별첨 #10. 물리적 보안 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」의 물리적 보안 요구사항에 따라 정보시스템이 위치한 구역·장비·매체가 비인가자에게 접근·훼손·노출되지 않도록 물리적 보호 기준과 운영 절차를 규정함을 목적으로 한다..

제 2 조(적용 범위)

본 지침은 다음 시설 및 자산에 적용한다.

1. 서버실, 전산실, 개발실 등 주요 정보자산이 위치한 장소
2. 워크스테이션·노트북·모바일 기기 등 업무용 단말기
3. 네트워크 장비 및 보안장비(스위치, 라우터, UTM, WAF 등)
4. 백업 저장매체(NAS, 외장 스토리지, 백업서버)
5. 출입통제 시스템이 설치된 모든 구욕

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
    - 물리적 보안 정책 승인
    - 물리적 사고 발생 시 대응 총괄
2. 정보보안담당자
    - 출입기록 점검
    - 물리적 보안 점검 및 위험 분석
3. 시설 및 관리부서
    - 출입통제 운영 및 권한 부여
    - CCTV·시건장치·보안설비 유지관리
4. 임직원 및 협력업체
    - 허가된 구역만 출입
    - 보안시설 훼손·무단 변경 금지

제 2 장 물리적 구역 보호

제 4 조(보안 구역 구분)

시설은 다음과 같이 구분하여 관리한다.

1. 일반구역: 사무실, 회의실 등 출입 제한이 필요하지 않은 구역

2. 제한구역: 개발실, 운영실 등 제한된 인원만 출입 허용
3. 통제구역: 서버실·네트워크실·백업실 등 최고 수준 통제가 필요한 구역

제 5 조(출입통제 운영)

1. 통제구역은 출입카드·지문 등 인증 수단을 사용한다.
2. 출입 권한은 최소한의 인원에게만 부여한다.
3. 협력업체·외부인은 반드시 방문 등록 및 담당자 동행이 필요하다.
4. 출입 기록은 1 년 이상 보관한다.
5. 퇴사·계약 종료자는 즉시 출입 권한을 회수한다.

제 6 조(CCTV 운영)

1. 서버실·통제구역 주요 출입구에 CCTV 를 설치한다.
2. 촬영 영상은 최소 30 일 이상 보관한다.
3. CCTV 영상은 CISO 승인 없이 조회하거나 외부 반출할 수 없다.

제 3 장 장비 및 매체 보호

제 7 조(서버·네트워크 장비 보호)

1. 서버·보안장비는 잠금장치가 있는 랙(Rack)에 설치한다.
2. 랙 키는 지정된 관리자만 보관한다.
3. 장비 이동·교체 시 기록을 남기고 관리한다.
4. 비인가자의 장비 접촉은 금지한다.

제 8 조(업무용 PC·노트북 보안)

1. 업무용 단말기는 부재 시 잠금 상태 유지
2. 책상 위·회의실 등에 단말기를 방치 금지
3. 분실·도난 시 즉시 보안담당자에게 보고
4. 외부 출장 시 화면잠금·암호화 스토리지 사용 필수

제 9 조(이동식 저장매체 제어

1. USB·외장하드 등 이동식 매체는 원칙적으로 사용 금지
2. 사용이 필요한 경우 CISO 승인 필요
3. 승인된 경우에도 다음 요구사항 준수:
    - 악성코드 검사 필수
    - 민감정보 저장 금지
    - 사용 후 즉시 삭제 또는 회수

제4장 백업 및 보관 매체 보호

제 10 조(백업 매체 보안)

1. 백업 서버·NAS 는 잠금이 가능한 별도 공간에 보관한다.
2. 백업본은 평문 저장 금지(AES-256 암호화)
3. 백업 매체 접근 권한은 최소 인원에게만 부여한다.

제 11 조(매체 반출 통제)

1. 데이터가 포함된 매체는 무단 반출 금지
2. 외부 반출이 필요한 경우 CISO 승인 필수
3. 반출 시 다음을 기록한다.
    - 반출자
    - 반출 목적
    - 반출 시각 및 반입 예정일
4. 반입 후 무결성 여부를 점검한다

제 5 장 물리적 점검 및 이상행위 대응

제 12 조(정기 점검)

1. 서버실·통제구역 물리적 점검은 월 1 회 이상 실시한다.
2. 점검 항목
    - 출입통제 정상 여부
    - 잠금장치·도어락 정상 동작
    - CCTV 운용 상태
    - 장비 훼손·이상 여부
3. 점검 결과는 1 년 이상 보관한다.

제 13 조(이상행위 대응)

다음 행위가 발생하면 즉시 정보보호책임자(CISO)에 보고한다.

1. 비인가 시간대의 출입
2. 반복적인 출입 실패 로그
3. 장비 훼손·열림 상태
4. CCTV 사각지대 접근 시도
5. 통제구역 내 무단 촬영·녹음 행위

제 14 조(물리적 사고 대응)

1. 사고 발생 시 즉시 서버실 격리 또는 전원 차단 검토
2. 사고 원인 조사(출입기록·CCTV·장비 상태)
3. 장비 교체 또는 복구
4. 사고 보고서 작성 후 CISO 승인

제 6 장 예외관리

제 15 조(예외 승인)

1. 특정 구역에 물리적 장치를 설치할 수 없는 경우 등 예외가 필요할 수 있다.
2. 사유·위험 분석·대체 통제를 포함하여 CISO 승인 후 적용한다.
3. 예외 기간 만료 즉시 원복한다.

제 7 장 부칙

제 16 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 17 조(개정)

본 지침은 정보보호책임자의 검토 후 개정한다.