

25개 항목 · 15분 셀프 진단

Microsoft Purview 민감도 레이블 운영 진단 체크리스트

라벨은 붙였는데 운영이 되고 있나요? 라벨 체계 설계부터 적용 자동화, 해제·변경 통제, DLP 연계, 감사까지 — 국내 기업 도입 사례에서 반복되는 25개 확인 항목을 점수로 진단합니다. Business Premium · E3 · E5 모두 해당됩니다.

1 라벨 체계 설계

라벨이 너무 많거나 기준이 모호하면 사용자가 아무거나 고르거나 아예 붙이지 않습니다.

- | | |
|---|----|
| ☐ 라벨이 5개 이하이고 이름만 봐도 등급을 알 수 있다 | 4점 |
| 예: 공개 · 내부 · 대외비 · 극비, 부서명 · 프로젝트명 라벨은 하위 라벨로. | |
| ☐ 각 라벨에 "어떤 문서에 붙이는지" 한 줄 기준이 문서화돼 있다 | 4점 |
| 사용자에게 보이는 라벨 설명(툴팁)에도 같은 문장이 들어가 있다. | |
| ☐ 라벨별 보호 동작(암호화 · 워터마크 · 외부 공유 제한)이 정해져 있다 | 4점 |
| "대외비인데 아무 제한 없음" 상태가 아니어야 한다. | |
| ☐ 기본(default) 라벨이 설정돼 있어 새 문서가 무라벨로 남지 않는다 | 4점 |
| ☐ 라벨 정책이 전 직원에게 게시돼 있고 게스트 · 서비스 계정 예외가 정리돼 있다 | 4점 |

2 적용 · 자동화

수동 라벨링에만 의존하면 실제 부착률은 보통 30%를 넘지 못합니다.

- | | |
|--|----|
| ☐ 라벨 부착률을 월 1회 이상 확인한다 | 4점 |
| Purview 콘텐츠 탐색기 또는 활동 탐색기 기준. | |
| ☐ 주민등록번호 · 카드번호 등 민감정보 유형에 자동 또는 권장 라벨링이 걸려 있다 | 4점 |
| E5: 자동 라벨링 정책. E3/BP: 최소한 DLP 정책으로 탐지. | |
| ☐ Teams · SharePoint 사이트 단위(컨테이너) 라벨을 쓰거나, 쓰지 않는 이유가 명확하다 | 3점 |
| ☐ 메일에도 라벨이 적용되고 외부 발송 시 동작(경고 · 차단)이 정해져 있다 | 4점 |
| ☐ PDF · 스캔 문서 · 구 버전 Office 파일에 대한 라벨 정책이 있다 | 3점 |

3 해제 · 변경 통제 — 가장 자주 비어 있는 영역

Purview는 라벨을 낮출 때 사유 입력만 요구할 뿐, 상급자 결재 단계가 없습니다. 이 영역이 비어 있으면 위 항목들이 무의미해집니다.

- | | |
|---|----|
| ☐ 사용자가 라벨을 스스로 낮출 수 있는지 여부를 라벨별로 알고 있다 | 4점 |
| "사유 입력 후 허용" 인지 "차단" 인지 라벨마다 확인. | |
| ☐ 라벨 해제 · 하향에 상급자(팀장 등) 결재 절차가 있다 | 5점 |
| 메일 · 전자결재 · 별도 도구 무엇이든, "누가 승인했는지" 남아야 한다. | |
| ☐ 결재자 부재 시 대결자(대리 승인) 규칙이 정해져 있다 | 3점 |
| ☐ 해제 요청 접수 → 처리까지 평균 소요 시간을 알고 있다 | 3점 |
| IT팀이 수동 처리한다면 보통 1~3일. 업무 병목의 신호. | |
| ☐ 해제된 문서의 외부 전달(다운로드 · 공유)에 횟수 · 기간 제한이 있다 | 3점 |

이 영역 5개 중 3개 이상 비어 있다면, 라벨 정책보다 해제 결재 체계를 먼저 세우는 것이 효과가 큼니다.

4 DLP · 접근 통제 연계

라벨은 "표시"일 뿐입니다. DLP와 조건부 액세스가 라벨을 조건으로 써야 실제 통제가 됩니다.

- | | |
|---|----|
| ☐ DLP 정책 조건에 민감도 라벨이 사용되고 있다
예: "대외비 라벨 + 외부 도메인 발송 → 차단". | 4점 |
| ☐ DLP 정책이 Exchange · SharePoint · OneDrive 세 곳 모두에 걸려 있다
E5: Teams 채팅 · 엔드포인트(USB·인쇄)까지. | 4점 |
| ☐ DLP 예외(오탐) 처리 절차와 담당자가 정해져 있다 | 3점 |
| ☐ 조건부 액세스로 관리되지 않는 기기에서의 다운로드를 제한한다
Entra ID P1(BP/E3) 이상이면 가능. | 4점 |
| ☐ 게스트 · 외부 공유 링크 정책이 라벨 등급과 연동돼 있다 | 3점 |

5 감사 · 운영

사고가 났을 때 "누가 언제 라벨을 바꿨는지" 5분 안에 답할 수 있어야 합니다.

- | | |
|---|----|
| ☐ 라벨 변경·해제 이력을 검색해서 보고서로 뽑을 수 있다
감사 로그 보존 기간(E3 180일 / E5 1년+)을 알고 있다. | 4점 |
| ☐ 월 1회 라벨·DLP 운영 리포트를 경영진 또는 보안위원회에 보고한다 | 3점 |
| ☐ 라벨 정책 변경에 대한 변경 관리(승인·기록) 절차가 있다 | 3점 |
| ☐ 신규 입사자 교육에 라벨 사용법이 포함돼 있고, 연 1회 리마인드한다 | 3점 |
| ☐ 라벨 운영 담당자(오너)가 지정돼 있고 IT 외 현업 담당도 있다 | 3점 |

점수 해석 (총 90점)

75점 이상 운영 단계. 자동화·엔드포인트 확장(E5 기능)을 검토할 때입니다.

50 ~ 74점 도입은 됐으나 통제가 비어 있는 상태. 3번(해제 통제)과 4번(DLP 연계)부터 채우세요.

49점 이하 라벨이 "표시"에 머물러 있습니다. 1번 체계 정리 → 3번 결재 체계 순으로 재설계가 필요합니다.

30분 무료 진단 — 체크리스트 결과를 보내주시면 우선순위를 정리해 드립니다

contact@ztlabs.co.kr · <https://ztlabs.co.kr>

LabelGate는 3번 영역(해제·변경 결재)을 전자결재식 조직도 결재선으로 채우는 도구입니다. SaaS 또는 온프레미스.