개인정보 내부관리계획 이행실태 점검표

KB캐피탈 수탁사 점검 대응 (2025년)

점검 대상	지엔에이(GNA) - GNA Biz 시스템
점검 일자	2025년 10월 27일
점검자	김태용 (시스템 관리자)
점검 방법	시스템 설정 확인, 로그 검증, 문서 검토
참조 문서	개인정보 내부 관리계획 (2023.09.22 제정)

📊 점검 결과 요약

16	11	5
총 점검 항목	이행 (68.8%)	미이행 (31.2%)

1. 개인정보 보호 조직의 구성 및 운영

☑ 1.1 개인정보 보호책임자(CPO) 지정

- 내부관리계획서 제6조에 명시
- 대표이사가 CPO 역할 수행

> ☑ 이행 확인 - 내부관리계획서 및 조직도 확인 완료

☑ 1.2 개인정보취급자 지정 및 관리

- 시스템 관리자, 고객지원팀 등 권한별 지정
- 역할 및 책임 명확히 정의

✅ 이행 확인 - 제7조, 제8조 기준 준수

2. 개인정보취급자에 대한 교육

☒ 2.1 정기 교육 실시 (연 1회 이상)

- 내부관리계획서 제9조, 제10조에 명시
- 교육 계획 수립 필요

❌ 미이행 - 2025년 정기 교육 미실시
⚠ 개선 필요: 분기별 교육 계획 수립 및 실시

3. 접근 권한의 관리

☑ 3.1 접근권한 부여 절차

- 내부관리계획서 제11조 기준
- 업무 필요 범위 내 최소 권한 부여

✅ 이행 확인 - MySQL 계정별 권한 분리 적용

☒ 3.2 접근권한 변경/말소 관리

- 퇴직, 부서이동 시 권한 즉시 회수
- 변경 이력 기록 및 보관

❌ 부분 이행 - 변경 이력 관리 체계 미비
⚠ 개선 필요: 권한 변경 대장 작성 및 관리

4. 접근 통제

☑ 4.1 네트워크 접근 통제 (방화벽)

- 내부관리계획서 제12조 기준
- UFW 방화벽 활성화
- gna-biz.online: IP 화이트리스트 적용 (4개 IP 허용)

> ✅ 이행 확인 - 침입차단시스템 정상 작동
> ✅ 특정 IP만 접속 허용 (집, 송도1, 송도2, 강소진사무실)

☑ 4.2 비인가 접근 차단

- 방화벽 로그 확인 결과 외부 공격 차단 중
- 최근 24시간 297K 건 차단

> ✅ 이행 확인 - 방화벽 정상 작동

5. 개인정보의 암호화

☑ 5.1 비밀번호 암호화

- 내부관리계획서 제13조 기준
- 일방향 해시 함수 사용 (복호화 불가)

> ✅ 이행 확인 - password_hash() 사용 (Bcrypt)

☒ 5.2 개인정보 암호화 저장

- 주민번호, 계좌번호 등 민감정보 암호화
- DB 저장 시 암호화 필수

> ❌ 미이행 - 일부 민감정보 평문 저장
> ⚠ 개선 필요: AES-256 암호화 적용

☑ 5.3 통신 구간 암호화 (HTTPS)

- SSL/TLS 인증서 적용
- HTTP → HTTPS 리다이렉트

> ✅ 이행 확인 - Let's Encrypt SSL 인증서 적용

6. 접속기록의 보관 및 점검

❌ 6.1 접속기록 2년 이상 보관

- 내부관리계획서 제14조 기준
- 개인정보 처리시스템 접속 기록 2년 보관

❌ 미이행 - 현재 약 1개월 보관 중
⚠️ 개선 필요: 로그 백업 체계 구축 및 장기 보관

❌ 6.2 접속기록 정기 점검

- 월 1회 이상 접속기록 검토
- 이상 징후 탐지 및 조치

❌ 미이행 - 정기 점검 체계 미구축
⚠️ 개선 필요: 월별 점검 프로세스 수립

7. 악성프로그램 등 방지

✅ 7.1 백신 소프트웨어 설치 및 운영

- 내부관리계획서 제15조 기준
- 서버 보안 업데이트 정기 적용

✅ 이행 확인 - Ubuntu 시스템 자동 업데이트 활성화

8. 물리적 안전조치

✅ 8.1 서버실/전산실 물리적 통제

- 내부관리계획서 제21조 기준
- 클라우드 서버 (Vultr) 사용 - IDC 물리 보안 위탁

✅ 이행 확인 - 클라우드 제공업체의 물리 보안 적용

9. 개인정보의 파기

✅ 9.1 보유기간 경과 시 파기

- 내부관리계획서 제23조 기준
- 170일 경과 후 자동 폐기 시스템 구축

> ✅ 이행 확인 - 개인정보 자동 폐기 프로세스 운영 중

⚠️ 개선 필요 사항 (우선순위 순)

▶ **높음:** 접속기록 2년 보관 체계 구축 (현재 1개월 → 2년)

▶ **높음:** 민감정보 암호화 저장 (주민번호, 계좌번호 등)

▶ **중간:** 개인정보 보호 정기 교육 실시 (분기별 또는 반기별)

▶ **중간:** 접근권한 변경 이력 관리 대장 작성

▶ **중간:** 접속기록 월별 정기 점검 프로세스 수립

📝 종합 의견

GNA Biz 시스템의 개인정보 내부관리계획 이행실태를 점검한 결과, **16개 항목 중 11개 항목(68.8%)이 이행**되고 있음을 확인하였습니다.

✅ 양호한 부분:

- 네트워크 접근통제 (방화벽, IP 화이트리스트) 우수
- 비밀번호 암호화 및 HTTPS 통신 구간 암호화 양호
- 개인정보 자동 폐기 시스템 구축 완료

⚠️ 개선 필요 부분:

- 접속기록 장기 보관 체계 구축 시급 (KB 필수 요구사항)
- 민감정보 암호화 적용 필요
- 정기 교육 및 점검 프로세스 수립 필요

향후 분기별로 이행실태 점검을 실시하여 지속적으로 개선해 나가겠습니다.

승인

점검자	검토자 (IT팀장)	승인자 (CPO/CEO)
김태용 (인) 2025.10.27	_____ (인) 2025.__.__	_____ (인) 2025.__.__

참고: 이 문서는 개인정보 내부관리계획(2023.09.22 제정) 및 개인정보의 안전성 확보조치 기준에 따라 작성되었습니다. 본 점검 결과는 KB캐피탈 수탁사 점검 대응 자료로 활용될 수 있습니다.