SEC-401 정보보안 및 데이터 분류/반출 규정

문서번호	SEC-401	버전	v1.0
시행일	2026-01-01	제정/개정	제정
소관부서	정보보안팀(InfoSec)	적용범위	전 임직원 및 협력사(접속 계정 보유자)
보안등급	사내 제한(직무)	승인	CISO

※ 목차는 Word 에서 '참조 > 목차'로 자동 생성할 수 있습니다.

개정 이력

버전	일자	개정 내용	작성/검토
v1.0	2025-12-08	데이터 분류/반출/외부 공유 기준 제정	InfoSec/법무/IT

용어 정의

기밀정보: 유출 시 회사/고객에 중대한 피해가 발생할 수 있는 정보

개인정보: 식별 가능한 개인에 관한 정보(이름, 연락처, 식별자 등)

반출: 회사 관리 영역(사내망/승인된 클라우드) 밖으로 데이터가 이동하는 행위

1. 데이터 분류 체계

등급	예시	보관/전송 기준
Public(공개)	채용 공고, 보도자료	제한 없음
Internal(사내)	일반 업무 문서	사내 계정 기반 공유
Confidential(기밀)	재무결산 자료, 소스코드, 고객 계약	암호화 + 접근제어 + 로그
Restricted(제한)	고객 개인정보 원본, 보안키, 인증정보	승인된 저장소만, 반출 금지(예외 절차)

2. 외부 공유 및 반출 원칙

- 기밀/제한 등급은 이메일 첨부 전송 금지(승인된 보안 전송 채널 사용).
- 개인 메신저/개인 클라우드(개인 구글드라이브 등) 업로드 금지.
- 협력사 공유는 NDA 체결 및 최소 권한 원칙을 준수한다.

3. 반출 예외 절차

1. 반출 필요 사유(업무 목적, 범위, 기간)를 작성한다.
2. 데이터 최소화(필요한 컬럼/기간만) 및 마스킹/익명화 적용을 우선 검토한다.
3. 승인 라인: 팀장 -> InfoSec -> 법무(계약/개인정보 포함 시) -> CISO(제한 등급)
4. 승인된 채널(보안 파일 전송/VDI 등)로만 반출하며, 만료 기간을 설정한다.

참고: 승인 없이 반출이 발생한 경우 즉시 보안팀에 사고 신고해야 한다(사고 대응 절차 SEC-701).

4. LLM/외부 AI 서비스 사용

- 외부 AI 서비스에 회사 '기밀/제한' 정보를 입력하는 행위는 금지한다.
- 내부 승인된 LLM/RAG 시스템만 사용하며, 프롬프트/응답 로그는 보안 규정에 따라 보관한다.
- 모델 학습/저장에 입력 데이터가 사용되는지(옵트아웃 포함) 정책을 사전 확인한다.

5. 위반 시 조치

고의 또는 중대한 과실로 보안 위반 시 징계 및 법적 조치가 가능하며, 손해배상 책임이 발생할 수 있다.

부록

E1. 반출 요청서 필수 항목

항목	내용
데이터 등급	Internal/Confidential/Restricted
반출 목적	프로젝트/고객 지원/외부 감사 등
반출 범위	파일명, 레코드 수, 기간
보호 조치	암호화, 마스킹, 만료일
수신자	조직/담당자, NDA 여부

본 문서는 테스트용으로 생성된 가상의 회사 내규 예시입니다. 실제 업무 적용 전 반드시 회사 공식 규정/담당 부서 확인이 필요합니다.