공공기관 업무에 생성형 AI 활용

N2SF가 예시로 든 '업무환경에서 생성형 AI 활용' 모델의 보안통제와 AI 보안 가이드북 항목(에이전틱 AI 보안대책 포함)을 봅니다.

구성 기준: 국가정보원 N2SF 정보서비스 모델 해설서 모델 2(업무환경에서 생성형 AI 활용, 2025.9)가 보안대책으로 든 통제 64개와 국가·공공기관 AI보안 가이드북 항목을 모았습니다(회사 정리).

조항 121개의 PCFILTER 지원 유형(지란지교소프트 판단)

직접 지원 1 · 부분 지원 15 · 증적 지원 6 · 재확인 중 6 · 고객 관리 필요 12 · 외부 솔루션·별도 통제 필요 79 · 확인 중 2

재확인 중 6개는 판정 규칙에 따라 지원 유형을 다시 확인하고 있어 아래 표에서 뺐습니다.

제품이 돕는 주요 조항

조항	요구	지원 유형
N2SF 보안 가이드라인 N2SF-DV-4	하드웨어 — 포트 및 입출력 장치 제어	직접 지원
N2SF 보안 가이드라인 N2SF-BC-1	블루투스 연결 — 블루투스 데이터 통신 제한	부분 지원
N2SF 보안 가이드라인 N2SF-DA-2	단말인증 — 정보서비스 식별 및 제한	부분 지원
N2SF 보안 가이드라인 N2SF-DT-1	데이터 전송 — 전송 권한 확인	부분 지원
N2SF 보안 가이드라인 N2SF-DU-2	데이터 사용 — 데이터 암호화 저장	부분 지원
N2SF 보안 가이드라인 N2SF-DV-6	하드웨어 — 통신 기능이 포함된 저장장치 제한	부분 지원
N2SF 보안 가이드라인 N2SF-IF-10	정보흐름 — 정보 전송 방식 제한	부분 지원
N2SF 보안 가이드라인 N2SF-IF-6	정보흐름 — 필터링 규칙 정보흐름 통제	부분 지원
N2SF 보안 가이드라인 N2SF-IF-7	정보흐름 — 데이터 유형 식별자 통제	부분 지원
N2SF 보안 가이드라인 N2SF-IF-8	정보흐름 — 인가되지 않은 정보 전송 통제	부분 지원
N2SF 보안 가이드라인 N2SF-IN-1(1)	정보시스템 구성요소 — 정보시스템 구성요소 최신상태 유지	부분 지원
N2SF 보안 가이드라인 N2SF-IN-6	정보시스템 구성요소 — 불필요한 구성요소 제거	부분 지원

외 10개 조항은 사이트에서 볼 수 있습니다.

고객이 할 일

- 모니터링 대상·알림 임계치 설정, 계정 활동 모니터링은 IAM·UEBA로 보완
- PC OS 비밀번호 정책(복잡도·주기) 적용은 OS·AD에서 설정
- 생체·토큰 인증체계 도입은 고객 몫, PCFILTER는 설정 여부 점검
- 허용할 정보서비스(사이트·AI·소프트웨어) 목록을 정한다.
- 결재 라인과 승인 기준을 정한다.
- 개인정보 외 업무정보 암호화는 별도 수단(DRM 등)으로 정한다.

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 망 보안체계 보안 가이드라인 1.0(국정원, 2025.9) https://www.ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bi4IwVbci5a1FamchlW1qNssCyKZu6ZLfUXAiW9SUOAvKlgmp4pbcUcyETJn6NrHSIACCUP_xvUj35ZGb7sJqI4
근거 문서: 국가 망 보안체계 보안 가이드라인 1.0(국정원, 2025.9) 부록2 모델2 https://www.ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bi4IwVbci5a1FamchlW1qNssCyKZu6ZLfUXAiW9SUOAvKlgmp4pbcUcyETJn6NrHSIACCUP_xvUj35ZGb7sJqI4
근거 문서: 국가 망 보안체계 보안 가이드라인 1.0(국정원, 2025.9) 부록1 https://www.ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bi4IwVbci5a1FamchlW1qNssCyKZu6ZLfUXAiW9SUOAvKlgmp4pbcUcyETJn6NrHSIACCUP_xvUj35ZGb7sJqI4
근거 문서: 국가 망 보안체계 보안 가이드라인 1.0(국정원, 2025.9) 부록2 모델4 https://www.ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bi4IwVbci5a1FamchlW1qNssCyKZu6ZLfUXAiW9SUOAvKlgmp4pbcUcyETJn6NrHSIACCUP_xvUj35ZGb7sJqI4
근거 문서: 국가 망 보안체계 보안 가이드라인 1.0(국정원, 2025.9) 부록2 모델10 https://www.ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bi4IwVbci5a1FamchlW1qNssCyKZu6ZLfUXAiW9SUOAvKlgmp4pbcUcyETJn6NrHSIACCUP_xvUj35ZGb7sJqI4
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.