별첨 #9. 보안 교육 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 15 조(보안 교육)에 따라 임직원 및 협력업체의 보안 인식을 강화하고, 서비스 운영에 필요한 보안 실무 역량을 체계적으로 확보하기 위한 보안 교육 운영 기준을 규정함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 대상에게 적용한다.

1. EAT-IT 전체 임직원
2. 외부 개발·운영 인력
3. 협력업체 및 유지보수 인력
4. 신규 입사자
5. 필요 시 계약직·파트너사 직원

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 보안 교육 총괄
   - 교육 계획 승인
   - 미이수자 조치 결정
2. 정보보안담당자
   - 교육 설계·운영 평가
   - 피싱 훈련 기획
   - 교육 결과 보고
3. 인사·관리부서
   - 교육 일정 공지
   - 교육 이수 관리
4. 임직원 및 협력업체
   - 지정된 교육 이수 의무
   - 보안정책 준수

제 2 장 정기 보안 교육

제 4 조(연 1 회 필수 보안 교육)

1. 전 임직원 및 외부 운영 인력은 연 1 회 이상 보안 교육을 반드시 이수해야 한다.
2. 교육 내용에는 최소 다음 항목 포함:
    - 개인정보보호 및 데이터 처리 원칙
    - 내부 정보 접근 규칙
    - 계정·비밀번호 관리
    - 악성코드·랜섬웨어 예방
    - 피싱·스미싱 대응
    - 물리적 보안
    - 모바일/원격근무 보안
    - 사고 발생 시 보고 절차
    - 밥세권 서비스 보안정책 주요 내용

제 5 조(부서별 실무형 교육)

1. 개발/운영/보안/기획 등 실무 관련 부서는 역할 기반 보안 교육(Role-Based Training)을 분기 또는 반기 단위로 시행한다
2. 예시
    - 개발팀: 보안코딩, OWASP Top 10, API 인증, 환경파일 보안
    - 운영팀: 서버 구성 보안, 패치 관리, 로그 분석
    - 보안팀: WAF/UTM 정책 운영, 침해사고 대응 실습
    - 기획/마케팅: 개인정보 처리 절차, 서비스 흐름 기반 보안 고려

제 3 장 신규 입사자 보안 교육

제 6 조(입사 즉시 교육)

1. 신규 입사자는 입사 첫날 또는 업무 시작 전 신규자 보안교육을 이수해야 한다.
2. 필수 교육 항목
    - 사내 보안정책 및 지침
    - 계정 발급 절차 및 접근통제
    - 기기 보안(노트북, 모바일 등)
    - 민감정보 처리 원칙
    - 외부 저장매체 사용 금지 정책
    - 사고 발견 보고 절차

제 7 조(미이수자 조치)

1. 교육 미이수자는 시스템 접근 권한 제한 또는 CISO 승인 필요
2. 협력업체 미이수 시 계약 준수 위반으로 간주
3. 반복 미이수자는 관리자에게 즉시 통보

제 4 장 피싱·랜섬웨어 대응 훈련

제 8 조(정기적인 모의 피싱 훈련)

1. 연 1~2 회 모의 피싱 훈련을 시행한다.
2. 훈련 유형
    - 이메일 피싱
    - 스미싱(문자 피싱)
    - 악성 URL 유도
3. 결과는 다음과 같이 분류
    - 클릭/입력 여부
    - 신고 여부
    - 대응 속도

제 9 조(랜섬웨어 대응 교육)

1. 악성 첨부파일 열람 금지
2. 개별 PC 백업 점검
3. 의심파일 발견 시 즉시 보안담당자 전달
4. 사고 발생 시 격리 절차 교육
5. 실제 사례 기반 설명 포함

제 5 장 운영 환경 보안 교육

제 10 조(클라우드·인프라 보안 교육)

필요 시 다음 분야 교육 진행

1. IAM 최소권한 설계
2. 보안그룹 관리
3. 로그 수집 및 경보 설정
4. Key Vault/Secrets Manager 운영

제 11 조(개발자 보안코딩 교육)

반기 1 회 이상 개발자를 대상으로 다음 교육을 시행한다.

1. 입력값 검증
2. 인증/인가 로직 구현
3. 환경파일(.env) 보안

4. JWT·OAuth·세션 보안
5. API Rate Limiting
6. 결제 파라미터 변조 방지

제 6 장 교육 운영 및 기록 관리

제 12 조(교육 방식)

다음 중 하나 또는 다수 방식으로 진행한다.

1. 온라인 교육
2. 집합 교육(오프라인)
3. 워크숍/세미나
4. 실습 기반 교육(Hands-on)

제 13 조(교육 이력 관리)

1. 교육 참석 기록은 1 년 이상 보관한다.
2. 기록 항목
    - 참석자 이름/부서
    - 교육 일시
    - 교육 내용
    - 시험/평가 여부
    - 훈련 결과(피싱 등)

제 14 조(교육 평가)

1. 필요 시 교육 이해도 평가 수행
2. 개발자/운영자 대상은 실습 기반 평가 가능
3. 평가 결과는 인사고과에 반영될 수 있다

제 7 장 예외관리

제 15 조(예외 승인)

1. 교육 참여가 불가피하게 어려운 경우
2. 사유서 제출 후 CISO 승인 필요
3. 승인 기간 종료 후 지체 없이 교육 이수

제 8 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.