랩 위드의 기술사업화 인사이트

2026.10.07 (수) | 오늘의 주제

[AI 활용 기초 시리즈 ⑦편] 우리 회사 자료, 이 워크플로우에 안전하게 연결하는 법 _ 기밀·보안 기초

1. 오늘의 기술사업화 뉴스

- (정책 동향) 한성숙 국무총리가 10 월 6 일 '금융·공공기관 개인정보 유출 대응 관계장관회의'를 주재하고, 보안 점검을 전 금융권으로 신속히 확대하라고 지시했습니다. 정부·공공기관이 운영하지 않거나 방치한 웹사이트는 서버와 데이터가 남아 있으면 공격 통로가 될 수 있다며 폐쇄하도록 했고, 금융·의료·교육 등 분야별로 나뉜 정보보안 체계도 재검토하기로 했습니다. *〈출처: 아이뉴스 24·한국사회복지저널, 2026.10.06〉*
- (정책 동향) 산업통상부가 국정감사 지적을 반영해 '제 6 차 산업기술보호 종합대책'을 마련하기로 했습니다. 기술유출 범죄수익의 몰수 대상을 넓히고 피해기업이 기술개발에 들인 비용을 손해액으로 인정하는 방안을 추진하며, 기술유출에 취약한 중소기업·대학의 보안 역량을 높이기 위해 보안설비 구축·컨설팅 지원도 확대합니다. *〈출처: 서울파이낸스·베타뉴스, 2026.10.07〉*
- (AI 산업 동향) 보안기업 로그프레소가 기업의 생성형 AI 사용 기록을 기존 보안 로그와 함께 분석하는 '챗 GPT 엔터프라이즈' 연동 앱을 출시했습니다. 대화 메시지·인증·관리 감사 등 로그 10 종을 모아, 고객 정보나 사내 소스코드 같은 기밀이 AI 에 입력됐는지 탐지·조사할 수 있게 했습니다. *〈출처: 디지털데일리, 2026.10.07〉*
- (투자 동향) 알테오젠이 국민성장펀드와 스카이레이크가 매칭해 만든 '스카이알트'를 대상으로 2,000 억원 규모 종류주식(전환우선주 1,000 억원·상환전환우선주 1,000 억원)을 발행해 투자를 유치합니다. 자금은 대전 신규 생산시설 건설과 신규 제품·기술 도입에 쓰입니다. *〈출처: 머니투데이 더바이오, 2026.10.06〉*
- (투자 생태계) AI 투자매칭 서비스 브이씨루트가 스타트업 소재지에 맞는 지역 의무투자 펀드를 우선 찾아 주는 기능을 선보였습니다. 10 월 1 일 기준 비수도권 13 개 시도에서 신규 투자가 가능한 지역펀드는 159 개, 결성액은 약 2 조 3,000 억원이며 부산이 35 개·7,854 억원으로 가장 많았습니다. *〈출처: 벤처스퀘어, 2026.10.06〉*
- (R&D 지원 동향) 기술보증기금과 서울대학교기술지주가 대학 기반 딥테크 스타트업 지원 업무협약을 맺었습니다. 서울대기술지주가 유망 기업을 추천하면 기보가 보증·투자 연계와 보증료 감면을 제공하고, 기술보호·임치, 컨설팅, IPO 지원까지 단계별로 연결합니다. *〈출처: 벤처스퀘어, 2026.10.06〉*

※ 오늘 뉴스 가운데 로그프레소의 사내 AI 사용 기록 분석 앱과 산업통상부의 기술유출 대응 강화는 본문에서 '우리 회사 자료를 AI 에 넣을 때 무엇을 지켜야 하는가'를 다루는 배경으로 함께 살펴봅니다.

2. 오늘의 한 조각 _ 우리 회사 자료, AI 워크플로우에 안전하게 연결하는 법

[AI 활용 기초 시리즈 ⑦편]

④~⑥편(9.28~10.2)에서는 업무를 단계로 나누고, 단계를 잇고, 사람이 확인할 지점을 정하는 법을 다뤘습니다. 오늘은 이 워크플로우에 우리 회사 자료를 넣을 때 무엇을 넣어도 되고 무엇은 넣으면 안 되는지, 기밀·보안의 기초를 정리합니다.

외부 AI 서비스에 입력한 자료는 우리 회사 컴퓨터를 떠나 서비스 회사의 서버로 전송됩니다. 서비스와 설정에 따라 대화 내용이 저장되거나 모델 개선에 쓰일 수 있고, 한 번 보낸 자료는 되돌려 받기 어렵습니다. 그래서 보안은 '조심해서 쓰자'는 다짐이 아니라, 워크플로우의 맨 앞 단계에 넣어 두는 규칙이어야 합니다.

첫째, 자료를 세 가지 등급으로 나눕니다.

국가정보원이 공공기관용으로 배포한 「챗 GPT 등 생성형 AI 활용 보안 가이드라인」(2023.6)도 비공개 업무자료와 개인정보는 입력하지 말 것을 권고합니다. 실무에서는 신호등처럼 초록·노랑·빨강 세 칸으로 나누면 판단이 빨라집니다.

등급	예시 자료	개인 계정 AI	회사가 계약한 기업용 AI	처리 방법
초록 (공개)	지원사업 공고문, 보도자료, 공개된 논문·특허	사용 가능	사용 가능	그대로 활용
노랑 (내부)	계획서 초안, 회의록, 일반 업무 문서	사용 금지	조건부 가능	회사명·인명·금액을 가린 뒤 입력
빨강 (기밀)	출원 전 핵심 기술, 소스코드, 고객·직원 개인정보, 미공개 재무자료, 보안과제 자료	사용 금지	사용 금지	외부 AI 에 넣지 않음 (회사 서버에 직접 설치해 자료가 밖으로 나가지 않는 방식만 검토)

둘째, 노랑 자료는 '가리기' 단계를 거쳐 넣습니다.

회사명은 'A 사', 사람 이름은 '담당자 1', 금액은 'X 억 원'처럼 바꾼 뒤 AI 에 넘기고, 결과를 받은 뒤 다시 원래 이름으로 되돌립니다. 바꾼 이름과 원래 이름을 짝지은 대조표는 사내에만 보관합니다.

이 가리기를 ④편에서 배운 단계 나누기에 맞춰 워크플로우의 첫 단계로 고정해 두면, 바쁜 날에도 건너뛰지 않게 됩니다. ⑥편의 검증 지점처럼, 보안도 사람의 기억이 아니라 절차에 맡겨야 지켜집니다.

셋째, 같은 AI 라도 계정과 설정에 따라 안전도가 다릅니다.

직원 개인 계정으로 업무 자료를 다루면 회사가 기록을 관리할 수 없습니다. 쓰고 있는 서비스의 설정에서 '대화 내용을 모델 학습에 활용'과 같은 항목이 꺼져 있는지, 대화 공유 링크가 외부에 공개되어 있지 않은지 확인해야 합니다.

오늘 뉴스에 소개된 로그프레소의 앱처럼, 회사가 관리하는 기업용 AI 계정의 사용 기록을 모아 기밀이 입력됐는지 확인하는 도구도 나오고 있습니다. 개인 계정을 회사 계정으로 옮겨야 이런 점검도 가능해집니다.

실제로 2023 년 국내 한 대기업에서는 직원들이 업무 편의를 위해 소스코드와 회의 내용을 외부 생성형 AI 에 입력한 사실이 알려지면서, 회사가 사내 생성형 AI 사용을 제한하고 보안 지침을 새로 만들었습니다. 규모가 작은 회사는 핵심 기술 하나가 회사 가치에서 차지하는 비중이 커서, 같은 일이 생기면 피해가 더 클 수 있습니다. 오늘 뉴스에서 산업통상부가 기술유출에 취약한 중소기업·대학의 보안 역량을 높이겠다고 한 것도, 작은 조직의 기술 보호가 정책 과제로 다뤄지고 있음을 보여줍니다.

넷째, 국가 R&D 보안과제 자료는 별도 기준을 따릅니다.

보안과제는 국가핵심기술(유출되면 국가 안보·경제에 큰 영향을 주어 법으로 보호하는 기술)을 비롯해 수출 제한 기술, 방위력 개선 관련 기술 등과 관련된 연구개발과제 가운데 지정됩니다. 지정되면 연구실을 보호구역으로 정해 출입을 관리하고, 연구 자료와 성과를 따로 보호하는 등의 보안관리 의무가 따릅니다.

수행 중인 과제가 보안과제라면 관련 자료를 외부 AI 에 넣기 전에 협약서와 기관 보안 규정부터 확인해야 합니다. 보안과제가 아니더라도 출원 전 기술이 담긴 자료는 위 표의 빨강 등급으로 다룹니다.

정리하면, 자료는 세 등급으로 나누고, 노랑은 가린 뒤에, 빨강은 넣지 않으며, 계정과 설정까지 점검하는 것이 보안 기초입니다. 10.9(금)은 한글날로 쉬고, 다음 ⑧편(10.12 월)에서는 'R&D 계획서 초안, AI 워크플로우로 잡는 법'을 주제로 ④~⑦편의 원칙을 실제 계획서 작성에 통째로 적용해 봅니다.

※ 출처: 국가정보원「챗 GPT 등 생성형 AI 활용 보안 가이드라인」(2023.06) · 「국가연구개발혁신법 시행령」 제 45 조(보안등급 분류) · 랩 위드 내부 정리 (2026.10.07)

3. 실전 체크리스트

✔ ③ 실전 체크리스트 _ 우리 회사 AI 자료 보안 점검

- 공유 폴더에서 AI 작업에 자주 쓰는 문서 열 개를 골라, 파일명 앞에 [초록]·[노랑]·[빨강] 등급을 붙여 둔다
- 우리 회사 기준 '빨강 목록'(출원 전 기술, 소스코드, 개인정보, 미공개 재무 등)을 한 장으로 정리해 전 직원에게 공유한다
- 업무에 쓰는 AI 서비스의 설정 화면을 열어 '대화 내용 학습 활용' 항목과 공유 링크 공개 여부를 확인한다
- 직원이 개인 계정으로 업무 자료를 AI 에 넣고 있는지 점검하고, 회사가 관리하는 계정으로 옮길 계획을 세운다
- 계획서·보고서 작성 워크플로우 첫 단계에 '회사명·인명·금액 가리기'를 넣고, 대조표의 보관 위치를 정한다
- 수행 중인 국가 R&D 과제의 협약서에서 보안등급을 확인하고, 보안과제라면 기관 보안담당자에게 AI 사용 가능 범위를 문의한다

4. 이번 주 마감임박 지원사업 (중앙정부 70% · 대전지역 30%)

- **[중앙]** 2026 년 납품대금 연동 우수기업 포상 모집 공고 **(~10.08)** · 중소벤처기업부
- **[중앙]** 2027 년 초격차 스타트업 프로젝트 기술사업화 및 투자유치 주관기관 모집공고 **(~10.12)** · 중소벤처기업부
- **[중앙]** 2027 년 스마트공장 구축지원사업 주관기관 모집 공고 **(~10.13)** · 중소벤처기업부
- **[중앙]**「2026 년 상생결제 확산 유공」포상 후보자 모집 공고 **(~10.13)** · 중소벤처기업부
- **[중앙]** 2026 년 성능인증(EPC) 신규신청 접수 공고(제 4 차) **(~10.14)** · 중소벤처기업부
- **[대전]** 지역디자인산업진흥사업」방위산업분야 디자인 시제품 개발(2 차) 기업 모집공고 **(~10.08)** · 대전디자인진흥원
- **[대전]** 2026 년 제 5 차 대전창업허브 및 대전소셜벤처캠퍼스 입주기업 모집 **(~10.13)** · 대전창조경제혁신센터

※ 10.08(목)~10.14(수) 마감 공고 중 중앙 5 : 대전 2 로 추렸습니다. 10.07 자 지원사업 브리핑이 아직 발행되지 않아 직전 회차인 10.06 자 데이터를 기준으로 삼았으며, 이 기간 브리핑에 실린 중앙 공고는 모두 중소벤처기업부 공고입니다. 10.09(금)는 한글날이므로 연휴 전후 마감 공고는 접수 마감 시각과 방법을 접수처에서 꼭 확인하시기 바랍니다. ※ 출처: 랩 위드 지원사업 브리핑 (2026.10.06 기준).

우리 회사 자료 중 어디까지 AI 에 넣어도 되는지 기준이 없으십니까? 자료 등급 분류부터 가리기 단계를 넣은 계획서 작성 워크플로우까지, 보안을 지키면서 AI 를 쓰는 R&D 기획 체계를 함께 설계해 드립니다.

→ 'R&D 사전기획' 컨설팅 상담

상담 신청 ☎ 010-6408-8557 | antipoto@gmail.com | cafe.naver.com/techcomwith

▶ **더 보기:** '보안 과제', 우리 기업은 해당할까? _ 혼동 줄이기 (cafe.naver.com/techcomwith/349)

▣ 랩 위드 컨설팅 솔루션 _ 사업화 전 단계를 전문가가 함께 설계합니다



랩 위드 AI R&D 전략 분석 플랫폼

"R&D 사업계획서, AI 로 구조화"

- 공고·RFP 분석 → 평가항목별 맞춤 전략 도출
- 정부 과제 DB 2,900+건·선행연구 검색
- 평가위원 관점 피드백으로 완성도 점검



IR 컨설팅 솔루션

"기업진단부터 모의 IR 까지 4STEP"

- 기업진단 → 투자전략 → IR Deck → 모의 IR
- 피치덱 10 장 구조·트랙션·Ask 설계
- 7 회차 온라인 관리로 단계별 코칭



기업진단 솔루션

"우리 회사 사업화 준비도 점수화"

- 기업정보·재무·기술개발·정성평가 종합
- 강·약점 종합 진단 리포트 자동 생성
- R&D·투자 준비 우선순위 제시

◆ 랩 위드 채널 _ 지금 바로 연결하세요

랩 위드는 매일 중앙정부·대전지역 12 개 기관 지원사업을 수집·분류해 고객사에 전달합니다. 브리핑·인사이트·AI 분석을 하나의 워크플로우로 연결 _ R&D·사업화 전략 수립 시간을 획기적으로 단축합니다.

◆ [3 기 모집] R&D 실무교육 아카데미 _ 될 때까지 지원하는 실습 교육

2026. 10.19(월)~10.20(화) | 과정별 1 일 완결 | 기술사업화 랩 위드(주) 교육장(대전 중구)

- 참가자 본인이 보유한 기술로 그날 R&D 연구계획서·PSST 사업계획서를 직접 작성하는 실습 과정입니다(R&D 과정은 본인 기술 1 건 보유 필수).
- R&D 평가위원이자 전문개인(엔젤)투자자인 대표이사가 직접 교육하고 지도합니다.
- DAY1 · 10.19(월) R&D 연구계획서 작성 실무 10:00~16:00 _ 30 만원 | DAY2 · 10.20(화) PSST 사업계획서 작성 실무 10:00~14:00 _ 25 만원
- 이어지는 기수: 4 기 11.9(월)~11.10(화)
- 날짜별 개별 신청 가능 · 각 과정 정원 4 명 선착순 마감
- TRACK B · 계획서 진단 클리닉(4 시간) _ 15 만원 ·
- 상시 접수(1~2 인은 평일 중 협의, 3 인 이상은 원하는 날짜로 별도 개설)
- 신청: 홈페이지 www.labwith.kr 실무교육 아카데미 페이지의 달력에서 원하는 날짜를 골라 신청하십시오.
- 문의: 010-6408-8557 · antipoto@gmail.com · 카카오톡 ID antipoto

기술사업화 랩 위드
Tech-Commercialization Lab WITH

기술사업화 랩 위드(주) 조남주 대표이사 · 공학박사 · 전문개인(엔젤)투자자

☎ 010-6408-8557 | antipoto@gmail.com

대전 본사 (34897) 대전광역시 중구 계백로 1615 번길 56, 진호빌딩 301 호

홈페이지: www.labwith.kr 네이버 카페: cafe.naver.com/techcomwith