# 별첨 #8. 백업 및 복구 지침

# 제 1 장 총칙

### 제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 14 조(백업 및 복구)에 따라 서비스 운영 데이터의 무결성·가용성을 확보하고, 장애·사고 발생 시 신속한 복구가 가능하도록 백업·저장·검증·복구 절차를 명확히 정의함을 목적으로 한다.

### 제 2 조(적용 범위)

본 지침은 다음 항목의 백업 및 복구 절차에 적용한다.

1. 서비스 운영 DB
2. 사용자 데이터 및 결제 관련 데이터
3. 서버 설정파일, 환경파일(.env), 인증서
4. 애플리케이션 코드 및 배포 패키지
5. 로그(시스템·보안·결제)
6. 인프라 및 구성 정보(IaC, Terraform 등)

### 제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 주요 백업 정책 승인
   - 복구 절차 전반 감독
2. 시스템관리자
   - DB/서버 백업 수행 및 자동화 관리
   - 백업 무결성 검증
3. 정보보안담당자
   - 백업 보관·암호화·권한관리 점검
4. 개발팀
   - 코드/배포 패키지 버전 관리 및 아카이브

# 제 2 장 백업 정책

### 제 4 조(백업 종류 및 주기)

1. 증분 백업 (Incremental Backup)
   - 주기: 일 1 회 이상
   - 대상: DB, 로그, 설정파일

- 시간: 서비스 비사용 시간 또는 새벽시간대

2. 전체 백업 (Full Backup)
    - 주기: 매월 1 일
    - 대상:
        1. 전체 DB
        2. 서비스 코드 및 패키지
        3. OS 설정 및 보안정책
        4. 환경파일(.env), 인증서
        5. IaC(Terraform, Ansible 등)
    - 백업 후 중앙 백업 스토리지로 전송
3. 스냅샷(Snapshot) 백업
    - 클라우드 인프라 또는 VM 사용 시
    - 주기: 주 1 회
    - 장애 대응 목적의 단기 보관
4. 긴급 백업(Emergency Backup)
   다음 상황 발생 시 즉시 실시:
    - 결제 시스템 변경
    - DB Schema 변경
    - 긴급 보안 패치 전
    - 사고 대응 중 증적 확보 필요 시

## 제 5 조(백업 대상 데이터)

1. DB 백업
    - 전체 DB 덤프
    - 결제 트랜잭션
    - 사용자 정보
    - 환경/구성 테이블(환경설정)
2. 파일 백업
    - 설정파일(config, nginx/apache/waf rule)
    - .env 및 Secret 파일
    - 서비스 로그
    - 인증서(CA, TLS 인증서 등)
3. 코드 및 배포 아카이브
    - Git 기준 태그(tag)별 스냅샷
    - 빌드/배포 패키지(artifact)
4. 보안·네트워크 구성 정보
    - 방화벽/라우팅/보안장비 설정
    - WAF/UTM 정책
    - IaC 정의파일

# 제 3 장 백업 보관 및 보호

### 제 6 조(보관 기간)

1. 증분 백업: 30 일 이상
2. 전체 백업: 1 년 이상
3. 결제 관련 백업: 5 년 이상
4. 법령 요구 시 연장 가능

### 제 7 조(백업 암호화)

1. 백업 데이터는 AES-256 으로 암호화하여 저장한다.
2. 복호화 Key 는 Key Vault 또는 HSM 에서 관리한다.
3. 외부 저장소(S3·NAS 등) 저장 시 SSL/TLS 전송 적용

### 제 8 조(백업 접근 통제)

1. 백업 서버 및 저장소는 별도 접근권한 부여
2. 접근 가능자: 시스템관리자 + CISO 승인 인원
3. 백업 데이터 다운로드는 기록을 남기며 승인 필요
4. 백업 저장소는 외부 네트워크에서 직접 접속 불가

### 제 9 조(교차 백업—DR 전략)

정책서 기반(본사-지사 간 교차백업)

1. 백업본은 본사와 지사 각각에 저장
2. 동일 지역/Zone 만 사용하는 것을 금지
3. 클라우드 사용 시 Multi-AZ / Multi-Region 구성 가능
4. DR(Disaster Recovery) 저장소에는 아래 데이터 필수 보관
    - 전체 DB
    - 서비스 설정
    - 결제 로그 및 정산파일
    - API Key/Secret Key(암호화 형태)

# 제4장 백업 무결성 검증

### 제 10 조(무결성 검증 절차)

1. 백업 생성 후 자동으로 Hash(SHA-256 이상)를 생성
2. 저장소에 저장된 백업본의 Hash 와 비교하여 위변조 확인
3. DB 백업본은 실제 복원 테스트 또는 쿼리 수행으로 정상 여부 검증

4. 오류 발생 시 즉시 새 백업 생성

### 제 11 조(정기 무결성 점검)

1. 월 1 회 백업본 복원 테스트 실시
2. 테스트 항목
    - DB 복원 가능 여부
    - 웹/서비스 구성 복원 여부
    - 인증서 정상 작동
    - 환경파일(.env) 복원 후 서비스 정상부팅 확인
3. 결과는 문서화하여 1 년 이상 보관

# 제 5 장 복구 절차

---

### 제 12 조(복구 프로세스)

1. 장애 인지 → 백업본 선택 → 복원 → 서비스 정상화 → 보고
2. 복구 절차는 사고대응지침과 연계

### 제 13 조(DB 복구 절차)

1. 영향 여부 확인 (손상 테이블·데이터 파악)
2. 백업본 선택
    - 최신 증분백업 → 불가 시 전체백업
3. 복원 실행
4. 서비스 재기동 전 아래 확인
    - 인덱스 정상화
    - Foreign Key/데이터 참조 온전성
    - 결제 및 트랜잭션 데이터 무결성

### 제 14 조(결제 데이터 복구)

1. 스냅샷 또는 이미지로 복원
2. 패키지/코드 복원
3. 환경파일(.env) 복원
4. TLS 인증서 재설치
5. 로그/설정파일 정상 여부 확인

### 제 15 조(결제 정합성 검증)

1. PG 사와 대조하여 거래내역 복원
2. 중복결제 또는 미완료 거래 존재 여부 확인
3. 파라미터 변조나 서명 검증 오류 발생 내역 점검

4. 고객 영향 범위 분석 및 안내 준비

### 제 16 조(복구 후 검증)

1. 서비스 기능 정상 동작 테스트
2. 관리자 페이지 로그인·권한 테스트
3. 결제 테스트(개발 PG 환경에서 재현 테스트)
4. WAF/UTM 정책 정상 적용 확인

# 제 6 장 키 문서화 및 보고

### 제 17 조(백업·복구 기록 보관)

다음 항목을 기록하고 1 년 이상 보관한다.

- 백업 생성 로그
- 복원 테스트 결과
- 백업 오류 발생기록
- 복구 실행 내역 및 결과

### 제 18 조(보고 절차)

1. Critical/High 사고로 복구 수행 시 CISO 보고
2. 결제 데이터 영향 발생 시 PG 사·대표자 보고
3. 복구 완료 후 요약보고 작성
    - 장애 발생 원인
    - 복구 과정
    - 예방대책

# 제 7 장 예외관리

### 제 19 조(예외 승인)

1. 물리적/운영 환경에 따라 백업 불가 시 예외 적용 가능
2. 사유·대체안·위험 분석 포함
3. CISO 승인 후 한시적 허용
4. 기간 종료 즉시 원복

# 제 8 장 부칙

### 제 20 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

### 제 21 조(개정)

본 지침은 정보보호책임자의 검토 후 개정한다.