데이터 보안 조치 보고서 – **AES-256** 암호화 적용

변경사항			
항목	암호화	적용여부	마이그레이션
이름		X	X
연락처	AES256	O	O
주소(동/호수)	AES256	O	O
계좌번호	AES256	O	O
비밀번호	SHA256	O	O
주민번호	AES256	O	O
엑셀다운로드	계정 패스워드 입력	O	X

1. 개요

본 문서는 서비스 내 사용자 정보 및 민감 데이터를 보호하기 위한 **AES-256** 암호화 적용 현황을 설명하며, 암호화 알고리즘, 적용 위치, 키 관리 방식을 포함한 기술적 보안 조치 사항을 보고합니다.

2. 적용 배경

- 개인정보보호법 및 ISMS-P 등 보안 인증 요건 준수
- 외부 유출 시 민감 정보 보호를 위한 비가역적 암호화
- DB 내 평문 데이터 저장 방지

3. 암호화 방식

항목	내용
알고리즘	AES (Advanced Encryption Standard)
키 길이	256비트 (AES-256)

항목	내용
블록 모드	ECB
패딩 방식	PKCS5Padding
문자 인코딩	Base64 인코딩 후 저장

4. 적용 대상

- 사용자 비밀번호 (SHA2 해싱 + AES-256 보완 시)
- 주민등록번호 또는 외부 인증 식별값
- API 통신 시 민감 파라미터
- 로그 저장 시 민감 필드 마스킹/암호화

5. 구현 방식

- 언어/프레임워크: Java (Kotlin),
- 암호화 키 관리: 별도 관리

6. 키 관리

- 암호화 키는 서버 내 보안 관리 시스템(AWS)을 통해 주입
- 정기적 키 교체 계획 수립 (예정)

7. 테스트 및 검증

- 단위 테스트 및 E2E 테스트에서 암복호화 정확성 검증 완료
- 복호화 실패 시 예외 핸들링 및 로깅 구현