

# 데이터 보안 및 개인 정보 보호 가이드라인 (AI 시스템용)



작성자: 데이터 보안 팀

날짜: 2023년 10월 5일

# 목차

---

1	요약	2
2	핵심 보안 원칙	3
2.1	출력물 최소화 및 즉시 수거	3
2.2	추측 가능한 데이터 피하기	3
2.3	안전한 기록 관리	3
2.4	FATF 규제 준수	3
2.5	IPFS DePIN 통합	4
3	결론	5



# 1 요약

이 리포트는 AI 시스템에서 개인 정보를 안전하게 처리하기 위한 보안 프레임워크를 제시합니다.  
주요 원칙은 최소한의 데이터 노출, 추측 가능한 정보를 피하고, FATF 지침 준수, IPFS DePIN  
통합을 포함합니다.



## 2 핵심 보안 원칙

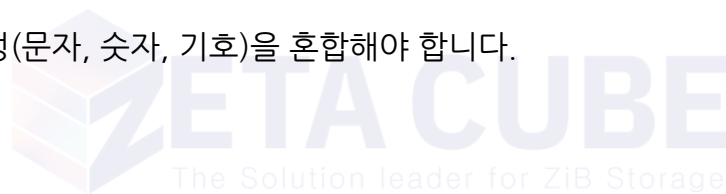
효과적인 데이터 보호는 개인 정보 노출을 최소화하고, 접근 제어를 강화하며, 안전한 기록 관리를 보장하는 체계적인 접근 방식을 필요로 합니다.

### 2.1 출력물 최소화 및 즉시 수거

업무 용도에 따라 출력 항목을 최소화하고 즉시 수거하여 유출 위험을 줄입니다. 제어된 물리적 접근이 있는 보안 공간에서 처리가 권장됩니다.

### 2.2 추측 가능한 데이터 피하기

연속적인 숫자, 생일, 전화번호와 같은 추측 가능한 데이터를 사용하지 마십시오. 비밀번호는 2가지 이상의 특성(문자, 숫자, 기호)을 혼합해야 합니다.



### 2.3 안전한 기록 관리

월렛 개인키, 암호화 키 또는 패스프레이즈가 로그에 포함되는 경우, 강력한 암호화 프로토콜을 사용하여 보관해야 합니다. 비밀번호는 12개 이상의 무작위 단어를 사용하는 것이 권장됩니다.

### 2.4 FATF 규제 준수

FATF 가이드라인은 거래 금액, 빈도, 송수신인 프로필 및 자금 출처에 대한 검증을 요구합니다. 두 가지 이상의 검색 조건을 사용하여 개인 정보 조회를 제한하십시오.

## 2.5 IPFS DePIN 통합

IPFS DePIN은 AI 시스템에서 개인 정보를 분산된, 안전한 방식으로 처리하도록 보장합니다.

이는 공유 데이터 소유권 및 탈중앙화된 보안을 가능하게 합니다.



### 3 결론

지속적인 데이터 보안은 위험을 완화하기 위해 적극적인 모니터링, 정기적인 보안 업데이트 및 FATF 규제 준수를 포함해야 합니다. IPFS DePIN과 같은 기술은 개인 정보 보호 및 시스템 효율성 모두를 강화합니다.

