

# 데이터 보안 및 개인 정보

## 보호 최고의 관행



작성자: 보안 팀

날짜: 2023-10-15

# 목차

---

1	요약	2
2	데이터 보안 프로토콜	3
2.1	비밀번호 및 자격 증명 관리	3
2.2	데이터 저장 및 암호화	3
2.3	출력물 관리	3
2.4	개인 정보 제외	3
2.5	백업 절차	3
3	결론	4



# 1 요약

이 리포트는 개인 정보 및 민감한 데이터를 보호하기 위한 구조화된 보안 프로토콜을 강조합니다. 주요 주제는 비밀번호 관리, 데이터 저장, 출력물 처리, 개인 정보 제외 및 백업 절차를 포함합니다.



## 2 데이터 보안 프로토콜

개인 정보 노출을 방지하기 위한 구조화된 지침을 강조합니다.

### 2.1 비밀번호 및 자격 증명 관리

예측 가능한 비밀번호(예: 생일, 전화번호)를 피하고 공개 영역(예: 포스트잇)에서 자격 증명 노출을 금지합니다. 테스트 또는 회사명과 같은 쉽게 유추 가능한 항목도 피합니다.

### 2.2 데이터 저장 및 암호화

필요한 경우 암호화하여 모바일 장치에 문서를 저장합니다. 월렛 개인키가 포함된 로그는 암호화하여 보관합니다.

### 2.3 출력물 관리



개인 정보가 포함된 출력물은 최소화하여 출력하고 즉시 수거하여 유출을 방지합니다.

### 2.4 개인 정보 제외

출력물 및 로그에서 주민등록번호 및 회원번호와 같은 개인 식별자(ID)를 제외합니다.

### 2.5 백업 절차

풀 백업을 기본으로 하여 차등 백업을 진행합니다. 민감한 데이터(예: 월렛 관련 데이터)는 소산백업을 통해 보호합니다.

### 3 결론

이러한 프로토콜은 데이터 유출을 방지하고 개인 정보를 보호하는 데 중요한 역할을 합니다.

정기적인 감사 및 보안 업데이트는 이러한 관행을 효과적으로 유지하는 데 필수적입니다.

