #4. 암호화 및 키 관리 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 9 조(암호화 및 키 관리) 및 제 11 조(결제 보안)에 따른 데이터 암호화, 키 생성·저장·폐기, TLS 설정, 결제 Key 관리 절차를 규정함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 암호화 대상 및 구성요소 전체에 적용한다.

1. 저장 데이터(Data-at-Rest)
2. 전송 데이터(Data-in-Transit)
3. 결제 시스템 API Key/Secret Key
4. 서버 환경파일(.env) 및 설정파일
5. HSM/Key Vault/Secrets Manager 에 저장된 키

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 암호화 정책 승인
   - Key 예외 승인
2. 정보보안담당자
   - 암호화 구성 점검 및 위험 분석
3. 시스템/네트워크 관리자
   - TLS/서버 암호화 적용 및 키 저장소 운영
4. 보안팀
   - 암호화 적용 코드·API Key 관리·환경파일 보안 준수

제 2 장 데이터 암호화 기준

제 4 조(저장 데이터 암호화)

1. 저장 데이터는 다음 기준을 따른다.
   - 민감정보(개인정보·결제정보·로그인 정보): AES-256
   - 토큰·서명·임시 정보: SHA-256 이상
2. 암호화 대상
   - 비밀번호(One-way Hash: bcrypt 또는 Argon2)
   - 사용자 개인정보

- 결제 관련 식별자(Transaction ID 제외)
- Access Token, Refresh Token
- 인증용 Secret

3. 다음 정보는 절대 저장 금지
    - 카드번호 전체
    - CVC, 유효기간
    - 카드 PIN
    - 결제 시 민감 매입정보

제 5 조(DB 컬럼 암호화)

1. DB 는 다음 컬럼에 대해 AES-256 기반 컬럼 암호화를 적용한다.
    - 사용자 정보(전화번호, 이메일 등)
    - 개인식별정보
    - 민감 로그 항목
2. 컬럼 암호화 적용 시
    - 암복호화 로직은 DBMS 기능 또는 전용 모듈로 구현
    - 복호화 권한은 최소 인원으로 제한
    - 복호화 이력 로그 필수

제 3 장 전송 구간 암호화

제 6 조(TLS 적용 기준)

1. 모든 전송 구간은 TLS 1.2 이상 적용
2. TLS 설정 최소 기준
    - TLS 1.0, 1.1 지원 금지
    - 강한 Cipher Suite 만 허용
    - HSTS 적용 (웹서비스)
    - 인증서 자동갱신(Let's Encrypt 또는 정책적 대안)

제 7 조(내부 통신 암호화)

1. 내부 서버 간 통신도 TLS 또는 안전한 터널(VPN, IPSec) 사용
2. DB 연결 시 TLS 또는 SSL 적용
3. Cache/Redis 등도 필요 시 TLS 적용

제4장 키 관리 기준

제 8 조(키 생성)

1. 키 생성 시 다음 기준 준수
    - 대칭키: 256bit 이상
    - 비대칭키: RSA 2048bit 또는 ECC 기반
2. 키 생성은 자동화된 키 관리 도구 또는 HSM 기반으로 수행한다.
3. 개발 환경에서 개인 로컬 PC 에서 키 생성 금지

제 9 조(키 저장 및 보호)

다음 위치에만 키 저장을 허용한다.

1. HSM(하드웨어 보안 모듈)
2. Key Vault (AWS KMS / Azure KeyVault / GCP Secret Manager)
3. CI/CD Secret Store
4. OS 환경파일(.env) — 단, 다음 조건 충족 시만
    - 권한 600
    - 서버 외부 접근 불가 영역
    - Git 등 VCS 저장 금지

금지되는 저장 위치

- GitHub, GitLab 등 VCS
- Slack, Notion 등 협업툴
- 코드 내 하드코딩
- 웹 루트 디렉토리

제 10 조(API Key 및 Secret Key 관리)

1. Key 는 시스템관리자 또는 지정된 개발자만 조회 가능
2. Key 노출 시 즉시 폐기하고 신규 Key 재발급
3. Key 는 다음 이벤트 발생 시 반드시 교체
    - 인력 변경(퇴사·팀 변경)
    - 시스템 침해 의심
    - 반기 1 회 이상 정기 교체

제 11 조(Key 접근 권한 관리)

1. Key 저장소 접근은 최소 인원으로 제한한다.
2. 접근 권한 변경 시, CISO 승인 필요
3. Key 접근 기록은 1 년 이상 보관

제 5 장 결제 시스템 암호화 기준

제 12 조(결제 데이터 보호

1. 결제 API Key·Secret Key 는 반드시
    - HSM
    - Key Vault
    - Secrets Manager

    에 저장한다.

2. 결제 요청·응답 구간은 TLS 1.2 이상
3. Webhook 검증 시 Signature/Hash 기반 무결성 검증 필수

제 13 조(PG 연동 보안)

1. PG 사는 화이트리스트 기반 IP 제한
2. Callback/Webhook 은 다음 기준을 충족
    - Timestamp
    - Nonce
    - 서명 검증
    - Hash 무결성 검증
3. 결제 오류 발생 시 기록은 5 년 이상 보관

제 6 장 키 수명주기(Lifecycle) 관리

제 14 조(키 교체)

1. 주요 암호 키는 연 1 회 이상 정기 교체
2. 긴급 상황(Key 유출, 시스템 침해 등)은 즉시 폐기 및 신규 발행
3. 교체 시 서비스 영향 최소화를 위해 롤링 방식으로 적용

제 15 조(키 폐기)

1. 폐기 시 즉시 Key Vault/HSM 에서 삭제
2. 키를 포함한 백업파일·로그 등은 검색 후 즉시 제거
3. 폐기 절차는 문서화하여 1 년 이상 보관

제 7 장 점검 및 모니터링

제 16 조(정기 점검

1. 암호화 적용 여부 점검: 분기 1 회
2. Key Vault 접근기록 점검: 월 1 회

3. 환경파일(.env) 노출 여부 점검: 월 1 회
4. TLS 설정 점검: 반기 1 회

제 17 조(이상행위 모니터링)

1. Key Vault 접근 실패 반복
2. 비정상 시간대의 Key 조회
3. 해외 IP 에서의 접근
4. 동일 계정의 과도한 Key 접근

발생 시 즉시 CISO 보고

제 8 장 예외관리

제 18 조(예외 승인)

1. 환경 제한으로 암호화가 어려운 경우
2. 반드시 사유·위험 분석·대체 통제 포함
3. CISO 승인 후 한시적 적용
4. 만료 즉시 원복

제 9 장 부칙

제 19 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 20 조(개정)

본 지침은 정보보보호책임자의 검토 후 개정한다.