

사장님용 웹·앱 보안 체크리스트 30

개발을 몰라도 30분이면 확인할 수 있게 만들었습니다. 회원 정보, 주문, 예약 데이터 등을 다루는 홈페이지·쇼핑몰·앱이라면 한 번은 꼭 점검해 보세요.

사용법 — 항목마다 “아니오” 또는 “모르겠다”면 체크하지 마세요. 체크되지 않은 **위험** 항목이 하나라도 있다면 이번 주 안에 조치하는 것을 권합니다.

위험 사고로 바로 이어짐 **주의** 사고 가능성 높음 **기본** 운영 습관

앱몬스터 (Appmonster) · appmonster.co.kr · appmonster.kr@gmail.com

본 자료는 일반적인 점검 안내이며 법정 인증(ISMS 등) 기준을 대체하지 않습니다. 2026.09 작성

1. 계정과 권한

- ☐ **1 관리자 페이지에 퇴사자·예전 외주업체 계정이 남아 있지 않다** 위험
확인 방법 · 관리자 메뉴의 운영자/사용자 목록을 열어 지금 일하는 사람만 있는지 봅니다.
- ☐ **2 관리자 계정 비밀번호를 여러 명이 같이 쓰지 않는다** 위험
확인 방법 · 공유 계정이라면 사람마다 계정을 따로 만들고 권한을 나눕니다.
- ☐ **3 관리자·호스팅·도메인·클라우드 계정에 2단계 인증이 켜져 있다** 주의
확인 방법 · 구글·카페24·가비아·AWS·Firebase 등 계정 보안 설정에서 확인합니다.
- ☐ **4 도메인·호스팅·앱스토어 개발자 계정의 소유자가 우리 회사다** 주의
확인 방법 · 외주업체 이메일로 가입돼 있다면 연락이 끊겼을 때 서비스를 옮길 수 없습니다.
- ☐ **5 계정 목록(무엇을, 누구 이메일로, 언제 결제하는지)을 문서로 갖고 있다** 기본
확인 방법 · 한 장짜리 표로 충분합니다.

2. 데이터베이스와 저장소

- ☐ **6 Firebase/Firestore 보안 규칙에 'if true'(전부 허용)가 없다** 위험
확인 방법 · Firebase 콘솔 → Firestore Database → 규칙 탭. Storage 규칙도 같이 봅니다.
- ☐ **7 로그인한 사용자는 '자기 데이터만' 읽고 쓸 수 있다** 위험
확인 방법 · 개발자에게 “다른 회원 주문 내역을 URL이나 앱에서 볼 수 있나요?”라고 물어보세요.
- ☐ **8 관리자 여부를 서버에서 판단한다 (앱 화면에서만 숨기지 않는다)** 주의
확인 방법 · 버튼만 숨기고 서버 권한이 열려 있으면 누구나 관리자 기능을 쓸 수 있습니다.
- ☐ **9 업로드 파일에 크기·형식 제한이 있다** 주의
확인 방법 · 이미지 자리에 실행 파일이나 대용량 파일을 올릴 수 없어야 합니다.
- ☐ **10 테스트용 데이터와 실제 회원 데이터가 분리돼 있다** 기본
확인 방법 · 개발용 DB·프로젝트를 따로 쓰는지 확인합니다.

3. 비밀정보(키·비밀번호) 노출

- ☐ **11 서버 비밀번호·서비스 계정 키·결제 비밀키가 공개 GitHub 저장소에 없다** 위험
확인 방법 · GitHub 저장소가 Public인지, 파일에 password·secret·key 같은 단어가 있는지 확인합니다.
- ☐ **12 앱 설치 파일이나 웹 소스보기에 결제·문자 발송 비밀키가 들어 있지 않다** 위험
확인 방법 · 브라우저에서 '페이지 소스 보기' 후 secret, key를 검색해 봅니다.
- ☐ **13 외주업체와 작업이 끝난 뒤 API 키·비밀번호를 교체했다** 주의
확인 방법 · 결제(PG), 문자, 지도, AI API 키를 교체했는지 확인합니다.
- ☐ **14 API 키에 사용 한도·허용 도메인 제한이 걸려 있다** 주의
확인 방법 · 구글 클라우드 콘솔 → 사용자 인증 정보에서 키 제한을 확인합니다.
- ☐ **15 비밀번호를 카톡·메일 본문으로 주고받지 않는다** 기본
확인 방법 · 비밀번호 관리 도구나 일회성 공유 링크를 사용합니다.

4. 개인정보

- ☐ **16 주민등록번호를 수집·저장하지 않는다 (법적 근거가 없는 경우)** 위험
확인 방법 · 회원가입·예약 양식에 주민번호 입력란이 있는지 봅니다.
- ☐ **17 비밀번호는 암호화(해시)되어 저장된다** 주의
확인 방법 · 개발자에게 “비밀번호를 관리자가 볼 수 있나요?” 답이 ‘예’면 위험합니다.
- ☐ **18 연락처·주소 등 민감한 정보에 접근할 수 있는 사람이 제한돼 있다** 주의
확인 방법 · 관리자 권한 등급별로 회원 정보 열람 범위를 확인합니다.
- ☐ **19 개인정보처리방침이 실제로 수집하는 항목과 맞다** 주의
확인 방법 · 방침에 적힌 수집 항목과 가입 양식을 비교합니다.
- ☐ **20 탈퇴 회원 데이터를 정해진 기간 후 삭제한다** 기본
확인 방법 · 보관 기간과 삭제 방식이 정해져 있는지 확인합니다.

5. 서버·도메인·인증서

- ☐ **21 SSL 인증서(https)가 유효하고 만료일을 알고 있다** 위험
확인 방법 · 주소창 자물쇠 → 인증서 → 유효기간을 확인합니다.
- ☐ **22 도메인 만료일을 알고 있고 자동 연장이 켜져 있다** 위험
확인 방법 · 도메인 구매처(가비아·호스팅케이알·카페24 등)에서 확인합니다.
- ☐ **23 서버·CMS(워드프레스·그누보드 등)·플러그인이 1년 이상 방치되지 않았다** 주의
확인 방법 · 관리자 화면의 업데이트 알림을 확인합니다.
- ☐ **24 사용하지 않는 관리 페이지·테스트 페이지가 인터넷에 공개돼 있지 않다** 주의
확인 방법 · /admin, /test, phpMyAdmin 같은 주소가 열리는지 개발자에게 확인합니다.
- ☐ **25 서버 접속(SSH·FTP) 계정이 필요한 사람에게만 있다** 기본
확인 방법 · 호스팅 관리 화면에서 접속 계정 목록을 봅니다.

6. 백업과 사고 대응

- ☐ **26 DB와 업로드 파일이 자동 백업되고 있다** 위험
확인 방법 · 백업 주기(매일/매주)와 보관 위치를 확인합니다.
- ☐ **27 백업으로 실제 복구해 본 적이 있다** 주의
확인 방법 · 복구 테스트를 안 한 백업은 없는 것과 같을 수 있습니다.
- ☐ **28 서비스가 멈추면 알림을 받는다** 주의
확인 방법 · 무료 가동 모니터링 도구로도 충분합니다.
- ☐ **29 사고 시 누구에게 연락하고 무엇을 먼저 할지 정해져 있다** 주의
확인 방법 · 개발 담당자 연락처, 계정 잠금, 비밀번호 교체 순서를 한 장으로 적어 둡니다.
- ☐ **30 분기마다 이 체크리스트로 다시 점검한다** 기본
확인 방법 · 달력에 반복 일정으로 등록해 두세요.

점검 결과 해석

결과	의미	권장 조치
위험 항목 중 미체크 1개 이상	외부에서 데이터를 보거나 서비스를 멈출 수 있는 상태일 가능성	이번 주 안에 조치. 직접 어렵다면 전문가 점검
위험 모두 체크, 주의 미체크 3개 이상	당장 사고는 아니지만 계정·만료·백업 문제로 중단될 수 있음	한 달 안에 조치 계획 수립
25개 이상 체크	기본 운영이 잘 되고 있음	분기마다 같은 체크리스트로 재점검

점검을 맡기고 싶다면

앱몬스터 보안 점검은 이 30개 항목을 실제 설정·코드·서버에서 직접 확인하고, 위험도별 리포트와 긴급 조치를 함께 드립니다.

1회 보안 점검 80만원부터 · 보안 유지보수 월 30만원부터 (부가세 별도)

의뢰: appmonster.co.kr/services · appmonster.kr@gmail.com

Firebase를 쓰신다면 → appmonster.co.kr/guides/firebase-security-rules