

AI 보안 현황 자가진단 체크리스트

기업 IT 보안 담당자용 | 소요 시간 약 5분



01 영역 1. AI 사용 현황 파악

#	점검 항목	예	아니오	모름
1	직원들이 업무에 사용하는 AI 서비스 목록을 파악하고 있다	☐	☐	☐
2	부서별·사용자별 AI 서비스 접속 이력을 조회할 수 있다	☐	☐	☐
3	IT팀이 승인하지 않은 AI 서비스 (Shadow AI) 사용 여부를 탐지할 수 있다	☐	☐	☐
4	개발팀이 사용하는 AI 코딩 도구 (Copilot, Claude Code, Codex 등)의 종류를 파악하고 있다	☐	☐	☐

02 영역 2. 접근 통제 및 정책

#	점검 항목	예	아니오	모름
5	생성형 AI 서비스에 대한 공식적인 허용/차단 정책이 존재한다	☐	☐	☐
6	AI 서비스를 전체 차단이 아닌 사용자·그룹별로 차등 허용할 수 있다	☐	☐	☐
7	웹 기반 AI(ChatGPT, Gemini, Claude 등)의 파일 업로드를 제어할 수 있다	☐	☐	☐
8	로컬 AI 또는 개발자 AI 도구의 LLM 통신을 중앙에서 제어할 수 있다	☐	☐	☐

03 영역 3. 민감정보 유출 방지

#	점검 항목	예	아니오	모름
9	AI 서비스에 입력되는 프롬프트 내 민감정보(개인정보, 사내 기밀 등)를 탐지할 수 있다	☐	☐	☐
10	Prompt Injection, Jailbreak 등 AI 악용 시도를 탐지·차단할 수 있다	☐	☐	☐
11	AI 관련 DLP 정책이 기존 데이터 보안 정책과 연계되어 있다	☐	☐	☐
12	AI를 통한 민감정보 유출 발생 시 담당자에게 즉시 알림이 전달된다	☐	☐	☐

04 영역 4. 모니터링 및 대응

#	점검 항목	예	아니오	모름
13	AI 사용 관련 위반 이벤트 리포트를 정기적으로 생성·검토하고 있다	☐	☐	☐
14	AI 보안 사고 발생 시 대응 절차 (플레이북)가 마련되어 있다	☐	☐	☐
15	경영진 또는 감사 요청 시 AI 사용 현황을 즉시 보고할 수 있다	☐	☐	☐

결과 해석

응답 패턴	진단 결과
✓ “예” 12개 이상	AI 보안 관리 체계가 잘 갖춰진 편입니다. 고도화 방안을 검토할 시점입니다.
⦿ “예” 7~11개	일부 영역에 공백이 있습니다. 우선순위를 정해 단계적 보완이 필요합니다.
! “예” 6개 이하	AI 사용 환경 전반에 걸쳐 보안 가시성과 통제 체계 구축이 시급합니다.
? “모름” 5개 이상	현황 파악 자체가 되어 있지 않은 상태입니다. 즉각적인 점검이 필요합니다.



AI 보안 현황 점검이 필요하신가요?

체크리스트 결과를 기반으로 맞춤형 진단을 받아보세요.



AI 보안 진단 요청하기 →