첨부 5

책임 있는 AI 사용 카드

AI 활용 사례 공모전 시즌3 · 업무 생산성 개선
회사·인명·수치·성분·금액은 모두 가렸습니다

고객의 기밀과, 고객이 다른 회사에서 받은 자료를 지키면서 AI를 계속 쓰기 위한 기준입니다. 처음부터 지켜 온 방식을 일하는 도중(10월 중순)에 문서로 정리했습니다. **이번 일에서 실제로 한 것**과 **앞으로 쓸 방법**을 나눠 적습니다.

1. 자료를 세 등급으로 나눕니다

등급	예	AI에 넣어도 되는 범위
A. 공개·대외용	브로셔, 초대 메일, 공개 회사 소개, 전시회 자료, 업계 공개 정보	제한 없음
B. 고객 내부 자료	미공개 투자 설명 자료, 고객과의 메일, 시험 성적서, 정산, 미팅 메모	학습 허용을 끈 환경에서, 그 업무에 필요한 부분만. 고객에게 AI 사용을 미리 알림(계약 조항)
C. 핵심·제3자 기밀	상대 기업에서 비밀유지계약으로 받은 자료, 소재 성분·배합·공정, 미공개 특허 원문	**원칙: 넣지 않음.** 예외는 아래 2의 두 가지뿐이며, 둘은 조건이 다름

애매하면 한 단계 높은 등급으로 취급합니다. 웹 검색어에는 고객 정보를 넣지 않습니다. 다른 AI에 넘기는 문서도 같은 기준을 지킵니다.

2. C등급의 예외 — 가리기와 동의는 다릅니다

- **가리기**: 먼저 그 문서 자체의 비밀유지 조건과 AI 처리 허용 범위를 확인. 회사명·수치·물질명 같은 식별정보를 [A사] [수치1]로 바꾼 뒤에도 **기밀이 남지 않는 경우에만** 넣고, 결과에서 되돌림. 원문은 넣지 않음
- **동의** (가려도 기밀이 남는 문서, 예: 기술 문서): 자료 주인(상대 기업 자료면 상대방까지)의 **서면 동의**와, 학습·보관 조건이 계약으로 정해진 업무용 환경이 둘 다 있을 때만
- 둘 다 아니면 **사람만** 처리. 가린 문서로 만든 용어집·번역 메모리는 PC 안 번역 프로그램에서 사용

이번 일에서 실제로 한 것
소재 성분 같은 핵심 기밀은 처음부터 받지 않았고 AI에도 넣지 않았습니다. AI에 외부 조사를 맡긴 작업지시서에는 「고객사 이름과 소재 성분·기술 세부는 검색어에도 문서에도 넣지 않는다」를 원칙으로 적었습니다.

3. 설정

- 사용한 AI 모두 「대화를 학습에 사용」 설정을 끔(10월 중순 확인)
- 설정과 약관은 바뀔 수 있어 정기적으로 다시 점검

4. 판단과 책임은 사람에게

- AI 초안은 사람이 문장마다 검수하고 사람이 보냄
- AI 초안을 고친 곳과 이유는 따로 기록(첨부 3)
- 무거운 질문은 두 AI에 따로 묻고 사람이 통합
- 위험은 판정하지 않고, 확인할 전문가에게 연결

5. 사실대로 말하기

- 미팅은 「확정」과 「조율 중」을 구분
- 계약·매출로 이어졌다고 쓰지 않음(진행 중)
- 같은 조건으로 재지 않은 시간 절감률은 쓰지 않음
- 나중에 떠올려 적은 시간 기록은 [추정]으로 표시

6. 상대를 존중하기

- 웹 문의 폼에 영업 연락을 받지 않는다고 밝힌 회사에는 보내지 않았습니다.
- 후속 메일에는 공개용 자료만 붙였고, 경쟁 가능성이 있는 곳에는 그마저 붙이지 않았습니다.
- 이 출품물에서는 고객사와 상대 기업의 이름, 인명, 시험 수치, 소재 성분, 금액을 모두 가렸습니다.

고객과 맺을 계약서에 넣을 AI 조항(안)
「업무 효율을 위해 생성형 AI 도구를 사용할 수 있습니다. 입력 내용이 학습에 사용되지 않도록 설정된 환경에서 사용하며, 귀사가 제3자로부터 비밀유지 조건으로 받은 자료와 귀사가 지정한 핵심 기밀은 사전 동의 없이 AI 도구에 입력하지 않습니다.」 — 법률 검토 전 초안

이 글과 첨부의 초안 작성에도 Claude를 썼고, 내용 확인과 최종 문장은 출품자가 했습니다.