# 이 AI, 계약 전에 이것부터 확인하세요

## 민간 클라우드 생성형 AI 도입 시 공직자·담당자가 알아야 할 보안 행동 가이드

국가정보원 AI보안 가이드북 및 보안성 검토 실시간 지침 반영

배포처: (주)스캐터엑스 대표이사 강명수 | 총괄기획: 최규호 본부장 | 배포일자: 2026년 10월 29일

# 목차


CH.1 이 AI, 도대체 뭔가요? 슬라이드 1~5

CH.2 이 AI, 어디까지 믿어도 되나요? 슬라이드 6~11

CH.3 절대 넣으면 안 되는 것들 슬라이드 12~21
★ 가장 중요한 챕터

CH.4 시스템이 어떻게 처리하나요? 슬라이드 22~30

CH.5 문제가 생겼을 때 어떻게 하나요? 슬라이드 31~35

# 지자체마다 AI를 도입하는데, 업체가 너무 많습니다

## 현실 설명

- API 연동으로 서비스를 만드는 업체가 난립해 있습니다.
- 도입 기관이 보안을 검증하기 어렵습니다.
- 그래서 국정원이 광역·기초·공기업·공공기관 도입 시 전수 보안성 검토를 합니다.
- 검토 때마다 새로운 지침이 발행됩니다.
- 이 가이드는 그 지침을 모두 담았습니다.

## 강조 메시지



**이 가이드를 읽으면
어떤 업체의 AI를 도입하든
무엇을 요구하고
무엇을 조심해야 하는지
알 수 있습니다.**

## 🔍 업체에 반드시 확인하세요

① 국정원 보안성 검토를 통과했나요? ② 공공 클라우드(NHN·KT·네이버) 인프라를 사용하나요? ③ CSAP 인증이 있나요?

# 이 AI는 내부 시스템과 연결되지 않습니다

## ✅ SaaS가 연결되는 것

- ✅ 인터넷 공개자료
- ✅ 법령·조례·고시
- ✅ 정부·지자체 누리집
- ✅ 공개 통계·보고서
- ✅ 사용자가 직접 올린 허용 파일



연결 불가

## 🔴 SaaS가 연결되지 않는 것

- 새올행정시스템
- 전자결재
- 민원시스템
- 인사·재정·회계시스템
- 기록관리시스템
- 내부 데이터베이스

**내부망 자료가 필요하면 SaaS가 아닌 구축형 사업으로 가야 합니다.**

## 🔍 업체에 반드시 확인하세요

① 내부망에 연결하지 않는다는 것을 문서로 확인해 주세요.

② SaaS와 구축형이 명확히 분리되어 있나요?

③ 내부 시스템 연계가 필요하면 구축형으로 안내하나요?

# 딱 한 줄만 기억하세요

"
**승인된 AI에,
허용된 정보만,
내가 책임지고**

국정원은 AI 사용을 금지하는 것이 아니라 통제하는 방향입니다.

🔍 **업체에 반드시 확인하세요**

① 기관이 허용한 정보 범위를 문서로 제공하나요? ② 보안정책 변경 시 기관에 사전 통보하나요?

# AI는 검색엔진이 아닙니다

## 검색엔진

있는 자료를 찾아서 보여줍니다

→ 없으면 '결과 없음'

## 생성형 AI

없는 것도 그럴듯하게 만들어냅니다

→ 없어도 그럴듯한 답변 생성

⚠ 법령·날짜·통계·판례는 특히 위험합니다.
반드시 원문을 직접 확인하세요.

🔍 업체에 반드시 확인하세요

① 외부 AI 서버에 바로 보내지 않고 공식 자료를 먼저 검색하는 구조인가요?
② 법령·조례·고시·통계를 우선 검색하는 기능이 있나요?

# 자신 있게 말해도 틀릴 수 있습니다

⚠️

## 자신감 있는 표현 ≠ 정확한 정보

- 🔴 존재하지 않는 법령조문을 사실처럼 답할 수 있습니다.
- 🔴 틀린 날짜·기간·금액을 정확한 것처럼 답할 수 있습니다.
- 🔴 없는 판례·통계를 실제처럼 인용할 수 있습니다.
- 🔴 기관명·사업명을 잘못 연결할 수 있습니다.

**AI 답변은 참고자료입니다. 공식 원문이 기준입니다.**

🔍 **업체에 반드시 확인하세요**

① 답변에 출처와 원문 링크를 함께 제공하나요?
② 자료를 못 찾으면 추정하지 않고 '못 찾았다'고 알려주나요?

# 출처를 알려줘도 직접 확인해야 합니다

⚠️ **AI는 없는 출처를 만들 수 있습니다.**
출처가 있어 보여도 실제로 없는 문서일 수 있습니다.

## 출처를 받으면 반드시 확인하세요:

- ☐ 출처가 실제로 존재하는지
- ☐ 공식 기관이 발행한 자료인지
- ☐ 원문 링크가 실제로 연결되는지
- ☐ 기준일·발행일이 언제인지
- ☐ 인용 내용이 원문과 일치하는지
- ☐ 정정·변경·폐지 자료가 있는지

## 🔍 업체에 반드시 확인하세요

① 출처 정보에 작성기관·게시일·원문 주소를 함께 제공하나요? ② 정정·변경·취소 공고도 연결해서 보여주나요?

# AI에게 맡기면 안 되는 업무 8가지

| | | | |
|---|---|---|---|
| ⭕ 행정처분 | ⭕ 복지대상 선정 | ⭕ 세금·부담금 결정 | ⭕ 채용·인사·징계 |
| ⭕ 계약·입찰 평가 | ⭕ 감사 결과 | ⭕ 민원 최종 법적 판단 | ⭕ 의료·안전·재난 결정 |

✅ **AI는 초안 작성과 자료 검색을 도울 뿐입니다.**
최종 판단은 반드시 담당 공직자가 합니다.

🔍 **업체에 반드시 확인하세요**

① 이런 업무에 AI 단독 판단을 금지하는 정책이 있나요? ② 공직자가 반드시 검토·승인해야 하는 절차가 설계되어 있나요?

# AI 답변은 이렇게 검증하세요

| 자료 유형 | 반드시 확인할 것 |
|---|---|
| 법령 | 명칭·조문번호·시행일·개정이력·예외규정 |
| 조례 | 해당 지자체·현행 여부·최근 개정·상위법 근거 |
| 판례 | 법원명·사건번호·선고일·현재 법령과의 관계 |
| 고시·공고 | 공고번호·시행일·정정·취소 여부·최신 첨부파일 |
| 통계 | 기준연도·단위·잠정치 여부·작성기관 |
| 보고서 | 발행기관·발행연도·연구방법·한계 |

🔍 **업체에 반드시 확인하세요**

① 답변 검증을 위한 원문 바로가기 기능이 있나요? ② 현행 법령 여부를 자동으로 표시하나요?

# 최종 책임은 AI가 아닌 나에게 있습니다

**'AI는 초안을 도울 뿐입니다.'**
**검토하고 결재한 공직자가 최종 책임을 집니다.**

## 🔴 하면 안 되는 것

- AI 답변을 그대로 민원 답변으로 발송
- AI가 작성한 보고서를 검토 없이 결재 상신
- AI 계산 결과를 확인 없이 예산 서류에 기재

## ✅ 해야 하는 것

- AI 초안을 바탕으로 원문 직접 확인
- 수치·출처·법령 조문 재검토 후 활용
- 담당자 검토·승인 후 최종 문서 작성

## 🔍 업체에 반드시 확인하세요

① 이 원칙이 서비스 이용약관과 계약서에 명시되어 있나요?

# 기관 승인 AI라도 뭐든 넣으면 안 됩니다

❌ **많은 분들이 이렇게 오해합니다:**
'기관이 승인한 AI니까 업무자료 다 넣어도 되겠지?'

✅ **정확한 기준은 이것입니다:**

**서비스 승인 ≠ 모든 자료 입력 허용**

**넣기 전에 이것을 각각 따져야 합니다:**

- ☐ 공개 또는 비공개 자료인가?
- ☐ 개인정보가 포함되어 있는가?
- ☐ 비밀·보안등급이 있는가?
- ☐ 기관이 입력을 허용한 자료인가?
- ☐ 외부 AI 서버로 전송이 허용되는가?

🔍 **업체에 반드시 확인하세요**

① 입력가능한 정보 범위를 기관별로 문서화해서 제공하나요? ② 기관이 허용 범위를 직접 설정할 수 있나요?

# 절대 넣으면 안 되는 정보 11가지

- 국가기밀·비밀자료
- 주민번호 등 고유식별정보
- 민원인 개인정보
- 건강·복지·장애정보
- 인사·감사·징계자료
- 공개 전 정책자료
- 비공개 입찰·계약정보
- 시설·시스템 취약정보
- 비밀번호·시스템 접근키
- 데이터베이스 접속정보
- 비공개 안보·보안정보

**이 중 하나라도 해당되면 입력하지 마세요.**

🔍 **업체에 반드시 확인하세요**

① 이 11가지를 자동으로 탐지·차단하는 기능이 있나요? ② 기관이 자체 금지 항목을 추가 등록할 수 있나요?

# 이름만 지우면 괜찮지 않나요?

❌ '이름만 지우면 개인정보가 아니겠지?'

⚠️ 이름이 없어도 이것들이 결합되면 특정인을 알아볼 수 있습니다:

지역 + 날짜 + 사건 + 가족관계 + 직위 + 질환 = 특정인 식별 가능

예시 (가상):

'○○구 거주 / 40대 / 교통사고 / 배우자 공무원 / 2024년 3월'

→ 이름 없어도 특정인 식별 가능

✅ 이름뿐 아니라 조합으로 특정될 수 있는 모든 정보를 제거해야 합니다.

🔍 업체에 반드시 확인하세요

① 단일 항목뿐 아니라 조합으로 개인이 특정될 수 있는지 문맥으로 판단하는 기능이 있나요?

# 민원 내용을 AI에 넣어도 될까요?

🔴 **원칙: 민원 내용은 입력하지 않습니다.**
민원 내용 자체로 개인이나 사건을 식별할 수 있습니다.

**이름을 지웠어도 이것이 남아 있으면 안 됩니다:**

- ⚠️ 지역·동네 정보
- ⚠️ 날짜·기간
- ⚠️ 구체적 사건 내용
- ⚠️ 가족관계·직업
- ⚠️ 질환·장애 정보
- ⚠️ 사업장·건물명

✅ **민원 답변 초안이 필요**하다면
개인 식별 정보를 모두 제거하거나
기관의 허용 절차를 먼저 확인하세요.

🔍 **업체에 반드시 확인하세요**

① 민원 관련 입력에 대한 별도 처리 정책이 있나요? ② 민감 민원 내용 입력 시 추가 경고 기능이 있나요?

# 공개된 정보면 다 써도 되나요?

## 🔴 공개 ≠ 자유 사용

**공개 정보라도 이것을 확인해야 합니다:**

- ⚠️ 개인정보가 포함되어 있는가?
- ⚠️ 저작권이 있는가?
- ⚠️ 이용약관에 제한이 있는가?
- ⚠️ 대량수집이 금지되어 있는가?
- ⚠️ 목적 외 이용이 제한되는가?
- ⚠️ 최신 자료인가?

✅ **공개 법령·조례·고시·공공 통계**는 활용 가능합니다.
단, 위 항목을 먼저 확인하세요.

🔍 **업체에 반드시 확인하세요**
① 공개정보 이용 기준과 제한 사항을 안내 자료로 제공하나요?

# 파일 올리기 전 반드시 확인하세요

⚠️ 화면에 보이지 않아도 AI는 읽습니다.

**파일 업로드 전 5초 확인:**

- ☐ 숨김 시트·숨김 행·숨김 열이 있는가?
- ☐ 주석·메모·변경이력이 있는가?
- ☐ 작성자·기관명 등 메타데이터가 있는가?
- ☐ 이미지 속 글자(주민번호·서명 등)가 있는가?
- ☐ 비밀번호·시스템 접근키가 있는가?
- ☐ 표 안의 표에 민감정보가 있는가?
- ☐ 내부 파일경로·링크가 있는가?

**하나라도 있으면 제거 후 업로드하세요.**

🔍 **업체에 반드시 확인하세요**

① 파일의 숨김시트·주석·메타데이터·OCR까지 자동 검사하나요?
② 검사 결과를 업로드 전에 사용자에게 알려주나요?

# 개인 ChatGPT·Gemini는 업무에 쓰면 안 됩니다

🔴 기관이 데이터 처리를 통제할 수 없습니다.

🔴 계정 탈취 시 기관이 조사 자체를 할 수 없습니다.

🔴 파일 업로드·사용기록을 기관이 확인할 수 없습니다.

🔴 국정원 지침 위반입니다.

## 기관이 승인한 AI만 사용하세요.

🔍 업체에 반드시 확인하세요

① 기관 승인 외 AI 사용을 차단하는 정책이 있나요?
② 이 금지 원칙이 사용자 교육 자료에 포함되어 있나요?

# 비밀번호를 실수로 입력했다면?

| | | |
|---|---|---|
| 1단계 | 즉시 폐기 | 해당 비밀번호·키·토큰을 즉시 사용 중단 |
| 2단계 | 새 정보로 교체 | 새 비밀번호·키로 즉시 교체 |
| 3단계 | 보안담당자 신고 | 기관 보안담당 부서에 즉시 알림 |
| 4단계 | 접속기록 확인 | 관련 계정 접속이력 조회 |
| 5단계 | 이상접속 점검 | 비정상 접속 여부 최종 확인 |

**대화에서 삭제하는 것만으로는 충분하지 않습니다.**

🔍 **업체에 반드시 확인하세요**

① 비밀번호·시스템 접근키 패턴을 자동 탐지해서 즉시 차단하나요?
② 탐지 즉시 관리자에게 자동 알림이 가나요?

# AI가 '자료 없음'이라고 해도 그대로 믿으면 안 됩니다

⚠️ '없다'는 답변 = 실제로 없는 것이 아닐 수 있습니다.

## AI가 못 찾는 이유가 있습니다:

- 검색 범위가 제한되어 있을 수 있습니다.
- 자료가 비공개로 전환됐을 수 있습니다.
- 메타데이터가 누락되어 있을 수 있습니다.
- 원문 접근이 제한되어 있을 수 있습니다.
- 검색 시점에 아직 갱신이 안 됐을 수 있습니다.

✅ AI가 '없다'고 해도 담당기관에 직접 문의하세요.
✅ 원문 게시판을 직접 확인하세요.

🔍 **업체에 반드시 확인하세요**

① 자료를 찾지 못했을 때 검색한 범위와 한계를 명확히 알려주나요?
② 추가로 확인할 기관·경로를 함께 안내하나요?

# 차단됐을 때 표현 바꿔 다시 넣으면 안 됩니다

## 🔴 이것도 모두 우회입니다 — 모두 정책 위반입니다:

- 글자를 나누어 입력 (주민 / 번호)
- 유사문자로 변경 (0 → O, 1 → l)
- 금지정보를 이미지로 변환해서 업로드
- 여러 질문으로 나누어 입력
- 개인 AI 계정으로 재시도
- 다른 외부 AI에 입력

## ✅ 차단됐을 때 올바른 절차:

| | | |
|---|---|---|
| 잘못 차단된 것 같다면 | → | 기관 관리자에게 오탐 신고 |
| 업무상 꼭 필요하다면 | → | 정식 정책 검토·승인 요청 |

## 🔍 업체에 반드시 확인하세요

① 우회 시도를 탐지하는 기능이 있나요? ② 우회 시도가 감사 기록에 남나요?

# 내가 질문하면 어떻게 처리되나요?

① 기관 인증 (SSO + 다중인증)
▼
② 질문·파일 입력 + 패턴 감지 검사 (필수)
▼
③ 공공·행정 자료 우선 검색
▼
④ 자료 특성별 검색
▼
⑤ 메타데이터 검색 (게시물·첨부파일 위치 확인)
▼
⑥ 공식 원문·첨부파일 확인

⑦ 최소 정보 구성
▼
⑧ 문맥 판단 검사 최종 판정 (권고)
▼
⑨ 사전 검증된 AI 호출
▼
⑩ 출처 포함 답변 제공
▼
⑪ 공직자 원문 직접 확인 ← 가장 중요 ★
▼
⑫ 파일 원본 즉시 삭제 / 감사로그 1년 보존

🔍 **업체에 반드시 확인하세요**

① 이 처리 흐름 전체를 문서로 제공하나요? ② 각 단계별 보안 통제가 실제로 적용되고 있음을 입증할 수 있나요?

# 공식 자료를 먼저 찾는 이유

**행정 업무에서는 답변의 자연스러움보다
근거와 책임성이 중요합니다.**

## 이것들을 먼저 찾습니다:

- 법률·시행령·시행규칙·조례·규칙·훈령·예규·고시·공고
- 대법원·헌법재판소·행정심판 판례
- 정부·지자체·의회 누리집 자료
- 통계청·나라장터·공공데이터포털
- 정부출연연구기관·지자체 연구원 보고서

✅ 없는 자료를 AI가 만들어내는 것을 방지합니다.
✅ 감사와 보고의 근거를 확보합니다.
✅ 특정 외산 AI나 단일 기업에 의존하지 않습니다.

🔍 **업체에 반드시 확인하세요**
① 어떤 공공 데이터를 우선 검색하는지 목록을 제공하나요? ② 특정 외부 기업 API에만 의존하지 않나요?

# 1차 보호: 패턴 감지 장치

✅ 필수 적용 사항

정해진 형식·단어·문장을 찾아 차단합니다.
실수가 없는 패턴 감지로 1차 차단을 진행하는 것이 가장 중요합니다.

## 탐지 대상:

- 주민번호·전화번호·계좌번호·여권번호
- 비밀번호·시스템 접근키·데이터베이스 접속정보
- 기관 고유 코드·비공개 사업명
- 기관이 직접 등록한 단어·문장·패턴

## 탐지 범위:

- 파일 본문 / 메타데이터 / 이미지 OCR
- 숨김 시트·숨김 행·열 / 주석·메모 / 표 안의 표

**패턴 감지 장치는 선택이 아니라 필수입니다.**

## 🔍 업체에 반드시 확인하세요

① 패턴 감지 장치가 반드시 적용되어 있나요?
② 기관이 자체 금지어·패턴을 직접 등록할 수 있나요?
③ 등록한 패턴이 다른 기관에 노출되지 않나요?
④ 파일 OCR·숨김시트·메타데이터까지 검사하나요?

# 2차 보호: 문맥 판단 장치

🟡 권고 사항

개별 문장에는 개인정보가 없어도
여러 문장을 결합하면 특정인·사업·정책을 알아볼 수 있습니다.
이를 의미와 문맥으로 판단하는 것이 문맥 판단 장치입니다.

**외부 AI 서버로 전송하기 직전에 최종 판단합니다:**

- 질문의 민감성
- 검색된 원문의 민감성
- 결합했을 때 특정인·사업 식별 가능성
- 기관 보안정책 일치 여부

**🔴 중요: 문맥 판단 장치에 모든 것을 의존할 수 없습니다.**

패턴 감지 장치가 기본이고,
문맥 판단 장치는 추가 안전장치입니다.
DLP가 허용했다고 완전히 안전한 것이 아닙니다.

**🔍 업체에 반드시 확인하세요**

❶ 문맥 판단 장치가 적용되어 있나요? (권고 사항) ❷ 패턴 감지 + 문맥 판단 2단계가 이중으로 작동하나요? ❸ 판정 결과가 감사 기록에 남나요?

# 시스템이 있어도 내가 먼저 지켜야 합니다

⚠️ 자동 감지 장치도 잘못 막거나 못 잡는 경우가 있습니다.
시스템은 보조 수단입니다.

### 🔴 잘못 막는 경우 (오탐)

실제로 문제없는 내용을
차단하는 경우

### 🔴 못 잡는 경우 (미탐)

문제 있는 내용을
통과시키는 경우

**시스템이 허용했다고 해서 완전히 안전한 것이 아닙니다.**
**공직자가 입력 기준을 먼저 지키는 것이 핵심입니다.**

🔍 **업체에 반드시 확인하세요**

① 오탐 발생 시 기관 관리자가 검토·수정 요청할 수 있나요? ② 미탐 가능성을 사용자에게 고지하고 있나요?

# 내 파일 원본이 외부로 나가나요?




✅ 파일 원본은 외부 AI 서버에 직접 전송되지 않습니다.

✅ 파일은 처리 후 즉시 삭제됩니다.

🔍 **업체에 반드시 확인하세요**

① 파일 원본이 외부 AI 서버로 전송되지 않는다는 것을 계약서에 명시할 수 있나요?

② 즉시 삭제 처리를 기술적으로 어떻게 보장하나요?

# 외부 AI 서버가 내 데이터를 학습에 쓰나요?

⚠️ **학습 금지 계약 ≠ 보관 안 함**
이 두 가지는 다른 문제입니다.

| 구분 | 내용 |
|---|---|
| 학습 금지 | 계약서에 명시 가능 / 반드시 확인 필요 |
| 데이터 보관 | 공급자·계약·설정에 따라 기간이 다름 |
| 신규 모델 도입 | 별도 검증·승인 절차 필요 |

🔴 **반드시 계약서에서 확인하세요:**
- 학습 사용 금지 명시 여부
- 외부 AI 서버의 데이터 보관기간
- 신규 모델 도입 시 재검증 절차

🔍 **업체에 반드시 확인하세요**
1. 외부 AI 서버의 학습 사용 금지가 계약서에 명시되어 있나요?
2. 외부 AI 서버의 데이터 보관기간을 확인할 수 있나요?
3. 신규 모델 도입 시 별도 검증·승인 절차가 있나요?

# 내 대화 기록은 얼마나 남나요?

| 데이터 유형 | 처리 방식 | 기간 |
|---|---|---|
| 업로드 파일 원본 | 처리 후 즉시 삭제 | 즉시 |
| 세션용 임베딩 | 세션 종료 후 삭제 | 최대 24시간 |
| 캐시·임시데이터 | 처리 종료 후 폐기 | 즉시 |
| 감사 로그 | 별도 보존 후 삭제 | 1년 |
| 공식 지식베이스 | 승인된 정책으로 관리 | 별도 정책 |

⚠️ 관리자가 대화를 열람할 때는 기록이 남습니다.
⚠️ 이름은 마스킹 처리됩니다. (예: 김OO, 박OO)

🔍 **업체에 반드시 확인하세요**

① 데이터 유형별 보존·삭제 정책을 문서로 제공하나요?
② 계약 종료 시 데이터 반환·삭제 확인 절차가 있나요?
③ 관리자 열람 시 기록이 남나요?

# 기관별 데이터는 완전히 분리되나요?

다른 기관의 자료가 내 화면에 나타나면 안 됩니다.
기관별로 계정·정책·데이터·로그·접근권한이 모두 분리되어야 합니다.

## 분리되어야 하는 것:

- ☐ 사용자 인증
- ☐ 애플리케이션·컨테이너
- ☐ 네트워크 정책
- ☐ 데이터 저장 영역
- ☐ 감사 로그 접근권한
- ☐ 외부 AI 모델 정책

## ⚠ 이것도 반드시 분리해야 합니다:

공직자용 / 대민서비스용 / 의회의원용

## 🔍 업체에 반드시 확인하세요

① 기관별 계정·정책·데이터·로그가 완전히 분리되나요?
② 공직자용·대민용·의회용 서비스가 분리 운영되나요?
③ 컨테이너뿐 아니라 인증·네트워크·저장소·로그도 함께 분리하나요?

# 보안 사고가 의심될 때 즉시 할 일

## 🛑 중단

복사·공유·반복조회 즉시 중단 화면 그대로 두기

▼

## 📞 신고

기관 보안담당자에게 즉시 연락 혼자 해결하려 하지 말 것

▼

## 📋 기록

발생 시각·화면·사용 기능·모델 보존 기관 절차에 따라 증적 확보

**🔍 업체에 반드시 확인하세요**

① 보안사고 발생 시 기관에 즉시 통보하는 절차가 있나요? ② 사고 조사를 위한 자료 제출 의무가 계약서에 있나요?

# 전보·퇴직·휴직 시 반드시 해야 할 것

⚠ 퇴직·전보 후에도 계정이 살아있으면
기관 전체 데이터가 위험해집니다.

| 상황 | 즉시 해야 할 것 |
|---|---|
| 전보 | 기존 계정 접근권한 변경·회수 |
| 퇴직 | 계정 즉시 비활성화·회수 |
| 휴직 | 기간 중 계정 일시 정지 |
| 승진 | 새 권한 범위 재설정 |
| 겸직 | 겸직 업무 범위만 권한 부여 |

⚠ 직급이 높아도 담당 업무 외 자료에는 접근할 수 없습니다.

⚠ 관리자 계정은 다중인증을 반드시 적용해야 합니다.

🔍 업체에 반드시 확인하세요

① 전보·퇴직·휴직 시 계정 즉시 회수 절차가 계약서에 명시되어 있나요?
② 관리자 계정에 다중인증이 적용되나요?
③ 계정별 접근 권한 변경 이력이 감사 기록에 남나요?

# 관리자가 먼저 정해야 할 것들

**도입 전에 반드시 결정해야 합니다.**
**정하지 않으면 공직자가 기준 없이 사용하게 됩니다.**

- ☐ 허용 업무와 금지 업무
- ☐ 입력 가능한 정보 범위
- ☐ 외부 AI 서버로 전송 가능한 정보
- ☐ 기관명·부서명 처리방식
  (포함 / 마스킹 / 일반화 / 제거)
- ☐ 허용 AI 모델 목록
- ☐ 기관 고유 금지어·패턴 등록
- ☐ 로그 열람 권한자와 절차
- ☐ 보안사고 신고 절차와 연락처
- ☐ 신규 모델 도입 시 재검증 절차
- ☐ 패턴 변경 시 승인·기록 절차

🔴 **이 항목들을 정하지 않고 서비스를 오픈하면 안 됩니다.**

🔍 **업체에 반드시 확인하세요**

① 기관 관리자가 이 항목들을 직접 설정할 수 있는 관리 화면이 있나요?
② 설정 변경 이력이 감사 기록에 남나요?
③ 국정원 추가 지침 발생 시 기관에 이행 의무가 계약서에 있나요?

# 해도 되는 것 vs. 하면 안 되는 것

## ✅ 해도 됩니다

- ✅ 공개 법령·조례·고시·판례 검색
- ✅ 보고서·민원 답변 초안 작성 (원문 확인 후 활용)
- ✅ 공개 통계·연구보고서 활용
- ✅ 업무 절차·기준 안내 요청
- ✅ 여러 공식자료 비교·요약 요청
- ✅ 공개 고시·공고 내용 확인
- ✅ 출처 확인 후 보고서에 인용
- ✅ 기관이 허용한 자료 파일 업로드 (숨김정보 확인 후)

## 🔴 하면 안 됩니다

- 🔴 주민번호·민원인 정보 입력
- 🔴 비밀번호·시스템 접근키 입력
- 🔴 비공개 내부 자료 복사해서 넣기
- 🔴 개인 ChatGPT로 업무 처리
- 🔴 차단됐을 때 우회 시도
- 🔴 파일 메타데이터 확인 없이 업로드
- 🔴 AI 답변을 그대로 결재 상신
- 🔴 AI 답변을 원문 확인 없이 민원 발송
- 🔴 공개 전 정책자료·인사자료 입력

## 🔍 업체에 반드시 확인하세요

① 이 두 컬럼 기준이 계약서와 이용정책에 명시되어 있나요? ② 사용자 교육 자료로 제공하나요?

# 계약서에 이것이 없으면 서명하지 마세요

## 🔴 반드시 계약서에 들어가야 할 6가지

① 데이터 학습 사용 금지 명시

② 계약 종료 후 데이터 반환·삭제 확인 절차

③ 보안사고 발생 시 기관 즉시 통보 의무

④ 국정원 추가 지침 발생 시 이행 의무

⑤ 감사 요청 시 자료 제출 의무

⑥ 외부 AI 서버 변경 시 사전 통보 의무

## 📋 공직자 10계명

① 승인된 AI만 사용한다
② 개인 계정으로 업무 처리 안 한다
③ 공식 자료를 먼저 확인한다
④ 내부망 자료를 외부 AI에 넣지 않는다
⑤ 개인정보·비밀번호를 넣지 않는다
⑥ 파일 올리기 전 숨김정보를 확인한다
⑦ 차단되면 우회하지 않는다
⑧ AI 답변 출처·현행성을 직접 확인한다
⑨ 이상 상황은 즉시 신고한다
⑩ 내부 시스템 연계는 구축형으로 간다

## 📞 문의처

- 기관 정보보안 담당부서
- 국가사이버안보센터 (국가정보원 산하)
- 국정원 AI보안 가이드북 (국가사이버안보센터 누리집)
- 개인정보보호위원회 (개인정보 관련 문의)

본 가이드는 국가정보원 AI보안 가이드북 및 보안성 검토 실시간 지침을 반영합니다.
기관별 보안담당 부서의 안내를 우선 적용하십시오.

## 🔍 업체에 반드시 확인하세요

① 이 두 컬럼 기준이 계약서와 이용정책에 명시되어 있나요?

② 사용자 교육 자료로 제공하나요?