ZeroTrust Labs

스타터 세팅 · 45개 항목 · 직원 10~500명 기업용

Microsoft 365 스타터 세팅 체크리스트

보안 담당자가 없는 회사가 Microsoft 365를 쓰기 시작할 때, 첫 2주 안에 켜 두어야 할 45가지입니다. 추가 솔루션 구매 없이 Business Premium부터 가능한 항목이 대부분이고, E3·E5에서만 되는 것은 따로 표시했습니다. 완료 시 증적(스크린샷·설정 내보내기)을 남기면 그대로 투자사·고객사 보안 점검표와 인증 준비 자료가 됩니다.

쓰는 법 — 각 줄의 ☐에 완료 표시 → "증적" 칸에 스크린샷 파일명이나 설정 위치를 적습니다. 라이선스 칸: **BP** = Business Premium부터, **E3** = E3부터, **E5** = E5에서만. ZeroTrust Labs 스타터 세팅 서비스는 이 45개를 1~2주 안에 적용하고 증적 폴더까지 넘겨 드립니다.

1 계정 · 로그인 (10)

뚫리는 사고의 대부분은 비밀번호 하나로 시작됩니다. 이 묶음을 먼저 끝내세요.

	항목	라이선스	증적 · 완료일
☐	**모든 사용자에게 2단계 인증(휴대폰 승인) 강제** 조건부 액세스 정책으로 강제. "보안 기본값"만으로는 예외 관리가 안 됨	BP	
☐	**관리자 계정 전용 2단계 인증 + 관리자 계정 2개 이하로 정리** 일상 업무용 계정과 관리자 계정 분리	BP	
☐	**비상용 관리자 계정(break-glass) 1개 생성, 오프라인 보관** 2단계 인증 장애 시 잠금 방지	BP	
☐	**구식 로그인(레거시 인증) 차단** 2단계 인증을 우회하는 옛 프로토콜 차단	BP	
☐	**회사 기기가 아니면 접속 제한 (등록된 기기 또는 웹 열람만)**	BP	
☐	**해외 로그인 차단 또는 승인 필요 (출장자는 사전 예외)**	BP	
☐	**흔한 비밀번호·회사 이름 포함 비밀번호 금지 목록 적용**	BP	
☐	**퇴사 처리 절차 문서화 — 당일 계정 차단·세션 종료·기기 초기화·메일함 보존·문서 소유권 이전**	BP	
☐	**공용·서비스 계정 목록 작성, 로그인 방식·담당자 지정**	BP	
☐	**위험 로그인(유출 비밀번호·불가능한 이동) 자동 차단**	E5	

2 회사 PC · 휴대폰 (9)

잃어버린 노트북 한 대가 회사 전체 자료 유출이 되지 않게.

	항목	라이선스	증적 · 완료일
☐	**모든 회사 PC를 기기 관리(Intune)에 등록** Windows · Mac	BP	
☐	**디스크 암호화(BitLocker/FileVault) 강제, 복구 키 회사 보관**	BP	
☐	**기기 상태 규칙 — 암호화·백신·업데이트·화면 잠금 미준수 시 접속 차단**	BP	
☐	**Windows 업데이트 자동 배포 일정 설정**	BP	
☐	**PC 백신·랜섬웨어 방어 켜기 및 중앙 관리 (Defender)**	BP	
☐	**개인 휴대폰의 회사 앱(아웃룩·팀즈)에만 보호 정책 적용 — PIN, 복사 제한, 원격 삭제**	BP	
☐	**USB 저장장치 정책 결정 (차단 / 읽기만 / 허용) 및 적용**	BP	
☐	**신규 PC 자동 설정(Autopilot) 등록 — 박스에서 꺼내 로그인만 하면 세팅**	BP	
☐	**직원에게 관리자 권한 제거 (필요 시 개별 승인)**	BP	

3 메일 · 피싱 (9)

사고의 90%는 메일로 들어옵니다. 대표 사칭 송금 메일이 1순위 위협입니다.

항목	라이선스	증적 · 완료일
☐ **발신자 인증 3종 설정 — SPF · DKIM · DMARC** 우리 도메인 사칭 메일 차단. DMARC는 관찰 → 격리 → 차단 순으로	BP	
☐ **스팸·악성코드 필터 정책 점검, 배달 후 자동 회수(ZAP) 켜기**	BP	
☐ **외부 발신 메일에 "[외부]" 표시**	BP	
☐ **첨부파일·링크 사전 검사 (안전한 첨부파일·안전한 링크)** E3는 Defender for Office 365 추가 필요	BP·E5	
☐ **대표·임원 이름 사칭 보호 대상 등록**	BP·E5	
☐ **메일 자동 전달(외부로) 차단** 계정 탈취 후 가장 흔한 유출 경로	BP	
☐ **피싱 신고 버튼 배포 및 신고 시 처리 흐름 정하기**	BP	
☐ **메일 흐름 규칙 — 특정 조건 메일의 팀장 승인 / 외부 발송 숨은참조 / 면책 문구** 회사 정책에 맞게 선택	BP	
☐ **피싱 모의훈련 1차 실시 및 결과 기록** E5 내장. 그 외는 외부 도구 또는 수동	E5	

4 문서 · 공유 · 유출 방지 (10)

"전체 공개" 링크 하나가 회사 전체 폴더를 열어 줍니다.

항목	라이선스	증적 · 완료일
☐ **외부 공유 기본값 결정 — 조직 전체 정책 (금지 / 인증된 게스트만 / 링크 만료)**	BP	
☐ **"모든 사용자" 익명 링크 비활성화 또는 만료 30일 강제**	BP	
☐ **기존 외부 공유 링크 전수 조사 및 정리**	BP	
☐ **게스트 초대 권한 제한 (관리자 또는 지정 담당만)**	BP	
☐ **문서 등급(민감도 레이블) 4단계 이내 설계 — 예: 공개 · 내부 · 대외비 · 극비**	BP	
☐ **등급별 보호 동작 설정 (대외비 이상 암호화·워터마크) 및 기본 등급 지정**	BP	
☐ **유출 방지 규칙 1개 이상 — 주민번호·카드번호가 든 메일·파일 외부 발송 시 경고**	BP	
☐ **등급 해제·하향 시 결재 규칙 결정 (누가 승인하는지)** M365에 없는 기능 — LabelGate 또는 수동 절차	—	
☐ **팀즈 · SharePoint 구조 정리 — 부서별 사이트, 소유자 2명 이상, 방치 사이트 정리**	BP	
☐ **외부 조직과의 팀즈 채팅 허용 도메인 제한**	BP	

5 백업 · 기록 · 운영 (7)

사고가 나면 "복구할 수 있나"와 "누가 했나"를 5분 안에 답해야 합니다.

	항목	라이선스	증적 · 완료일
☐	**감사 로그 켜짐 확인, 보존 기간 확인 (기본 180일 / E5 1년+)**	BP	
☐	**메일·파일 보존 정책 1개 이상 (예: 삭제해도 1년 보관)**	BP	
☐	**백업 방식 결정 — Microsoft 365 Backup(사용량 과금) 또는 외부 백업** 휴지통 93일만으로는 랜섬웨어 대응 불가	추가	
☐	**보안 점수(Secure Score) 현재 값 기록 — 시작점**	BP	
☐	**보안 알림 수신자 지정 (관리자 메일 + 담당자), 주간 요약 켜기**	BP	
☐	**직원 안내 1회 — 2단계 인증·피싱 신고·문서 등급 사용법 (30분)**	—	
☐	**운영 문서 1장 — 담당자, 관리자 계정, 비상 계정 위치, 퇴사 절차, 사고 시 연락처**	—	

세팅 담당 · 완료 확인

서명: _____ 날짜: _____

고객사 확인

서명: _____ 날짜: _____

45개를 직접 하실 시간이 없다면

ZeroTrust Labs 스타터 세팅: 1~2주 안에 적용, 증적 폴더 전달, 직원 안내 포함. 이후 월 관리로 이어집니다. — contact@ztlabs.co.kr · https://ztlabs.co.kr