개인정보 보호 및 보안

관리 지침

작성자: 보안 팀

날짜: 2023-10-25

목차

1 요약

본 지침은 출력물 최소화, 추측 가능한 정보 제한, 데이터 저장 및 백업 관리, 월렛 관련 로그 암호화, 그리고 개인/법인별 데이터 처리를 통해 개인정보 보호를 강화하는 것을 목표로 합니다.

2 개인정보 보호 관리 프레임워크

본 문서는 업무 효율성과 개인정보 보호를 균형 있게 유지하기 위해 출력물 관리, 비밀번호 관리, 데이터 보관, 로그 보안 및 백업 전략을 다룹니다.

2.1 출력물 최소화 및 수거

업무 목적에 따라 출력 항목을 최소화하고 즉시 수거하여 무단 접근을 방지합니다. 출력물은 즉시 회수되어 보안 저장소에 보관됩니다.

2.2 추측 가능한 정보 제한

생일, 연속적인 숫자, 전화번호, 또는 아이디와 유사한 비밀번호는 사용하지 않습니다. 테스트용 회사명 또는 유추 가능한 용어는 금지됩니다.

2.3 모바일 저장 제한 및 암호화

문서 파일은 모바일 기기에 저장하지 않습니다. 업무상 저장이 필요한 경우 암호화 및 접근 제한을 통해 보안을 강화합니다.

2.4 로그 내 월렛 개인키 보안

로그에 월렛 개인키, 암호화 키 또는 패스프레이즈가 포함되지 않도록 합니다. 포함된 경우 암호화하여 보관하여 무단 접근을 방지합니다.

2.5 데이터 백업 전략

풀 백업을 기본으로 하여 차등 백업을 사용합니다. 웰렛 운영 데이터 및 민감한 정보에는 소산 백업을 적용하여 데이터 유출 위험을 최소화합니다.

3 결론

본 지침은 출력물 관리부터 데이터 백업까지의 체계적인 접근 방식을 통해 보안과 효율성을 균형 있게 유지합니다. 지침 준수는 위험을 완화하고 개인정보 보호를 강화하는 데 필수적입니다.