국가·공공기관 AI보안 가이드북

국가·공공기관 AI보안 가이드북

기준 문서: 국가·공공기관 AI보안 가이드북 (2025.12) · 적용 범위: 공공(권고) · 확인일 2026-10-23

조항 57개의 PCFILTER 지원 유형(지란지교소프트 판단)

부분 지원 4 증적 지원 1 재확인 중 2 고객 관리 필요 10 외부 솔루션·별도 통제 필요 40

재확인 중 2개는 판정 규칙에 따라 지원 유형을 다시 확인하고 있어 아래 표에서 뺐습니다.

제품이 돕는 주요 조항

조항	요구	지원 유형
M09	AI시스템 로깅 · 모니터링	부분 지원
M13	입 · 출력 필터링	부분 지원
M15	가드레일 다중화	부분 지원
M17	AI시스템 경계보안 강화	부분 지원
M30	사용자 교육 및 보안정책 수립	증적 지원

고객이 할 일

- 외부 AI 파일 입력 승인 절차를 내부 규정으로 정하고, 승인 이력을 보관
- 프롬프트 로그를 정기 분석하고 분석 기록 보관, AI 응답(출력) 로그는 별도 수단 마련
- 생성형 AI별 차단 정책·개인정보 정책 설정, 기밀 키워드 등록, 출력 필터링·적대적 문구 탐지는 별도 수단 마련
- 외부 AI 파일 첨부 차단·확장자·크기 정책 설정, 프롬프트 길이·횟수 제한은 별도 수단 마련
- PC 측 통제 외에 중계서버·AI서비스 보안기능 등 다른 단계의 보호장치를 함께 배치
- 허용할 외부 AI서비스 목록과 그룹·사용자별 정책 지정, 망연계 구간 방화벽·중계서버는 별도 구성

이 내용은 법률 자문이 아닙니다. 적용 여부는 조직의 상황에 따라 다릅니다. 지원 유형은 지란지교소프트의 판단이며 인증기관의 판단이 아닙니다. 실무에 참고용으로만 활용하시기 바랍니다.

발행 지란지교소프트 데이터사업부문 · 자사 제품 기준 · AI 판정 후 원문 대조 · 판정 v15(2026-10-23) · 생성 2026-11-02
근거 문서: 국가·공공기관 AI보안 가이드북(국정원, 2025.12) https://www.ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bi4IwVbci5a1FamchlW1qNssCyKZu6ZLfUXAiW9SUOAvNweQY_U_riHeJG4MbYAX_3cYu0dKvbkFyAgc_uNHfeX
조항별 원문 출처는 사이트의 조항 카드에 있습니다.