정보보호산업법 시행령 개정

정보보호 공시 대응 전략 가이드

AhnLab

정보보호 공시 의무 강화, 기업의 새로운 과제

최근 잇따른 해킹 사고로 국민적 불안이 커짐에 따라, 이를 신속히 극복하고 국가 차원의 정보보호 역량을 강화하기 위한 「범부처 정보보호 종합대책(10.22., 관계부처 합동)」이 발표됐습니다. 이에 따라 2027년부터 정보보호 공시 의무가 확대될 예정입니다. 이제 기업은 보안 체계를 갖췄는지 여부를 넘어 보안이 실제로 어떻게 운영되고 있는지를 데이터와 증빙으로 설명해야 하는 단계에 접어들었습니다.

본 가이드는 정보보호산업법 시행령 개정안의 주요 변화와 공시 항목별 요구사항을 바탕으로, 기업이 공시 대응을 위해 어디서부터 무엇을 점검하고 어떻게 대응해야 하는지를 실무 관점에서 소개합니다.

정보보호 공시 , 이렇게 바뀝니다

1. 매출 기준 삭제

매출과 무관, 상장사라면 모두 대상

기존에는 매출 3,000억 원 이상 상장 기업에 한해 정보보호 공시 의무가 적용됐으나, 시행령 개정 이후에는 유가증권·코스닥 상장 법인 전체가 공시 대상에 포함된다. 기업 규모나 매출과 무관하게, 상장한 모든 기업에 공시 의무가 부여된다.

실무 포인트

- “우리 회사는 매출 규모가 작다”는 이유로 공시 제외 불가
- 상장사라면 조기 대응 여부가 공시 리스크로 연결
- 공시 준비 여부를 경영 차원의 이슈로 격상할 필요

2. ISMS 인증 기업 공시 대상 포함

ISMS 인증, 이제는 공시 대응까지 고려해야 할 단계

ISMS 인증 의무 기업은 기존에는 정보보호 공시 대상이 아니었으나, 이번 개정으로 공시 대상에 신규 포함된다. ISMS 인증을 받으면 공시 의무가 자동으로 부여된다.

실무 포인트

- ISMS 인증 보유 여부만으로는 불충분
- ISMS 인증 체계가 실제로 어떻게 운영되고 있는지 공시로 설명 필요
- ISMS 운영 문서, 점검 이력, 대응 기록을 공시용 증빙 관점에서 재정비 필요

3. 예외 조항 축소

모든 예외 삭제로 공시 사각지대 해소

기존에 공공기관, 금융회사, 소기업 등 일부 대상에 적용되던 예외 조항이 삭제됐다. 이는 공시 제도의 형평성을 높이고, 보안 사각지대를 줄이기 위한 조치로 해석된다.

실무 포인트

- 과거 예외 적용 여부를 전제로 한 판단은 더 이상 무효
- "우리는 예외 대상"이라는 인식 재검토 필요
- 공시 대상 여부를 최소가 아닌 최대 기준으로 해석하는 접근 필요

우리 회사도 대상인가? 적용 범위 전면 확대

구분	개정 전	개정 후
상장 기업	매출 3000억 ↑	상장 법인 전체
ISMS 인증	공시 의무 없음	공시 의무 대상 신규 포함
예외 조항	공공·금융 부문, 소기업, 전자금융업자 등 제외	모든 예외 조항 삭제

공시 대응 자가 진단 체크리스트

정보보호 공시 대응을 위해서는 개별 항목을 단편적으로 점검하기보다, 공시 대상 판단, 운영 체계 점검, 데이터·증빙 확보라는 영역별로 점검하는 접근이 필요합니다.
아래 체크리스트는 각 준비 영역별 실무 과제와 함께, 필요한 역량과 대응 가능한 보안 영역을 정리한 것입니다.

1. 공시 대상·적용 범위 판단

	Check List	필요 역량	대응 가능한 보안 솔루션
✓	개정안 기준 우리 기업이 의무 대상에 포함되는가?	규제 해석·컴플라이언스 체계 수립	보안 컨설팅
✓	공시 오류 발생 시 수정 프로세스를 숙지하고 있는가?	공시 운영 리스크 관리·프로세스 체계 수립	공시 프로세스 관리 워크플로우, 내부 통제 솔루션
✓	CISO에게 공시 의무 확대 내용을 보고했는가?	경영진 보고·보안 거버넌스 강화	이사회 보고용 GRC 리포트

2. ISMS 기반 운영 체계 점검

	Check List	필요 역량	대응 가능한 보안 솔루션
	전담 및 겸직 인원의 산정 기준이 명확한가?	보안 인력/조직 관리 및 운영	ITSM 기반 인력 운영 관리, 조직도, 직무기술서, CISO/CPO 체계도
	보유 인증의 유효기간과 범위가 최신인가?	인증 유지 및 감사 대응	ISMS/ISO 등 인증서, 인증 적용 범위 증빙 자료, 사후심사/갱신 결과
	임직원 정보보호 교육 수료율 기록이 구비되었는가?	보안 인식 제고 및 교육 증빙 확보	SAT(Security Awareness Training) 플랫폼, 교육 이수 이력
	침해사고 대응 훈련 및 취약점 점검 보고서가 있는가?	사고 대응(IR) 체계 및 취약점 관리	DR/XDR, SIEM, SOAR, 취약점 스캐너(VA), 모의침투 테스트 서비스, 모의 피싱 훈련 솔루션
	재무/인사 부서와 데이터 협의 채널을 가동했는가?	전사 협업 기반 데이터 수집 프로세스	전자 결재/협업 시스템

3. 공시용 데이터·증빙 체계 확보

	Check List	필요 역량	대응 가능한 보안 솔루션
	전년도 정보보호 관련 지출 내역을 확보했는가?	정보보호 투자 집계 및 증빙 체계	IT 재무 관리(FinOps) 도구, 보안 예산 관리 모듈, 보안 예산 편성서, 집행 전표, 계약서 및 인보이스 기반 투자 집계, 연간 투자 추이 리포트
	공시 산출 근거를 기록한 내부 증빙 가이드가 있는가?	감사 가능한 증빙 관리 및 문서화	정책·증적 관리 시스템(DMS), 로그 감사 시스템, 컴플라이언스 리포팅 도구
	공시 대상 IT 자산 현황이 최신화되어 있는가?	IT 자산 식별 및 가시성 확보	ITAM(IT Asset Management), 네트워크 자산 탐지 솔루션
	증빙 로그를 보관하는 보안 솔루션 상태를 점검했는가?	로그 보관·무결성·감사 추적성 확보	로그 관리, SIEM, 보안 감사 추적 솔루션

공시 리스크를 줄이는 단계별 대응 전략

정보보호 공시 의무 확대에 효과적으로 대응하기 위해서는 공시 대상 여부와 현재 보안 수준을 객관적으로 진단하고, 관리체계와 기술적 보호 조치를 강화한 뒤 운영 결과를 데이터 기반으로 증빙할 수 있는 공시 체계를 마련해야 합니다. 안랩은 이를 위해 'GAP 진단 - 보안 역량 강화 - 데이터 기반 공시'로 이어지는 3단계 대응 방향을 제시합니다.

Step. 1
현재 수준 점검(GAP 진단)
- 공시 항목 대비 준비 수준 점검
- 부족한 영역(GAP) 식별
- 우선순위 설정

Step. 2
컴플라이언스 대응 인프라 구축
- 엔드포인트·네트워크 보안 통제
- 위협 탐지·대응 체계
- 취약점 점검·조치·관리

Step. 3
감사·공시 대응 증빙 체계 완성
- 로그·이벤트 통합 관리
- 공시 항목별 데이터 정합성 확보
- 경영진·외부 제출용 리포트 체계 마련

정책 변화에 대응하는 안랩 통합 보안 전략

안랩 보안 솔루션은 정보보호 공시 항목별 요구사항을 충족하기 위한 운영 데이터와 증빙을 체계적으로 확보·관리하는 데 활용될 수 있습니다. 안랩은 공시 대응 과정에서 필요한 보안 활동을 실제 운영 결과로 연결할 수 있도록 지원합니다.

	안랩 보안 솔루션	공시 증빙 활용 예시
인력·조직 운영	보안 컨설팅 서비스	**전담 조직 운영 입증** 조직도, 직무기술서, 보고 자료 정형화
보안 통제	AhnLab EPP/V3	**엔드포인트 보안 적용** 자산 수량, 백신 설치율, 탐지/차단 관리
위협 대응	AhnLab EDR/MDR	**침해사고 대응** 이상 행위 탐지 이력, 대응 시간 로그 관리
경계 보안	AhnLab XTG	**트래픽·접속 통제** 방화벽 정책 적용 현황, IPS 차단·VPN 접속 이력 관리
지능형 위협	AhnLab MDS	**알려지지 않은 위협 분석** 의심 파일 동적 분석 건수, 제로데이 탐지 관리
취약점 관리	AhnLab ESA(단말)/ 서버·네트워크 취약점 컨설팅/ASM	**보안 점검·조치** PC 취약점 점검 /조치 이력 관리
통합 모니터링 관리	AhnLab XDR/MXDR AhnLab MSS	**실시간 모니터링** 보안 이벤트 모니터링 및 현황 관리

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901