

개인정보 보호 처리 지침



작성자: 보안 팀

날짜: 2023-10-25

목차

1 요약	2
2 개인정보 처리 보안 조치	3
2.1 개인정보 출력물 안전 처리	3
2.2 비밀번호 및 자격 증명 보안	3
2.3 안전한 로깅 관행	3
2.4 데이터베이스 자격 증명 관리	3
2.5 테스트에서 추적 가능한 정보 피하기	4
3 결론	5



1 요약

본 리포트는 개인정보를 안전하게 관리하기 위한 구조화된 지침을 제공하며, 출력물, 비밀번호, 로깅, 데이터베이스 및 검색 프로세스에 대한 조치를 강조합니다.



2 개인정보 처리 보안 조치

본 섹션은 출력물, 비밀번호, 로깅 및 검색 프로세스에 대한 보안 조치를 강조합니다.

2.1 개인정보 출력물 안전 처리

개인정보 출력물은 업무 용도에 따라 최소화되어야 하며, 즉시 수거해야 합니다. 출력물은 주민등록번호와 같은 민감한 정보를 포함해서는 안됩니다. 검색은 두 가지 이상의 조건을 통해 제한해야 합니다.

2.2 비밀번호 및 자격 증명 보안

생일 또는 전화번호와 같은 예측 가능한 비밀번호는 피해야 합니다. 비밀번호 노출(예: 포스트잇)은 금지됩니다. 데이터베이스 자격 증명은 하드코딩되어서는 안됩니다.



2.3 안전한 로깅 관행

로그는 월렛 개인키 또는 암호화 키를 저장해서는 안됩니다. 이러한 정보가 포함될 경우 암호화하여 보관해야 합니다.

2.4 데이터베이스 자격 증명 관리

데이터베이스 자격 증명은 프로그램 코드에 하드코딩되어서는 안됩니다. 대신 보안 저장소를 사용하고 암호화해야 합니다.

2.5 테스트에서 추적 가능한 정보 피하기

테스트는 회사명 또는 사용자 신상과 같은 추적 가능한 정보를 사용해서는 안됩니다. 테스트 데이터는 가상 데이터로 대체해야 합니다.



3 결론

이러한 지침을 준수함으로써 조직은 개인정보 유출을 최소화하고 법적 위험을 완화하며, 개인 데이터를 보호하기 위한 체계적인 접근 방식을 보장합니다.

