

붙임1 정보보호산업법 시행령 개정 설명자료

□ 개정 주요내용

- (개정배경) 최근 디지털 전환이 산업 전반으로 확대되며 사이버 침해 사고가 지속적으로 증가함에 따라, 기업 등이 적절한 정보보호 활동을 하고 있는지 현황을 공개하는 정보보호 공시 제도의 강화 필요성 제기

[정보보호 공시 제도] (참고1)

- 안전한 인터넷 이용환경 조성과 기업의 정보보호 수준 향상을 위해 기업의 정보보호 투자·인력·활동 등 정보보호 현황을 공개하는 제도(‘16년 자율 공시 도입, ‘22년 의무화)

※ (법적근거) 「정보보호산업의 진흥에 관한 법률」 제13조, 동법 시행령 제8조, 동법 시행 규칙 제3조의2, 정보보호 공시에 관한 고시

- (개정사항) 공공성과 사회적 영향력이 높은 상장사(유가증권·코스닥 시장), 및 이용자 개인정보 보호가 필수인 ISMS 인증 기업으로 의무대상 확대

- 공공기관·금융회사·소기업을 제외하고 있던 예외 규정 폐지

- (개정목적) 국민의 알 권리를 보장하고, 기업의 자발적 정보보호 투자 유도를 통해 산업 전반의 보안 역량 및 침해사고 대응력 강화

- (기대효과) 공시를 계기로 기업이 자체적으로 내부 사이버보안 관리체계를 점검·보완해 침해사고 대응력을 강화하고, 투명한 정보공개를 통해 이용자·투자자의 신뢰 확보 및 시장 경쟁력 강화

<정보보호 공시 의무대상 개정안>

구분	현행	개정안
사업분야	회선설비 보유 기간통신사업자	좌동
	집적정보통신시설 사업자	
	상급종합병원	
매출액	클라우드컴퓨팅서비스제공자 유가증권시장 및 코스닥시장 상장법인 중 매출액 3,000억 이상	(개정)유가증권시장 및 코스닥시장 상장법인
이용자 수	정보통신서비스 직전년도 말 직전 3개월 일일평균 이용자 수 100만명 이상 기업	(개정)정보통신서비스 직전년도 일일 평균 이용자 수 100만명 이상 기업
ISMS 인증기업	(신설)	전년도말 기준 ISMS 인증을 받거나 유지하고 있는 자
예외 기준	공공기관, 소기업, 금융회사, 전자금융업자	(삭제)

붙임2 정보보호산업법 시행령 개정 FAQ

□ FAQ

- (Q1.) 정보보호 공시 제도란 무엇인가요?

A. 정보보호 공시 제도는 기업이 정보보호 투자, 인력, 관리체계 등 정보 보호 현황을 외부에 공개하도록 하는 제도입니다. 이를 통해 이용자와 투자자가 기업의 정보보호 수준을 확인할 수 있도록 하고, 기업의 자발적인 보안 투자 확대를 유도합니다.

- (Q2.) 이번 시행령 개정의 핵심 내용은 무엇인가요?

A. 이번 개정의 핵심은 정보보호 공시 의무대상 확대입니다. 기존 일부 기업에 한정되던 공시 의무를, 사회적 영향력이 큰 기업 전반으로 확대하여 제도의 실효성과 형평성을 강화합니다.

- (Q3.) 어떤 기업이 이번 개정안을 통해 공시 의무 대상이 되나요?

A. 다음 요건 중 하나에 해당하는 경우 공시 의무가 발생합니다.

- 유가증권시장(KOSPI) 또는 코스닥(KOSDAQ) 상장 법인(SPAC 제외)
- 전년도 ISMS 인증을 받았거나 유지 중인 기업
- 정보통신서비스 부문 연평균 일일 이용자 수 100만 명 이상 기업
- 예외 대상이었던 공공기관·금융회사·소기업 중 법령 기준 충족 기업

- (Q4.) 기존과 달라진 주요 사항은 무엇인가요?

A. 이번 개정안의 주요 내용은 아래와 같습니다.

- (전 상장사 확대) 유가증권시장, 코스닥시장 상장 기업(매출액 조건 삭제)
※ 단, 기업인수목적회사(SPAC) 제외
- (이용자 수 기준 변경) 직전 4분기 ⇒ 전년도 연평균
- (신설) 전년도 말 기준 ISMS 인증을 받거나 유지하고 있는 자(자율 인증 제외)
※ 신규 예상 : 대학교, 정보통신매출액 100억 이상 사업자 포함 등
- (제외조건 삭제) 공공기관·금융회사·소기업에 대한 일괄 예외 규정 삭제

현행 분야(대상자)		개정안 분야 (대상자)	
사업 분야	기간통신사업자	유지	기간통신사업자
	IDC사업자		IDC사업자
	상급종합병원		상급종합병원
	클라우드사업자		클라우드사업자
매출액	3천억 이상 상장사	⇒ 개정 전 상장사(매출액 조건삭제)	
이용자수	100만 이상(직전 4분기)	이용자 수	100만 이상(연평균)
신설		신설	ISMS 인증 의무기업 (정보통신매출액 100억 이상)
제외기준	공공,금융,소기업	삭제	제외기준 기준 삭제 (공공, 금융, 소기업 포함)

○ (Q5.) 새로운 보안 투자나 인력 채용이 의무화되나요?

- A. 아닙니다. 이번 개정은 새로운 보안 설비 구축이나 인력 배치를 강제하는 제도가 아닙니다. 기업이 이미 수행 중인 정보보호 투자·활동 현황을 공개하는 정보공개형 제도입니다.

○ (Q6.) 기업 입장에서 어떤 부담이 생기나요?

- A. 정보보호 관련 내부 자료 취합, 공시 항목 정리 및 시스템 입력 등 행정적·관리적 부담이 발생합니다. 다만, 이미 수행중인 정보보호 현황을 공개하는 제도이기 때문에 추가 부담이 제한적이며, 또한, 공시 경험이 없는 중·소기업의 지원을 위해 가이드라인, 교육, 컨설팅 등 이행 지원을 병행할 예정입니다.

○ (Q7.) 기업에는 어떤 이점이 있나요?

- A. 기업에서는 정보보호 수준에 대한 대외 신뢰도 제고, 투자자·거래처 대상 기업 이미지 개선, 내부 정보보호 관리체계 점검 및 정비 계기 등의 이점이 있습니다.

○ (Q8.) 언제부터 적용되나요?

- A. 시행령 개정 절차 완료 후 '27년부터 시행될 예정이며, 구체적인 공시 일정과 작성 방법은 가이드라인 및 별도 안내를 통해 공지될 예정입니다. ※ 정보보호 공시 종합 포털 : isds.kisa.or.kr

○ (Q9.) 정보보호 공시는 어떤 방식으로 공시해야 하나요?

- A. 정보보호 공시 종합 포털(isds.kisa.or.kr)을 통해 정해진 공시 양식에 따라 정보보호 투자, 인력, 인증·평가·점검, 활동을 입력·제출하는 방식으로 진행됩니다.

※ 정보보호 공시 제도는 기업 공시 제도와는 별도의 제도로, 기업 전자공시시스템(dart)가 아닌 정보보호 공시 종합 포털에 관련 양식을 매년 6월 30일까지 제출하여야 합니다.

○ (Q10.) 정보보호 공시 관련 문의는 어디로 하면 되나요?

- A. 정보보호 공시제도 관련 문의는 **한국인터넷진흥원 정보보호 공시 종합포털(isds.kisa.or.kr)** 및 isds@kisa.or.kr로 문의 바랍니다.

참고1 정보보호 공시 제도 소개

□ 정보보호 공시 제도

- (개요) 정부는 안전한 정보통신서비스 이용환경 조성과 기업의 정보 보호 수준 향상을 위해 기업의 정보보호 현황을 공개하는 정보보호 공시 제도를 운영 중('16년 자율 공시 도입, '22년 의무화)

※ (법적근거) 「정보보호산업의 진흥에 관한 법률」 제13조, 동법 시행령 제8조, 동법 시행규칙 제3조의2, 정보보호 공시에 관한 고시

- (공시내용) 정보보호 투자 · 인력 현황, 정보보호 관련 인증 · 평가 점검에 관한 사항 및 이용자 정보보호를 위한 활동 현황

공시 항목	주요내용
정보보호 투자 현황	▶ 정보기술부문 투자 대비 정보보호부문 투자 현황 등
정보보호 인력 현황	▶ 정보기술부문 인력 대비 정보보호부문 전담인력 현황 등
정보보호 관련 인증·평가·점검	▶ ISMS, CSAP 등 정보보호 관련 인증·평가·점검 현황 등
정보보호를 위한 활동 현황	▶ 정보보호 투자 활성화 실적, 정보보호 인식 제고 교육 등 기업의 정보보호를 위한 대내외 활동 현황 등

- (적용대상) (자율)정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자, (의무)사업분야, 매출액, 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자

- (공시기한) 매년 6월 30일까지 정보보호 전자공시시스템 등록

- (공시 이행 혜택) ISMS, ISMS-P 인증 수수료 30% 할인(자율공시 기업), 공시 우수기업 과기부 장관 표창 수여 및 KISA 지원사업 가점 부여(자율공시 기업)

- (미준수 시 제재) 기한 내 공시하지 않거나 공시 검증을 거부 · 방해, 수정요청에 따르지 않은 경우 최대 1천만 원의 과태료 부과

과태료 항목	1차 위반	2차 위반	3차 이상
정보보호 현황을 공시하지 않은 경우	300만원	600만원	1,000만원
공시 내용의 검증을 거부 또는 방해하거나 수정 요청에 따르지 않은 경우	300만원	600만원	1,000만원

□ 정보보호 공시 양식

[회사명] 정보보호 현황

「정보보호산업의 진흥에 관한 법률」 제13조, 같은 법 시행령 제8조 및 「정보보호 공시에 관한 고시」에 따라 다음 사항에 대해 공시합니다.

작성 기준일 : 20 . .

정보기술부문 투자액(A)	
	(B) 투자총액((1)~(5) 총 합계)
	(1) 정보보호시스템 구축비 및 유지보수비
	(2) 정보보호서비스 및 컨설팅 이용료
	(3) 정보보호 교육·훈련비 및 인건비
	(4) 물리보안 제품 및 서비스 이용료
	(5) 기타 정보보호 관련 비용 (정보보호 소모품, 정보보호 관련 보험비 등)
1. 정보보호 투자 현황	B / A
	특기사항*
	총임직원
	정보기술부문 인력(C)
2. 정보보호 인력 현황	내부인력
	외주인력(D)
	계
	D / C

	CISO/CPO 지정 현황	구분	지정 여부	직책	임원 여부	겸직 여부	CEO 직속 여부
		CISO					
		CPO					
특기사항*							
3. 정보보호 관련 인증, 평가, 점검 등에 관한 사항							
4. 정보보호를 위한 활동 현황	IT 자산 식별 목록 및 관리	정성적인 추가 활동내역은 별지로 추가 가능 침해사고 대응체계 수립 및 운영 최고의사결정기구(이사회 등)의 정보보호 활동에 관한 의사결정 정보보호 교육 등 인식제고 활동					
	정보보호 정책·지침 마련 및 운영						
	정보보호 전담 조직 운영						
	침해사고 대응체계 수립 및 운영						
	최고의사결정기구(이사회 등)의 정보보호 활동에 관한 의사결정						
	정보보호 교육 등 인식제고 활동						
	기타 정보보호 활동 내역						

* 해당 항목의 작성은 공시 기업의 선택사항

(회사명) 대표이사 OOO는 상기 공시 내용에 거짓이 없음을 확인하였습니다.

0000. 00. 00.

(회사 대표이사 직인)