정보보호 공시
가 이 드 라 인

2021. 12.

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

정보보호 공시
가 이 드 라 인

2021. 12.

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

정보보호 공시 가이드라인

CONTENTS

Ⅰ 총칙 04

Ⅱ 공시 내용 09

Ⅲ 공시 이행절차 및 사후검증 33

Ⅳ FAQ 40

Ⅴ 한눈에 보는 정보보호 공시 과정 46

[첨부 1] 정보기술 및 정보보호부문 자산 분류표 48

[첨부 2] 정보보호 서비스 분류표 55

Ⅰ 총칙

목 적

**이용자에게 객관적인 기업 선택의 기준을 제시하고,
기업은 정보보호를 기업경영의 중요요소로 포함**

- 사회·경제 전반의 **디지털 대전환**이 이루어지면서 **사이버 침해사고**가 기업의 경제적 피해, 대외 신뢰도 저하 등 **기업 경영**에 **직접적**인 **영향**을 끼치게 됨에 따라
  - 정보통신서비스 관련 기업뿐만 아니라, 이용자의 개인정보를 대량으로 보유한 전자상거래 기업 또는 중요 연구개발 정보를 보유한 첨단기업 등 **모든 기업**에 있어 **정보보호**가 **핵심 경쟁력**으로 **부각**됨

- 그러나 **기업**의 **정보보호 현황**은 **위험관리**(Risk Management)와 **관련된 주요 정보**이지만 그 동안 시장에서 **투명**하게 **공개**되지 **못했음**
  - 경영주체들은 **정보보호**를 투자가 아닌 **비용**으로 **인식**하는 경향이 많고, **이해관계자**들은 해당 기업의 **정보보호 현황**을 알 수 없어 **불충분한 정보**로 **서비스 이용, 투자** 등 **의사결정**이 이루어짐

- 정보보호 공시제도는 **이용자 보호 및 알권리를 보장**하고 **기업**의 **자발적인 정보보호 투자를 촉진**하기 위한 제도로써,
  - **(주주) 기업**의 **잠재적 재무상태 변화**에 **주요**한 **영향***을 미칠 수 있는 **정보보호 현황**에 대한 **주주**의 **알권리 확보**

    * 기업의 중요 정보 유출, 징벌적·법정 손해배상제도 도입에 따른 강화된 배상책임, 소비자 신뢰도 저하 등으로 인한 큰 재무적 변동이 발생 가능
  - **(소비자·국민)** 기업 등이 보유하고 있는 다양한 **정보**의 **보호수준을 간접적**으로 **파악**할 수 있도록 하여 **소비자 선택권 강화**
  - **(기업)** 기업 스스로 **정보보호 수준**을 **객관적**으로 **파악**하고, 이용자 등에게 **정보보호 활동**을 **공시**함으로써 **법적 근거**를 갖고 **기업**의 **보안 투자 정도**를 **외부**에 **알릴** 수 있는 **기회**

적용 대상

- **(자율공시)** 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자(정보보호산업법 제13조제1항)

※ 정보통신 서비스(유·무선통신 서비스, 방송 서비스 등), 쇼핑몰, 포털, 인터넷 뱅킹 등 인터넷을 통해 사업 활동을 하는 영리, 비영리 업체 모두 포함

관련근거

「**정보보호산업의 진흥에 관한 법률**」 **제13조(정보보호 공시)** ① 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있다. 이 경우 「자본시장과 금융투자업에 관한 법률」 제159조에 따른 사업보고서 제출대상 법인은 같은 법 제391조에 따라 정보보호 준비도 평가 결과 등 정보보호 관련 인증 현황을 포함하여 공시할 수 있다.

- **(의무공시)** 사업분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자(정보보호산업법 제13조제2항)

관련근거

「**정보보호산업의 진흥에 관한 법률**」 **제13조(정보보호 공시)** ② 제1항에도 불구하고 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 공시를 도입할 필요성이 있는 자로서 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제1항에 따른 정보보호 현황을 공시하여야 한다. 다만, 다른 법률의 규정에 따라 정보보호 현황을 공시하는 자는 제외한다.

정보보호 공시 의무대상 기준

사업 분야	• 회선설비 보유 기간통신사업자(ISP) ※「전기통신사업법」 제6조제1항
	• 집적정보통신시설 사업자(IDC) ※「정보통신망법」 제46조
	• 상급종합병원 ※「의료법」 제3조의4
	• 클라우드컴퓨팅 서비스제공자 ※「클라우드컴퓨팅법」 시행령 제3조제1호
매출액	• 정보보호 최고책임자(CISO)* 지정·신고해야하는 유가증권시장 및 코스닥시장 상장법인 중 매출액 3,000억 원 이상
이용자 수	• 정보통신서비스 일일평균 이용자 수** 100만 명 이상 (전년도말 직전 3개월간)

* Chief Information Security Officer: 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 담당하는 정보보호 최고책임자

** 이용자 수: 순방문자수(Unique View : IP 기준 1일 방문자 수)

정보보호 공시 의무 예외 기준

공공기관	• 공기업 및 준정부기관 등 ※「공공기관운영법」
소기업	• 평균매출액 120억 원 이하 기업 ※「중소기업기본법 시행령」 제8조제1항 – 업종별 매출액 기준 상이(10~120억원), 정보통신업은 50억원 이하
금융회사	• 은행, 보험, 카드 등 금융회사 ※「전자금융거래법」 제2조제3호
전자금융업자	• 정보통신업 또는 도·소매업을 주된 사업*으로 하지 않는 전자금융업자 ※「전자금융거래법」 제2조제4호, 한국표준산업분류

* 하나의 기업이 둘 이상의 서로 다른 업종을 영위하는 경우에 직전 사업연도의 매출액 비중이 가장 큰 업종을 기준으로 해당 기업의 주된 업종을 판단함

※ 소기업의 경우, 「중소기업 범위 및 확인에 관한 규정」에 따라 중소기업현황정보시스템을 통해 발급받은 확인서 제출 필요

주요 용어

주요 용어	설명
정보보호 공시 제도	이용자의 안전한 인터넷 이용과 기업의 정보보호 투자 활성화를 위해 기업의 정보보호 투자 인력활동 등에 관한 정보를 공개하도록 하는 제도
공시대상연도	정보보호 공시를 이행하는 연도의 직전연도 ※ 예를 들어 기업의 회계연도가 4월부터 다음해 3월까지라고 하더라도 2022년에 공시하려고 할 경우 자산의 감가상각비나 비용을 산정할 때 자료는 2021년 1월 1일부터 12월 31일까지 발생한 자료를 바탕으로 정보보호 현황을 작성(공시연도의 직전연도의 회계자료를 바탕으로 공시자료를 산출하기 때문)
정보보호 투자현황	정보보호 공시자가 공시대상연도의 투자액에서 정보기술부문 투자액과 정보보호부문 투자액을 산정하여 산출한 자료
정보기술부문 투자액	IT 기획·개발·운영·유지·보수 및 정보보호 등에 소요되는 모든 경비의 합계로서 기업회계기준에 따라 발생주의*에 의한 비용
정보보호부문 투자액	정보보호 등에 소요되는 모든 경비의 합계로서 기업회계기준에 따라 발생주의*에 의한 비용 ▸정보기술부문으로 분류된 자산(감가상각비)·인건비·비용 중에서 정보보호와 관련된 자산·인건비·비용을 분류하여 산출
정보보호 인력현황	정보보호 공시자가 공시대상연도의 인력에서 정보기술부문 인력과 정보보호부문 인력을 집계하여 산출한 자료
정보기술부문 인력	정보기술부문 인력은 정보기술 및 정보보호 업무를 전담하는 내부인력(정규직, 계약직)과 외부인력(사내파견, 외부전담)의 공시대상연도 월평균 인원
정보보호부문 전담인력	정보보호부문 전담인력은 정보보호 업무를 전담하는 내부인력(정규직, 계약직)과 외부인력(사내파견, 외부전담)의 공시대상연도 월평균 인원
정보보호 관련 인증·평가·점검 등에 관한 사항	정보보호 공시자가 공시대상연도 내에 취득하거나, 인증 기간이 공시대상연도 내에 유효한 인증, 평가, 점검 현황
정보보호를 위한 활동	정보보호 공시자가 공시대상연도 내에 수행한 정보보호 관련 내·외부 활동

* 발생주의는 회계처리를 하는 방법의 하나로 현금 유출입 시점에 관계없이 거래나 그 밖에 경제적 가치가 창출, 변형, 교환, 이전 또는 소멸되는 시점에 거래를 기록하고 표시하는 것

Ⅱ 공시 내용

정보보호 현황 서식

- 정보보호 공시 기업은 「정보보호산업의 진흥에 관한 법률 시행령」 제8조에 제시된 4개의 항목에 대하여 공시대상 연도의 정보기술 및 정보보호 실적 자료를 집계하고, 정보보호 현황을 산출하여 작성함

정보보호 현황 서식

<table>
<tr><td rowspan="5">1. 정보보호
투자 현황</td><td colspan="2">정보기술부문 투자액(A)</td><td></td></tr>
<tr><td colspan="2">정보보호부문 투자액(B)</td><td></td></tr>
<tr><td rowspan="2">주요 투자 항목*</td><td></td></tr>
<tr><td></td></tr>
<tr><td colspan="2">B / A</td><td></td></tr>
<tr><td colspan="3">특기사항*</td><td></td></tr>
<tr><td rowspan="7">2. 정보보호
인력 현황</td><td colspan="2">총임직원</td><td>(내부인력)</td></tr>
<tr><td colspan="2">정보기술부문 인력(C)</td><td>(내부인력 + 외주인력)</td></tr>
<tr><td rowspan="3">정보보호부문
전담인력(D)</td><td>내부인력</td><td>(정규직+계약직)</td></tr>
<tr><td>외주인력</td><td></td></tr>
<tr><td>계</td><td></td></tr>
<tr><td colspan="2">D / C</td><td></td></tr>
<tr><td colspan="2">CISO/CPO 지정 현황</td><td><table><tr><td>구분</td><td>직책</td><td>임원 여부</td><td>겸직 여부</td><td>주요 활동</td></tr><tr><td>CISO</td><td></td><td></td><td></td><td></td></tr><tr><td>CPO</td><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td colspan="3">특기사항*</td><td></td></tr>
<tr><td colspan="3">3. 정보보호 관련 인증, 평가, 점검 등에 관한 사항</td><td></td></tr>
<tr><td colspan="3">4. 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황</td><td></td></tr>
</table>

* 해당 항목의 작성은 공시 기업의 선택사항

- 정보보호 공시자는 공시대상연도에 처리하거나 발생한 회계 및 인증 내용을 기준으로 정보보호 현황을 작성하여 공시하여야 함

정보보호 현황 자료 산출 방법

1. 정보보호 투자 현황 산정

정보보호 투자현황 준비자료

준비 자료	작성 내용	비고
회사사업 소개자료	주요 사업 분야별 사업 내용	정보보호 대상 파악
조직도	공시대상연도의 조직도	정보기술/정보보호 조직 확인
공시대상기간의 자산대장	회계부서에서 고정자산으로 등록한 자산들의 감가상각 계상 대장. 자산명과 감가상각비 등 표시	당기 감가상각액
공시대상기간의 비용원장	공시대상연도 1월1일부터 12월31일까지 처리한 비용 원장(전표일자, 적요, 금액 등 표시)	
외주용역비 내역	정보기술부문, 정보보호부문 외주비 상세내역(기안서, 계약서 등)	정보기술/정보보호 용역비 산정
정보기술부문, 정보보호부문 인원 관련 인건비	공시대상연도에 근무한 정보기술/정보보호 인력들의 급여, 상여, 퇴직급여, 급여성 복리후생비 합계	연봉 등의 다른 대안 가능

- 정보기술부문/정보보호부문 투자액은 정보기술/정보보호 관련 ①유·무형자산(감가상각비)과 ② 비용(자산과 인건비 제외), ③ 인건비로 산출함

  - 이를 확인하기 위해서는 회계부서 등의 협조를 통해 자산대장, 비용원장 및 외주 용역 내역과 인건비 내역 등의 자료를 통해 투자액 집계표를 작성하여 보관해야함

    ※ 인건비는 정보기술 및 정보보호 인력현황에 속하는 내부직원(정규직, 계약직)들의 급여, 상여, 퇴직급여, 급여성 복리후생비의 합계를 말함

정보기술부문과 정보보호부문 투자액 집계표

구분	정보기술부문 투자액	정보보호부문 투자액
유·무형자산 (감가상각비)		
인건비		
비용(감가상각비, 인건비 이외)		
합계		

정보보호 투자 현황 산식

$$\text{정보기술부문 투자액 대비 정보보호부문 투자액의 비율(B/A) (단위 : %)} = \frac{\text{정보보호부문 투자액(B) (단위 : 원)}}{\text{정보기술부문 투자액(A) (단위 : 원)}} \times 100$$

- 정보보호 투자액 중 공시대상연도에 이용자 보호, 보안수준 제고 등을 위해 시스템 구축, 제품 구입 등에 투자한 대표적인 항목은 공시 서식의 '주요 투자 항목'에 작성 가능함(의무 작성 항목은 아니며 기업의 선택사항)
  - 「정보보호산업의 진흥에 관한 법률」에 따라 지정된 우수정보보호제품, 정보보호 성능평가 받은 제품을 개발 및 도입한 내역이 있다면 '주요 투자 항목'에 작성 가능

우수 정보보호제품	• 「정보보호산업의 진흥에 관한 법률」 제18조(우수 정보보호기술등의 지정)와 관련하여 우수 정보보호 제품으로 지정된 제품
정보보호 성능평가	• 「정보보호산업의 진흥에 관한 법률」 제17조(성능평가 지원)와 관련하여 정보보호 제품의 보안 및 각종 성능을 측정하여 품질 향상을 이끌고 시장경쟁력과 기업의 신뢰도를 확보하는 제도

※ 한국인터넷진흥원 또는 정보보호산업진흥포털(ksecurity.or.kr)에서 우수정보보호 제품, 정보보호 성능평가 제품 목록 등을 확인할 수 있음

- 비용원장 등에 사용부서가 명시되어 있고, 사용부서가 정보기술 부서 또는 정보보호 부서인 경우 해당 내역을 정보기술부문 투자액 또는 정보보호부문 투자액로 인정받을 수 있어 정보보호 투자 현황 산정에 유용함

- 가능하다면 기업의 내부 회계정보시스템에서 보이는 모든 항목을 포함하여 받는 것이 자료 산출 시 유리함
  - 자산대장에는 자산명, 취득일자, 상각개시일, 취득원가, 내용연수, 잔존가치, 감가상각방법, 자본적지출내용, 공시대상연도 감가상각비 명 등이 포함되어 있어야 함
  - 비용원장에는 공시대상연도 비용의 계정과목, 발생일자, 금액, 적요 명 등이 포함되어 있어야 함

1.1 자산의 분류 및 산정

- 유·무형자산의 경우 자산대장 등을 활용해 산출할 수 있으며, 당기 감가상각비용 투자액으로 인정함

  * 공시대상연도 감가상각 대상 유무형자산의 모든 감가상각비 인정

  - 기업에 따라 구매한 IT 자산을 감가상각으로 처리하지 않고 구입한 연도에 비용으로 처리하는 경우나 아웃소싱 또는 렌탈 서비스를 이용하는 경우에는 자산(감가상각비)이 없거나 적을 수 있음

> **예** 유·무형 자산의 감가상각비는 구입한 날로부터 내용연수 기간 동안 기업 내 규정에 따라 상각액이 정해지며, 보통 PC 등은 3년이나 경우에 따라서는 2년 또는 4년으로 처리하는 기업도 있음

* 공시대상연도가 2020년인 경우 감가상각비는 2020년 12월 31일자 2020년간 감가상각액임

- 자산분류는 [첨부1] 정보기술 및 정보보호부문 자산 분류표를 준용하거나 내부 자산 분류체계를 적용하여 자산대장에서 정보보호 투자 현황을 산정함

자산대장 (예시)

자산분류(계정명)		자산명	취득일	취득원가	사용 부서	감가상각비 (2020년*)
대분류	소분류					
무형자산	소프트웨어	이메일발송솔루션	2017.11	5,000,000	IT팀	
무형자산	소프트웨어	DB암호화	2018.12	50,000,000	보안팀	
무형자산	소프트웨어	DB접근제어	2018.12	15,000,000	보안팀	
무형자산	특허권	특허	2020.12	500,000,000	영업팀	
유형자산	시설장치	노트북	2017.11	100,000,000	IT팀	
유형자산	비품	가구	2018.02	10,000,000	총무팀	
유형자산	건물	본사건물	2000.01	-	-	-

- 내부 자산분류체계를 적용하여 자산대장을 작성한 경우에는 [첨부1] 정보기술 및 정보보호부문 자산 분류표의 분류체계와 매핑하여 누락이나 불명확한 분류가 있는지 검토하고,

  - 누락 또는 불명확한 자산분류에 대해서는 한국인터넷진흥원을 통하여 정보기술/정보보호 자산으로 분류할지 여부를 확인하고 정보기술/정보보호투자 현황으로 산정함

자산대장 –정보기술/정보보호 자산 분류 (예시)

자산분류(계정명)		자산명	취득일	취득원가	사용 부서	감가 상각비	정보기술	정보보호
대분류	소분류							
무형자산	소프트웨어	이메일발송솔루션	2017.11	5,000,000	IT팀		○	
무형자산	소프트웨어	DB암호화	2018.12	50,000,000	보안팀		○	○
무형자산	소프트웨어	DB접근제어	2018.12	15,000,000	보안팀		○	○
무형자산	특허권	특허	2020.12	500,000,000	영업팀		x	
유형자산	시설장치	노트북	2017.11	100,000,000	IT팀		○	
유형자산	비품	가구	2018.02	10,000,000	총무팀		x	
유형자산	비품	서버	2019.12	-	-		○	
유형자산	건물	본사건물	2000.01	-	-	-	x	

- 정보보호 제품에 대한 투자액 산정 시 정보보호 전용 제품만을 인정하고 있어 정보보호 기능을 별도로 분리·산정할 수 없는 유형자산의 투자금액(감가상각비)은 정보보호 투자금액으로 인정하지 않음

정보기술부문 투자 인정	사용부서와 상관없이 회사 내 모든 PC와 부속장치, 모니터, 프린터, 복합기, TV(모니터 대용), 의료정보시스템, 원격회의 시스템, 빔 프로젝터, 스캐너, PDA, 태블릿, IP전화기 등
정보보호부문 투자 인정	문서파쇄기(세단기), 노트북 케이블 락, 모니터 보안경, 보안USB 등
	물리적 보안 제품(CCTV, 바이오인식, 접근제어, 알람모니터링 등)과 물리 보안 서비스(세콤, ADT캡스, 시큐리티넘버원 등)(단, 물리보안서비스 인력의 인건비는 제외. 외주인력에서도 제외) ※ 단, 사업 분야의 특성을 고려하여 기업의 선택에 따라 정보보호 자산 또는 비용으로 포함하지 않아도 무방함
	재해, 재난 등에 따른 서비스 중단을 대비하여 구축하는 백업 서버 등의 재해복구시스템 및 외주용역의 IT 재해복구 서비스 이용료 ※ 업무 연속성 측면에서 정보보호 투자로 인정함
	「정보보호산업의 진흥에 관한 법률」에 따라 지정된 우수 정보보호 제품, 정보보호 성능평가 제품 개발 및 도입 비용
정보기술부문 투자 불인정	방송·무대용 조명장비, 의료기기 등
정보보호부문 투자 불인정	정보보호 기능이 일부 내재된 제품 및 정보보호 전용제품이 아니지만 정보보호를 목적으로 구입한 제품(물리적 망분리를 위한 PC 등)

1.2 비용의 분류 및 산정

- 비용원장에서 일반적으로는 지급수수료, 통신비, 유지보수비, 서비스 이용료, 사무용품비, 도서용품비, 교육훈련비, 임차료, 외주용역비 같은 계정과목 중 정보기술/정보보호 관련 비용들을 산정함
  - 비용원장 계정과목 중 정보기술/정보보호 비용이 없을 것으로 보이는 영업비, 잡비, 차량유지비, 광고선전비, 이자비용, 기부금 등의 계정은 산출할 필요 없음

- 비용원장 계정과목 중 급여, 상여, 복리후생비 등의 인건비와 관련된 계정과목은 정보기술 인력과 정보보호 인력이 먼저 확정된 다음 그 인력들의 인건비를 산출해야 하므로 비용원장 계정과목에서 산정할 필요 없음

비용원장 (예시)

전표일자	계정과목	적요	사용부서	금액
2020.01	지급수수료	메신저 사용료	IT팀	
2020.02	지급수수료	복합기 사용료	영업팀	
2020.01	외주용역비	외주용역 일반 인건비	IT팀	
2020.02	외주용역비	외주용역 일반 인건비	총무팀	
2020.04	외주용역비	ISMS컨설팅 비용	보안팀	
2020.04	소모품비	백신 사용료	보안팀	
2020.01	통신비	전용선비	IT팀	
⋮	⋮		⋮	

- 비용원장은 적요 항목을 기준으로 정보기술부문 비용을 분류하고, 분류된 정보기술부문 비용에서 정보보호부문 비용을 분류함
  - 적요 항목에 같은 내용이더라도 사용부서가 정보기술 부서라면 정보기술 비용으로 인정함. 마찬가지로 사용부서가 정보보호 부서라면 정보보호 비용으로 인정함
  - 다만, 적요 항목이 명백히 정보기술/정보보호부문 관련 비용과 관련이 없는 비용(식사비, 접대비, 교통비 등)은 제외함

비용원장 –정보기술/정보보호 분류 (예시)

전표일자	계정과목	적요	사용부서	금액	정보기술	정보보호
2020.01	지급수수료	메신저 사용료	IT팀		○	
2020.02	지급수수료	복합기 사용료	영업팀		○	
2020.01	외주용역비	외주용역 일반 인건비	IT팀		○	
2020.02	외주용역비	외주용역 일반 인건비	총무팀		x	
2020.04	외주용역비	ISMS컨설팅 비용	보안팀		○	○
2020.04	소모품비	백신 사용료	보안팀		○	○
2020.01	통신비	전용선비	IT팀		○	

1.3 인건비의 산정

- 정보기술/정보보호부문의 인건비는 정보보호 인력 현황에서 파악된 정보기술/정보보호부문 전담 인력 중 내부 인력들에 대한 인건비로 산정함(외주인력은 외주 용역비에 포함)

- 정보기술 및 정보보호 인력의 인건비는 회계상 비용을 토대로 하되 기본급, 연봉, 성과급, 상여 등 급여, 퇴직급여, 급여성 복리수행비 항목에 따라 세부 근거 자료를 추가 확인하여 산정함

  - 급여 및 상여 산정액은 회계 상 내역과 일치하여야 하며, 인별 급여의 기초자료는 연봉계약서, 원천징수영수증 또는 급여대장에 근거함
  - 인건비 산정 시 정보기술/정보보호 전담인력들의 급여 등은 급여대장, 원천징수영수증 등으로 확인되는 급여 총액임

- 기업내부 기준에 따라 개인별 인건비의 공개가 어려운 경우 또는 인원이 많아서 개인별로 산정하기가 어려운 경우에는 부서나 팀별로도 인건비를 산정할 수 있음

  - 이 경우 부서나 팀에 소속된 인력들에 대한 기본 정보, 예를 들면 소속부서/팀, 담당 업무 같은 정보를 별도로 준비하여 근거 마련이 필요함

개인별 인건비 산출내역 (예시)

사번	이름	부서	업무	연봉	4대보험(회사)	기타 복리후생비
1975012	홍길동	IDC센터		65,000	3,400	1,500
2005145	성춘향	IT운영팀		45,000	1,340	1,200
⋮	⋮	⋮	⋮	⋮	⋮	⋮

※ 항목은 회사의 운영방침에 따라 달라질 수 있으나, 회계 상의 인건비 및 복리후생비와 서로 설명이 될 수 있어야 함

부서별 인건비 산출내역 (예시)

부서/팀 명	대상자수	급여 (a)	상여 (b)	퇴직급여 (c)	급여성 복리후생비 (d)		총인건비 (a+b+c+d)
					4대보험	기타복리	
정보기술 1부	33	000	000	000	000	000	0,000
정보보호 1팀	8	000	000	000	000	000	0,000
합계	41	000	000	000	000	000	0,000

- 정보기술/정보보호 인력이 R&D에 참여하는 경우 그 인력의 인건비가 R&D비용에 반영되게 되고, 그 비용을 정보기술/정보보호 투자로 인정할 경우 인건비가 이중으로 산출될 수 있어 주의가 필요함

- 퇴직급여는 인별 퇴직급여 산정방식에 따라 계산하여야 함

  - 확정급여형(DB형) 또는 퇴직보험금을 사내 유보할 경우
    - ▸ 계속 근무 중일 경우: 인별 퇴직급여충당부채에서 전기 퇴직급여충당부채를 차감
    - ▸ 당기 중 퇴직할 경우: 퇴직 시 정산금액에서 전기 퇴직급여충당부채를 차감
  - 확정기여형(DC형)일 경우 당기 인별 퇴직보험사에게 불입한 금액임. 회계 상 퇴직급여로 계상한 금액과 일치해야 함

확정급여형 (DB형) 퇴직연금	회사가 근로자의 퇴직연금 재원을 외부 금융회사에 적립하여 운용하고, 근로자 퇴직 시 정해진 금액을 지급하는 제도로 회사의 운용손익이 회사에 귀속됨. 국제회계기준을 적용하는 회사는 보험수리적 기법을 사용하여 확정급여채무의 현재가치를 계산하고, 사외 적립자산의 공정가치를 차감하여 퇴직급여로 계상함
확정기여형 (DC형) 퇴직연금	회사가 매년 연간 임금총액의 일정비율(1/12이상)을 적립하고, 근로자가 적립금을 운용하는 방식임. 국제회계기준을 적용하는 회사는 근로자에게 당해연도 기여만큼을 근로자에게 지급하는 동시에 의무가 없어지기 때문에 불입금액만큼 퇴직급여로 계상함

- 급여성 복리후생비의 경우, 인별로 급여 처리되거나 합리적으로 추정 가능한 내역(예: 건강보험료, 국민연금의 회사부담금 등)을 산정함
  - 다만, 명절선물비처럼 인별 추적이 불가능할 경우 관련 비용을 전사인원수로 나누어 계산하여도 합리적일 경우 정보기술 또는 정보보호 금액으로 인정함

- 인건비 산정 시 위의 산정 방법 대신에 개인별 연말정산에서 회사 지급분(총급여)을 개인별 인건비로 산정할 수 있음

1.4 외주 용역비의 산정

- 보안관제, 보안컨설팅, 보안성 지속서비스* 및 유지보수 등을 위한 비용을 외주 용역비로 산정함

※ 정보보호 업무를 수행하는 전문서비스 기업 목록은 한국인터넷진흥원 또는 정보보호산업진흥포털(ksecurity.or.kr)에서 확인할 수 있음

* 보안성지속서비스 : 보안업데이트, 보안정책관리, 위협/사고분석, 보안기술 자문, 보안성 인증(KCMVP 등) 효력 유지 등

- 외주 업체 한 곳에 정보기술서비스와 정보보호서비스를 같이 받을 경우 계약서상 업무 내용 및 용역비가 명확히 정보기술 부문과 정보보호 부문으로 구분이 가능한 경우 인정할 수 있음
  - 외주 용역비 중 정보기술 부문(IT 인프라 운영)과 정보보호 부문(보안관제)에 해당하는 업무가 명확하게 구분되는 경우에는 각각 정보기술부문 투자액과 정보보호부문 투자액으로 분류하여 산정함
  - 계열사 또는 전문 IT업체에 전체 IT업무와 정보보호 업무를 일괄 위탁한 경우에는 계약서 또는 세부 명세서를 통하여 계약금액에서 정보보호부문 투자액을 분리하여 산정함. 만약 일괄 위탁업무에 정보기술부문 업무에 해당하지 않는 업무가 포함된 경우에는 해당 업무만큼의 계약금액을 정보기술부문 투자액에서 제외하고 산정해야 함

- 외주업체 한곳에 정보기술 서비스와 정보보호 서비스를 같이 받을 경우 해당 외주 용역 서비스에 대하여 정보기술 서비스와 정보보호 서비스를 분리하여 계산서를 받아 처리한다면 차후에 정보기술 비용과 정보보호 비용을 분류 산정하는데 도움이 됨

- 외부 정보기술서비스에 정보보호 서비스가 부분적으로 포함되어 있으나 별도로 명확하게 금액 분리가 어려운 경우 해당 서비스 제공업체(예, IDC, 클라우드 서비스 등)의 정보보호 공시 결과를 활용하여 간접적인 방법(간주투자액)으로 정보보호 투자금액을 산출할 수 있음

- 간주투자액은 '외부 정보기술서비스 이용대가'에 서비스 제공 업체의 '정보기술부문투자 대비 정보보호 투자 비율'을 곱하여 산정함(다만 간주투자액 산정방법은 서비스 제공업체가 정보보호 공시를 한 경우에 한함)

※ 외부 정보기술 서비스 이용 시, 정보보호 서비스 이용료의 직접 산정이 가능한 경우, 간주투자는 인정하지 아니하고 직접투자로 인정해 산정함

예 A사가 B호스팅 업체의 호스팅 서비스를 이용하면서 서비스 이용에 따른 대가로 1,000만원을 지불하였고, B호스팅업체의 정보기술부문 투자 대비 정보보호 투자비율이 10%였다면 A사의 정보보호부문 투자액은 자체 정보보호부문 투자액에 100만원(=1000만원x10%)을 더하여 계산

예 A사가 B호스팅 업체의 호스팅 서비스를 이용하면서 서비스 이용에 따른 대가로 1,000만원을 지불하였고, 보안강화를 위해 추가 옵션을 선택해 이에 따른 대가로 20만원을 지불하였으며 B호스팅업체의 정보기술부문 투자 대비 정보보호 투자비율이 10%였다면 A사의 정보보호부문 투자액은 자체 정보보호부문 투자액에 120만원(=1,000만원x10% + 20만원)을 더하여 계산

1.5 특기사항(선택)

- 정보보호 투자비중(%)에 대한 업종별·규모별 착시효과 완화 등을 위해 이용자 등을 대상으로 기업별로 정보보호 투자 현황에 대해 설명 또는 기타 노력 사항을 서술형으로 작성 가능(자율기재 사항)

예 제조기업으로 개인정보 미취급 등의 사유로 타 분야 대비 투자 금액이 낮으나 ▲▲시스템 도입으로 랜섬웨어 등 공격으로부터 정보보안에 만전을 기함

신산업 R&D 등을 위한 IT 투자 규모 확대로 공시해당연도 정보보호 예산 비율이 낮아 보이나 투자 금액 규모로는 전년 대비 **% 상승함

- 국내외 관계사가 정보보호 시스템 등을 공동이용하는 등의 상황으로 인하여 국내 정보보호 투자액을 별도로 구분 및 작성하기 어려운 경우, '특기사항' 항목을 통하여 정보보호에 대한 기업의 노력을 작성하여야 함

예 A회사의 경우, 국내외 관계사가 정보보호 시스템 등을 공동으로 이용하고 있고, 이에 대한 글로벌 차원의 정보보호 투자를 시행하고 있으며, 안정적인 서비스 제공을 위해 정보기술예산의 약 ■%를 정보보호 예산으로 투자 중임

제로트러스트 프로그램 확장, 오픈소스 보안 강화, 보안 인력 양성 등 정보보호를 위해 △년간 000억 달러를 투자함

한국 내 ■■ 서비스 제공을 위해 본사는 ▲▲의 기간통신서비스와 정보보호 시설 등을 활용하고 있어 정보보호 투자 현황 또한 그에 준함

2. 정보보호 인력 현황 산정

- 총 임직원(내부인력), 정보기술부문 인력, 정보보호부문 인력을 산정하기 위한 기초 자료로서 조직도, 원천징수이행상황명세서(신고 인원수 표시)가 필요하며 정보기술부문과 정보보호부문은 내부인력, 외주인력을 포함하여 인원명단을 작성함

정보보호 인력현황 준비자료

준비 자료	작성 내용	비고
조직도	조직별 직무기술	정보기술/정보보호 조직 확인
원천징수이행상황 명세서	공시대상연도의 12개월 (1월부터 12월까지)	총임직원 수 산정
정보기술부문 전담조직 인원수 및 업무내용	내부인력으로 부서, 직무, 입퇴사 일자 정보 (정보기술 전담인력 검토)	조직도 내 위치 표시
정보보호부문 전담조직 인원수 및 업무내용	내부인력으로 부서, 직무, 입퇴사 일자 정보 (정보보호 전담인력 검토)	조직도 내 위치 표시
정보기술/보호부문 직무기술서	전담부서에 속해 있지 않지만 정보기술/정보보호 직무를 전담하고 있는 경우	CEO 또는 CISO 서명
상주/비상주 외주인력 현황	용역명과 월별 투입공수(M/M)를 소숫점 한자리 까지 해서 표시	외주용역 계약서, 계약내용 포함

- 총 임직원 수는 정보보호 공시자의 내부직원만을 대상으로 하며 원천징수이행상황명세서상의 근로소득 인원을 월별로 평균하고 소수점 한자리 이하는 반올림한 인원으로 산정함

- 정보보호 인력은 정보기술부문 인력과 정보보호부문 전담인력을 각각 합산하고 정보보호부문 전담인력을 정보기술부문 인력으로 나누어 산정함

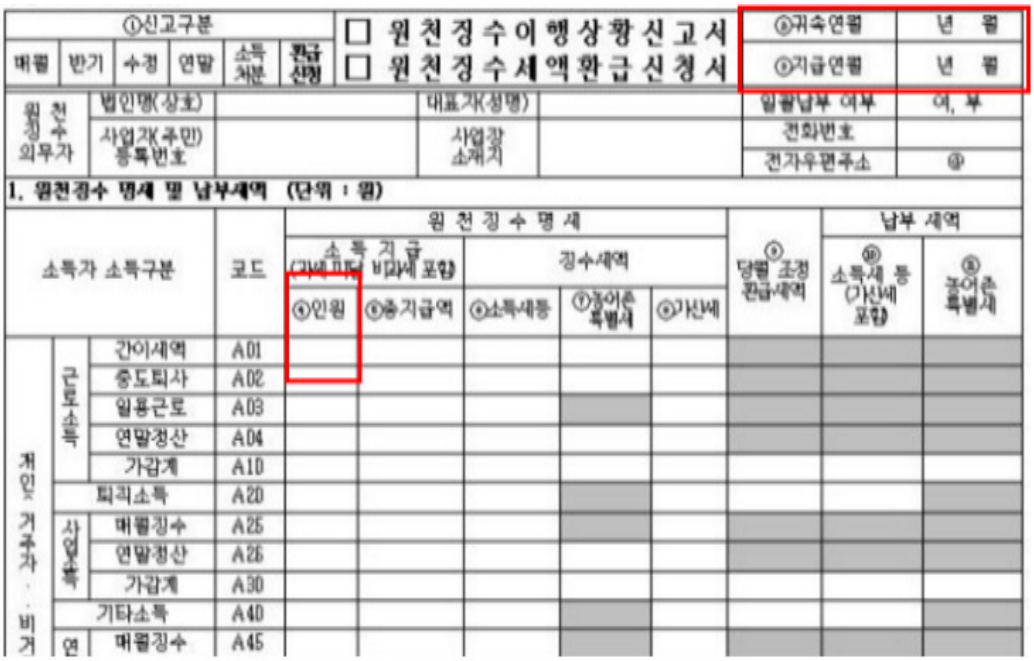
정보보호 인력 현황 산식

$$\text{정보기술부문 인력 대비 정보보호부문 인력의 비율(B/A) (단위 : \%)} = \frac{\text{정보보호부문 전담인력(B) (단위 : 명)}}{\text{정보기술부문 인력(A) (단위 : 명)}} \times 100$$

- 정보기술/정보보호 관련 업무를 하고 있다고 하여도 외부 고객사에 파견되어 상주 또는 비상주로 고객사의 IT 서비스를 목적으로 근무하는 직원은 정보기술/정보보호 인력으로 포함하지 않음

- 타 기업의 정보기술/정보보호부문 외주용역을 수주하는 IT 전문기업의 경우, 특정 프로젝트 파견 기간 이외에 복귀하여 기업 내부 IT업무(정보기술/정보보호)를 수행한 인력은 해당 기간만큼 정보기술/ 정보보호부문 인력에 산입할 수 있음

총 임직원 수 산정 (예시)



① 신고구분: 매월 / 반기 / 수정 / 연말 / 소득처분 / 환급신청

□ 원천징수이행상황신고서
□ 원천징수세액환급신청서

⑥ 귀속연월: 년 월
⑦ 지급연월: 년 월

원천징수의무자: 법인명(상호) / 대표자(성명) / 사업자(주민)등록번호 / 사업장 소재지

일괄납부 여부: 여, 부
전화번호
전자우편주소 ⑫

1. 원천징수 명세 및 납부세액 (단위 : 원)

소득자 소득구분			코드	원천징수 명세					⑨ 당월 조정 환급세액	납부 세액	
				소득 지급 (과세미달, 비과세 포함)		징수세액				⑩ 소득세 등 (가산세 포함)	⑪ 농어촌 특별세
				④ 인원	⑤ 총지급액	⑥ 소득세등	⑦ 농어촌 특별세	⑧ 가산세			
개인 거주자 · 비거	근로소득	간이세액	A01								
		중도퇴사	A02								
		일용근로	A03								
		연말정산	A04								
		가감계	A10								
	퇴직소득		A20								
	사업소득	매월징수	A25								
		연말정산	A26								
		가감계	A30								
	기타소득		A40								
	연	매월징수	A45								

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	월평균
내부인력	104	106	107	106	100	100	100	101	104	101	100	89	101.5

- 정보기술부문 인력은 정보기술 업무를 전담하는 내부직원, 외부직원의 공시대상연도 월평균 인원으로 집계되고, 정보보호 전담인력은 정보보호 업무를 전담하는 내부인력(정규직, 계약직)과 외주인력(사내파견, 외부전담)의 월평균 인원으로 집계함

정보보호 인력 현황 (예시)

구분		인원수	근거 자료
총임직원(내부인력)		101.5 명	원천징수이행상황명세서
정보기술부문전담인력	내부인력	32.5 명	
	외주인력	11.0 명	
	소계	43.5 명	
정보보호부문전담인력	내부인력 (정규직+계약직)	2.2 명	
	외주인력	2.0 명	
	소계	4.2 명	
정보기술부문 인력 대비 정보보호부문 전담인력의 비율		9.7 %	

- 정보보호 인력현황은 조직도 및 외주용역 계약을 검토하여 정보기술/정보보호부문 인력현황을 파악하고 정규직, 계약직, 외부직원으로 구분하며 필요시 부서 및 개인의 직무기술서와 외주 용역 계약서 등이 필요함

2.1 정보기술부문 및 정보보호부문 내부인력

내부인력 요건

구분			세부 내용
내부 인력	정규직	기간의 정함이 없는 근로자	• 「근로기준법」에 따라 근로계약을 체결한 근로자 중 다음 '기간제 근로자', '단시간 근로자', '일용 근로자'에 해당하는 사람을 제외한 근로자
	계약직	기간제 근로자	• 「기간제 및 단시간근로자 보호 등에 관한 법률」 제2조제1호에 따른 '기간제근로자' 중 1년 이상 계약된 근로자

※ 기간의 정함이 없는 계약직(무기계약직)의 경우, 일반계약직과 달리 기간의 정함이 없지만 본래 소속이 계약직군에 포함되기 때문에 계약직으로 인정

- 정보보호 공시자가 내부 규정에 따라 IT 기획·개발·운영·정보보호 등 정보기술 전담조직을 운영하는 경우에는 해당 부서 전체 인력을 정보기술부문 인력으로 산정함

- 정보보호 공시자가 내부 규정에 따라 정보보호 전담조직을 운영하는 경우에는 해당 부서 전체 인력을 정보보호부문 인력으로 산정하며 정보기술부문 인력명단에서 “정보보호” 항목에 체크하여 작성함

  - 직원이 많아 개인별 구분이 어려운 경우 조직별로 정보기술/정보보호 업무조직을 구분 표시하고 해당 조직 인원 전체를 정보기술/정보보호부문 인력으로 산정함

조직별 정보기술/정보보호부문 인력현황 (예시)

조직명		조직업무	정보기술	정보보호	월별 인원수											
본부/실	부/팀				1	2	3	4	5	6	7	8	9	10	11	12
	A팀	시스템 운영	○	△												
	B팀	S/W 개발	○													
	C팀	정보보호센터	○	○												
	D팀	시스템 유지보수	○													
	E팀	콘텐츠 개발	△													
⋮	⋮	⋮	⋮	⋮												

※ 조직 내 일부 인원만 정보기술/정보보호 업무에 해당할 경우에는 별도 표시하고 해당 인력을 인력별로 인력 현황표에 구분하여 표시함

인력별 정보기술/정보보호부문 인력현황 (예시)

조직명	직급	성명/사번	수행업무	직무	직렬	입사일	퇴사일	정보기술	정보보호
D팀	부장	김**	유지보수 총괄	IT				○	
D팀	과장	박**	시스템 모니터링	보안				○	○
D팀	사원	이**	장애 처리	IT				○	
⋮	⋮	⋮	⋮	⋮	⋮			⋮	⋮

※ 입사일과 퇴사일은 공시대상연도에 근무한 이력을 파악하기 위한 것으로 이를 바탕으로 월별 근무인력을 산정할 수 있음

- 정보기술/정보보호부문 전담부서 소속 인력이 아니더라도 정보기술/ 정보보호 부문 업무를 전담(100%)하여 일하고 있는 인력은 최고경영자 또는 임원급(CISO)이 확인(결재, 서명 등)한 기업의 공식 문서(직무기술서 등)를 근거로 정보기술/정보보호부문 인력에 포함시킬 수 있음

- 정보기술/정보보호부문 인력이 매월 동일한 인원으로 유지되지 않고 신규 입사, 부서 이동, 퇴사 등의 사유로 변경이 발생한 경우에는 월별 인력을 파악하여 12개월간의 평균 인력을 산정함

정보기술/정보보호부문 내부인력 산정 (예시)

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	월 평균
정보기술부문	32	32	32	32	32	33	33	33	33	33	33	32	32.5명
정보보호부문	6	5	5	6	5	4	4	5	6	6	5	5	5.2 명

※ 정보보호부문 인원 중 1월 16일 입사하여 12월 15일 퇴사한 자의 경우 1월에는 0.5명으로 산정되며 2월~11월은 1명으로, 12월은 0.5명으로 산정되는 것임

정보기술부문 및 정보보호부문 주요업무

부문	주요업무	업무 예시
정보기술부문	IT 기획 및 관리	• IT 전략 수립·관리 및 IT관련 규정·지침 관리
		• IT 예산 및 자원계획 수립·관리와 배정·집행
		• IT 자원 도입 검토 및 구매 관리
		• IT 인력 인사·성과관리 및 교육 계획 수립·시행
		• IT 아키텍처 정책표준 수립·관리 및 IT 아키텍처 현행화
		• IT 프로젝트관리 및 통합품질관리시스템운영
		• 형상관리정책 수립·운영 및 프로그램 형상 관리
		• 테스트방법론과테스트계획관리및테스트품질관리
		• IT 감사 및 IT 감리 기획·실시 등
	IT 개발 및 유지 보수	• 전산개발 범위와 처리기능 정의, 개발 세부계획 수립
		• 시스템 상세업무요건 정의 및 시스템 인터페이스·데이터 분석
		• 입출력자료, 업무처리 단위별프로그램, 오류코드 등 설계
		• 프로그램 구현 및 산출물 작성

부문	주요업무	업무 예시
정보 기술 부문	IT 개발 및 유지 보수	• 테스트수행
		• 프로그램 이행 및 시스템 적용
		• 프로그램 유지보수 등
	IT 운영 및 보수정비	• 메인프레임 운영체제, 스토리지 등 운영·보수정비 및 데이터베이스 관리
		• 서버 운영체제, 미들웨어, 스토리지 등 운영·보수정비 및 데이터베이스 관리
		• 네트워크 운영 및 네트워크 장애 관리
		• 콜센터시스템 및 콜센터교환기 운영
		• 단말기, 자동화기기 등 시스템 개발 및 운영
		• 단말기, 주변기기 등 업무용 전산기기 배정 설치·운영
		• 전산기기 자산관리 및 장애관리(보수정비 포함)
		• 단말기, 자동화기기, 인터넷, 콜센터 등 채널 통합시스템 관리·운영
		• 대내·외 시스템간 연계(Interface)·중계시스템 관리·운영
		• 전산센터(종합상황실 포함) 운영 및 전산백업·소산매체 관리·운영
		• 재해복구센터(전산백업시스템 포함) 관리·운영
		• IT 업무지속성계획 수립·관리 및 업무지속성훈련 실시
		• 시스템 모니터링 등 IT 서비스 관리 시스템(ITSM) 운영
		• 센터집중처리·배치 처리, 보고서 추출 등 일괄전산작업 처리 등
정보 보호 부문	정보보호 기획 및 관리	• 내부 정보보호 정책 수립 및 정보보호 관련 규정·지침 제·개정
		• 정보보호 교육 계획 수립 및 교육 실시
		• 정보기술부문 관련 정보보호 대책 수립 및 시행
		• 모의해킹, 디도스 대응훈련 등 비상대응훈련 계획 수립 및 실시
		• IT 내부 통제(법규준수 포함) 관리
		• 취약점 분석·평가 및 그 이행 계획 수립
		• 모의해킹, 디도스 대응훈련 등 비상대응훈련 계획 수립 및 실시
	개발 및 유지보수	• 정보시스템 개발시 정보보호 요구사항 정의
		• 정보보호 요구사항 검토 및 시험, 개선조치 이행
		• 정보시스템 및 정보보호 시스템 시험 운영

부문	주요업무	업무 예시
정보보호부문	개발 및 유지보수	• 정보시스템 소스 프로그램 이력 관리
		• 정보시스템 및 정보보호 시스템 운영 이관 및 통제절차 이행
		• 정보보호 아키텍처 유지관리
	정보보호 운영	• 취약점 분석·평가 시행
		• 정보기술부문 관련 보안성 검토
		• 모의해킹, 디도스 대응훈련 등 비상대응훈련 실시
		• 침해시도에 대한 실시간 보안 관제 및 통합보안관제시스템 운영
		• 외부 직원 출입 통제 및 노트북, USB 등 반출·입 통제 시스템 구축·운영
		• 침해방지·대응시스템 구축·운영
		• 시스템 접근 통제, 권한 관리 및 사용자 인증 관련시스템 구축·운영
		• 고객 정보 보호 및 정보 유출 방지 시스템 구축·운영 등

2.2 정보기술부문 및 정보보호부문 외주 인력

- 정보기술부문 인력 및 정보보호부문 인력은 기업에 상근하는 내부인력 및 외주인력으로 한정하며, 공시대상연도의 월 평균 인원으로 산정함
  - (외주인력) 기업과의 외부주문, 하도급 계약 등에 따라 업무를 처리하는 업체에 소속된 상시 종업원으로서 파견 근로자 및 사내하도급 근로자를 포함

외주인력 요건

구분		세부 내용
외주인력	파견 근로자	• 「파견근로자보호 등에 관한 법률」 제2조제5호에 따른 “파견근로자”
	사내하도급 근로자	• 「사내하도급근로자 근로조건 보호 가이드라인」에 따른 “사내하도급 근로자”

관련근거

「**근로기준법**」 **제2조(정의)** ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. "근로자"란 직업의 종류와 관계없이 임금을 목적으로 사업이나 사업장에 근로를 제공하는 사람을 말한다.
2.~8. (생략)
9. "단시간근로자"란 1주 동안의 소정근로시간이 그 사업장에서 같은 종류의 업무에 종사하는 통상 근로자의 1주 동안의 소정근로시간에 비하여 짧은 근로자를 말한다.

「**기간제 및 단시간근로자 보호 등에 관한 법률**」 **제2조(정의)** 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "기간제근로자"라 함은 기간의 정함이 있는 근로계약(이하 "기간제 근로계약"이라 한다)을 체결한 근로자를 말한다.

「**파견근로자보호 등에 관한 법률**」 **제2조(정의)** 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1.~4. (생략)
5. "파견근로자"란 파견사업주가 고용한 근로자로서 근로자파견의 대상이 되는 사람을 말한다.

사내하도급근로자 근로조건 보호 가이드라인 II. 정의
1.~3. (생략)
4. "사내하도급 근로자"란 수급사업주가 사내하도급계약을 이행하기 위해 고용한 근로자를 말한다.

- 외주 용역계약을 통하여 정보보호 공시자의 정보기술/정보보호부문 업무를 상시 전담하는 인력은 외주인력으로 산정하며 시스템 개발, 보안 컨설팅 등의 단기 외주 용역 인력*은 포함하지 않음

  - 다만, 단기 외주 용역이라 하더라도 분기/반기/년 등 일정단위로 반복해서 이뤄지는 외주 용역은 정보기술/정보보호부문 업무로 인정함

  * 단기 외주 용역은 용역기간이 1년 이내이면서 단발성으로 이루어지는 모든 용역을 말함

예 계약서상 투입공수가 10명으로 되어 있다면, 실제로는 10명 초과(백업 목적 등으로) 또는 미만으로 수행하고 있는 경우에도 계약서에 기재되어 있는 10명만을 인정함

외주인력 포함 기준

구분	기준 내용
1	• 기업의 정보기술부문 업무 수행을 위한 정보화 기획, 정보통신 인프라 운영, 정보보호 등의 정보기술부문 업무 종사자를 포함
2	• 정보통신 인프라의 하드웨어 또는 소프트웨어 등의 유지보수를 수행하기 위한 제조사의 상시 운영 기술인력을 포함
3	• 외주인력 중 월·주 단위 등 부정기적이거나 일시적인 인력은 제외 (예시) 정보시스템 개발 프로젝트를 수행하기 위하여 상주하는 외주업체의 정보기술부문 업무 종사자는 제외

● 정보보호 공시자의 IT 서비스를 위해 근무하는 외주인력은 사내파견 인력과 외부전담 인력으로 구분되며, 외주 용역 계약에 명시되어 있는 인원수를 정보기술/정보보호부문 인력으로 인정함

- 외주인력(사내 파견) : 정보보호 공시자(공시기업)에 파견 나와 정보기술, 정보보호 업무를 상근 전담하는 인력

> **예** 일반적인 외주용역 형태로서 인프라운영 아웃소싱, 보안관제 아웃소싱 등

- 외주인력(외부 전담) : IT 전문회사(또는 계열사)가 정보기술과 정보보호를 턴키 아웃소싱하는 경우, 해당 용역비 범위 내에서 정보보호 공시자의 정보기술, 정보보호 전담 인력을 구분

> **예** 계열사에 IT 업무 턴키 위탁용역

외주용역별 정보기술/정보보호부문 산정 (예시)

협력사명	담당부서	담당자	용역명/수행업무	정보기술	정보보호	월별 인원수											
						1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
B회사	C팀	김**	일반IT	○		2	2	2	2	2	2	2	2	2	2	2	2
B회사	C팀	이**	보안업무	○	○	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
C회사	C팀	이**	보안관제	○	○	3	3	3	4	4	3	3	4	5	6	4	4

정보기술/정보보호부문 외주인력 산정 (예시)

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	월평균
정보기술부문	10	10	11	11	11	11	11	11	12	12	11	11	11.0명
정보보호부문	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0명

2.3 CISO/CPO 지정 현황

- 기업별 정보보호 최고책임자(CISO), 개인정보 보호책임자(CPO)의 직책, 임원여부, 겸직여부 및 대표적인 내·외부 활동 건수 등을 작성함
  - '특기사항'을 활용하여 공시대상연도의 CISO·CPO의 정보보호 관련 대표적인 대내외 발표, 학술지 기고, 위원회 운영, 외부 자문, 자격 취득 등 상세 활동을 기재할 수 있음

CISO·CPO 지정 현황 작성(예시)

CISO/CPO지정현황

구분	직책	임원 여부	겸직 여부	주요 활동
CISO	본부장	O	X	5건
CPO	실장	X	CIO	3건

특기사항	CISO 주요 활동 : △△제도 개선 자문위원 참여(○○. ○○.~○○. ○○.) CPO 주요 활동 : ■■학술 발표(주제 : ------)

2.4 특기사항(선택)

- 정보보호 인력 비중(%)에 대한 업종별·규모별 착시효과 완화 등을 위해 이용자 등을 대상으로 기업별로 정보보호 인력 현황에 대해 설명 또는 참고할 사항을 서술형으로 작성 가능(자율기재사항)

예

당사는 IT 기업으로 정보보호 인력이 전 직원의 **%이며, 일부 정보보호 업무는 정보기술부문 인력이 겸임하여 수행하고 있어 전담인력 규모가 상대적으로 낮음

전문적이고 안전한 정보보호 서비스를 제공하고자 정보보호부문 인력을 자체 운영하지 않고, IT전문기업의 ▲▲서비스 이용계약을 체결하여 운영 중

- 국내외 관계사가 정보보호 시스템 등을 공동이용하는 등의 상황으로 인하여 국내 정보보호 인력을 별도 구분 및 작성이 어려운 경우, '특기사항' 항목을 통해 정보보호에 대한 기업의 노력을 작성해야 함

예

A회사의 경우 글로벌 차원에서 정보보호 체계를 구축 및 운영 중에 있음.

전 세계 ○○개 지역에서 ○○개 이상 서비스를 제공하기 위하여 약 ○,○○○명의 정보보안 전문가를 활용하여 사이버공격 위험을 대비함.

한국 내 ■■ 서비스 제공을 위해 본사는 ▲▲에게 정보기술/정보보호부문을 아웃소싱하고 있어, 전담인력의 규모와 수준이 ▲▲에 준함

3. 정보보호 관련 인증, 평가, 점검 등에 관한 사항

- 정보보호 및 개인정보보호 관리체계 인증, 정보보호 준비도 평가, 클라우드 서비스 보안인증(CSAP) 등 기업이 취득한 국내외 정보보호 관련 주요 인증, 평가, 점검을 위한 기업의 노력을 작성함
  - 국제 인증 제도에는 ISO/IEC 27001, ISO/IEC 27017, CSA STAR, SOC 등이 있음
  - 정보보호 관련 인증, 평가, 점검 등을 취득하지 않은 경우, '정보보호 공시 서식' 문항에 '해당사항 없음'으로 표기함

- 정보보호 공시자가 취득한 정보보호 인증, 평가, 점검에 대한 인증서, 평가서, 점검결과서 등을 준비하고 인증서별 유효기간과 발행기관 등을 정리하여 인증 유효기간이 공시기간 내에 있을 경우 정보보호 관련 인증, 평가, 점검 현황 목록으로 작성함

- 인증의 범위는 법정 인증(강제 인증, 임의 인증)과 민간 인증이 포함되며, 민간 인증의 경우에는 표준 및 인증 요구조건 공개와 서면(시험보고서 포함)으로 요구조건 적합 사실을 보증하는 2가지 조건을 충족한 경우에 정보보호 인증, 평가, 점검 실적에 포함될 수 있음

국내·외 정보보호 관련 인증 현황 (예시)

인증 종류	인증제도 설명	비고
정보보호 및 개인정보보호 관리체계 인증서	• 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 증명하는 제도 * 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(과학기술정보통신부, 개인정보보호위원회 고시)	국내
클라우드 서비스 보안인증서	• 클라우드컴퓨팅서비스 사업자가 제공하는 서비스에 대해 정보보호 기준의 준수여부를 평가·인증하는 제도 * 클라우드컴퓨팅서비스 정보보호에 관한 기준(과학기술정보통신부 고시)	국내
정보보호 준비도 등급 평가서	• 보안투자 비율 및 인력 조직 확충, 법규준수 등 기업의 정보보호 준비 수준을 평가하여 일정 등급을 부여하는 제도 * AAA~B 5등급, 개인정보보호지표 만족시 인증마크에 'P' 부여	국내
데이터베이스 품질 인증서(데이터보안)	• 기업·기관에서 중요 데이터나 개인정보가 저장되어진 데이터베이스를 대상으로 데이터보안에 대한 기술요소 전반을 심사, 심의하는 제도 *데이터베이스 접근 제어, 암호화, 작업결재, 취약점 분석	국내
ISO/IEC 27001	• 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 정보보호 관리체계 국제규격 인증	국외
ISO/IEC 27701	• 국제표준화기구(ISO) 및 국제전기기술위원회(IEC) 에서 제정한 EU GDPR 등 전세계의 개인정보보호 요구사항을 충족하는 글로벌 개인정보 관리체계 국제규격 인증	국외
ISO/IEC 27799	• 국제표준화기구(ISO) 및 국제 전기기술위원회(IEC)에서 제정한 의료정보보호 관리체계 국제규격 인증	국외
ISO/IEC 27017	• 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 클라우드 서비스 정보보호 관리체계 국제규격 인증	국외
CSA STAR	• 영국표준협회와 미국 클라우드시큐리티 얼라이언스가 공동으로 평가하는 클라우드서비스 정보보호 인증	국외
FedRAMP	• 클라우드 제품 및 서비스에 대한 보안평가, 인증 및 지속적인 모니터링에 대한 표준화된 연방 보안 인증 프로그램	국외
SOC	• 국제인증업무기준에 따라 서비스의 안정성과 내부 통제 수준을 평가하는 제도	국외

* 예시 이외의 다른 정보보호 관련 인증·평가제도 기재 가능

국내·외 정보보호 인증, 평가, 점검 공시 작성 (예시)

공시 항목	공시 내용
국내·외 인증·평가·점검 현황	• 정보보호 및 개인정보보호 관리체계 인증(유효기간 : ****. **. **.~****. **. **.) – △△ 서비스의 정보보호 및 개인정보보호를 위한 일련의 활동이 인증기준에 적합함을 보증 • 클라우드 서비스 보안 인증 – □□ 데이터 센터 각 운영에 대한 안정성 확보 및 서비스 제공 • ISO/IEC 27001 – 정보보호 수준의 지속적인 개선 및 이용자 요구사항 충족을 보장하는 국제인증 • SOC 2, 3 – 이용자의 개인정보보호에 중점을 두고 서비스 안정성과 내부통제 수준을 평가하는 국제인증 ※ SOC 3의 경우, 국내에 **개 기관만이 인증 획득

4. 정보보호를 위한 활동 현황

- 정보보호 투자 활성화 실적, 임직원의 정보보호 인식 제고 교육 등 기업의 정보보호를 위한 대내외 활동을 작성함

- 사이버 위협정보 분석·공유시스템(C-TAS)* 활용 등 협력 활동, 사이버 위기 대응을 위한 모의훈련 참여**, 업무지속계획(BCP)*** 수립 등이 정보보호 활동에 해당함

  * 한국인터넷진흥원에서 운영 중인 사이버 위협정보의 수집, 분석 및 공유 플랫폼(일반회원과 공유회원으로 구분)

  ** 한국인터넷진흥원에서 민간 기업의 침해사고 대응체계 객관적 점검과 임직원 보안인식 제고를 위해 매년 정기적으로 실시하고 있는 모의훈련

  *** Business Continuity Plan : 재난 발생시 업무 연속성을 유지하기 위한 계획으로 랜섬웨어 등 사이버공격 예방 대책, 사고시 확산단계별 대응계획 등 반영

- 「개인정보 보호법 시행령」제30조, 제48조의2에서 규정하고 있는 개인정보의 안전성 확보 조치를 위한 활동 등 공시대상연도에 수행한 내·외부활동도 공시 가능함

구분	정보보호 활동 세부내용
개인정보의 안전성 확보 조치	1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

- 정보보호 공시자가 공시대상연도에 이행한 정보보호 활동에 대하여 활동을 증명할 수 있는 문서나 메일, 홈페이지 화면 등을 근거로 작성함

- 정보보호 활동에 대하여 연간 수행 횟수(수행주기)를 표기하고 각 세부 활동 건수를 집계하여 정보보호 활동 공시 자료를 작성함

  - 정보보호 활동내역이 없는 경우, '정보보호 공시 서식' 문항에 '해당사항 없음'으로 표기함

정보통신서비스 이용자의 정보보호 활동 (예시)

구분	정보보호 활동 세부내역	건수
정보보호 투자 활성화 실적 및 정보보호 관련 활동	• 사이버위협 정보 분석공유 시스템(C-TAS) 참여(일반 또는 공유회원) • 업무지속계획(BCP) 수립 • 국내외 정보보호 기업과 양해각서(MOU) 체결 • 정보보호 관련 수상 내역(ICT 대상, 공시 우수기업 지정) • 사이버위험 배상책임보험 가입 • 정보보호 관련 국내외 콘퍼런스 참가(세션 발표, 전시 부스 설치 등)	6건
임직원의 정보보호 인식제고 교육 및 지원	• 사이버 위기대응 모의훈련 실시(자체 점검, KISA 주관훈련 등) • 임직원 정보보호 및 개인정보보호 수준진단 • 월별 임직원 보안의식 제고 활동 추진(정보보호의날, 자가진단 등) • 임직원 대상 사내 정기 정보보호 교육과정 개설	4건
정보보호 전담인력 관리 활동	• 사내 우수보안사례 발굴 및 내부 시상 • 정보보호 공모(모의해킹대응대회 등), 세미나 개최 등 지원 • 취약점 제보 및 보상제도 도입	3건
이용자 정보보호 인식 제고활동	• 정보보호 취약계층 대상 보안인식 제고 캠페인 실시 • 이용자 참여형 정보보호 콘텐츠 마련 • 정보보호 생활 실천수칙 마련 및 배포 • 대표 홈페이지 팝업 및 공지사항 내 실천수칙 게시	4건
계	17건	

Ⅲ 공시 이행절차 및 사후검증

정보보호 공시 세부 절차

① 정보보호 현황 작성

- 정보보호 최고책임자(CISO)의 주관 하에 정보보호 전담부서/IT 부서 및 회계부서, 인사부서 등이 협업하여 「정보보호 공시에 관한 고시」의 [별표 3] 정보보호 공시내용 양식에 따라 정보보호 현황을 작성함

② 정보보호 현황 승인

- 정보보호 공시자의 최고경영자는 확정된 정보보호 현황을 최종적으로 확인하고 승인·결재함

- 최고경영자의 승인·결재를 통하여 정보보호 최고책임자가 주관하여 공시하는 정보보호 현황은 기업의 책임 하에 제공되는 사항임

③ 정보보호 현황 제출

- 정보보호 공시자의 최고경영자가 승인·결재한 정보보호 현황을 과학기술정보통신부 전자공시시스템(이하 'ISDS')을 통하여 입력하며, 불가피한 경우에는 한국인터넷진흥원에 전자파일 형태로 제출*가능

  * 한국인터넷진흥원 정보보호 공시 담당자 이메일 주소 : isds@kisa.or.kr

  - 입력 또는 제출할 때 「정보보호 공시에 관한 고시」의 [별표 4] 정보보호 공시 내용 사후검증 동의서도 같이 제출하여야 가능

- 「정보보호 공시에 관한 고시」의 [별표 4] 사후검증 동의서 대신 회계법인이나 정보시스템 감리법인으로부터 공시 내용에 대해 사전점검을 받고 사전점검 확인서를 제출하는 것도 가능함(선택사항)

- 자율적으로 정보보호 현황을 작성한 상장기업은 한국거래소 자율공시시스템(KIND)에도 정보보호 현황을 자율공시 할 수 있음(정보보호산업법 제13조 제2항에 따른 의무대상자는 해당되지 않음)

※ KIND 공시의 경우, 정보보호 공시자는 사유발생일 다음 날까지 정보보호 현황을 KIND에 입력하고 최고경영자가 공시를 승인·결재한 정보보호현황 보고서를 첨부(공시유형 : 자율공시, 정보보호)

관련근거

유가증권시장 공시규정 시행세칙 제8조(자율공시) ① 규정 제28조에서 "세칙에서 정하는 사항"이란 다음 각 호의 어느 하나에 행하는 사항을 말한다.
1.~16. (생략)
17. 「정보보호산업의 진흥에 관한 법률」제13조제1항에 따른 정보보호 현황

코스닥시장 공시규정 시행세칙 제13조(자율공시) ① 규정 제26조에서 "세칙에서 정하는 사항"이란 다음 각 호의 어느 하나에 해당하는 사실 또는 결정을 말한다.
1.~15. (생략)
16.「정보보호산업의 진흥에 관한 법률」제13조제1항에 따라 정보보호 현황을 공개하기로 결정한 때

- 차후 사후 검증 대상에 선정되었을 경우를 대비하여 정보보호 현황 작성에 사용되었던 자료는 별도 보관 또는 기록이 필요함

  - 회계 및 인사자료의 경우 사후검증을 대비하여 각 사안별(자산대장, 비용원장, 인력현황(외주 포함) 등) 자료를 정보기술부문 및 정보보호부문으로 분류한 집계표를 작성 보관하여야 함
  - 산출된 정보보호현황에 대해 회계법인이나 정보시스템감리법인에게 사전점검을 받아 사전점검 확인서를 같이 제출할 경우에는 사후검증 대상에서 제외됨

④ 정보보호 현황 확인 및 게시

- 한국인터넷진흥원은 정보보호 공시자가 제출한 정보보호 현황을 확인함. 이때 정보보호 현황 내용 및 최고경영자의 승인 여부 누락 등을 확인하며, 누락된 정보가 있을 시 정보보호 공시자에게 알림

⑤ 공시 내용의 변경

- 공시내용 변동으로 수정이 필요한 경우에는 변동 내용에 대해 최고경영자 확인 후 변경 공시할 수 있음

  - 다만, 한국거래소 KIND 자율공시의 경우에 50%이상 변경 공시하게 되면 불성실 공시(공시 번복)로 인한 제재 조치(벌점 부과)를 받을 수 있음

⑥ 공시 이행 후속조치

- 공시를 이행한 기업은 이행을 확인한 날로부터 「정보보호 공시에 관한 고시」의 [별표 5]에 따른 정보보호 공시 이행 표시를 할 수 있음. 다만, 공시 이행 표시를 사용하는 경우에 공시 유효기간을 함께 표시하여야 함

> **예** 공시 이행 표시를 기업의 홈페이지에 게시할 경우 공시 이행 표시에 마우스가 위치하거나 클릭할 때 유효기간이 표시되도록 설계하거나, 종이문서에 표시할 경우에는 공시 이행 표시 아래나 옆에 유효기간을 표시할 수 있음

공시내용의 사후검증

1. 개요

- 정보보호 공시 내용의 투명성, 신뢰성 확보를 위해 과학기술정보통신부는 한국인터넷진흥원을 통하여 공시 이행 기업의 공시 주요 내용의 정확성을 검증할 수 있음

  - 다만, 회계법인이나 정보시스템 감리법인으로부터 공시 내용에 대해 사전점검을 받고 확인서를 제출한 기업은 사후 검증 대상에서 제외됨

- 사후검증은 기업의 협조를 전제하에 이루어지는 것으로 기업이 정확하고 쉽게 정보보호 현황을 산출하도록 행정지도하기 위함이며, 기업이 부담하는 비용은 없음

2. 사후 검증 절차

① 사후검증 대상 선정

- 컨설팅을 받은 기업 또는 회계 법인이나 정보시스템 감리법인으로부터 공시 내용에 대해 사전점검을 받고 확인서를 제출한 기업을 제외한 기업은 사후 검증대상이 될 수 있음
  - 대상기업에게 사후 검증 대상이 되었음을 통보하고 일정을 협의하여 검증을 진행함

② 공시 점검단 구성

- 공시 점검단은 공시제도에 대한 높은 이해도와 정보보호현황 자료에 대해 판단기준을 제시할 수 있는 전문가로 구성·운영함

구분	자격요건
회계사	• 공인회계사법에 의한 공인회계사로 등록 된 회계사
정보시스템감리사	• 전자정부법에 의한 감리원 자격을 취득한 자
정보보호 전문가	• ISMS-P 인증심사원, 정보보호 컨설턴트 등 정보보호 관련 업계 6년 이상 종사자

③ 사후검증 실시

- 사후 검증 대상으로 선정된 기업은 정보보호현황 산정을 위해 사용되었던 자료들을 준비하여 사후 검증에 대비함

- 공시 점검단은 업체가 준비한 자료를 검토하여 기업이 「정보보호 공시에 대한 고시」에 따라 적정하게 정보보호현황을 산정하였는지를 확인하고 검토하며 그 결과를 보고서로 작성하여 한국인터넷진흥원에 제출함

구분	검증기준
투자액	• 인건비, 자산대장, 비용원장 등 투자액 현황을 증명할 수 있는 자료 검토(투자액의 20% 미만 오차 범위 허용)
인력	• 직무기술서, 조직도, 원천징수이행상황명세서, 외주용역 계약서 등 인력현황을 증명할 수 있는 자료 검토(인력의 20% 미만 오차 범위 허용)
인증, 평가, 점검사항	• 정보보호 공시자가 취득한 정보보호 인증, 평가, 점검에 대한 인증서, 평가서, 점검결과서 확인
정보보호활동	• 정보보호 활동 증빙자료(활동사진, 회의록, 활동 결과물 등) 검토

④ 사후 검증 결과 확인 및 통보

- 한국인터넷진흥원에서는 사후 검증 결과보고서를 검토하여 기업에게 통보한다. 공시 점검단의 결과보고서에서 허위공시 등으로 판단한 경우는 그 내용을 심의위원회에 전달하여 최종심의 및 의결하도록 하고, 정정 공시가 이루어질 수 있도록 기업을 지원함

⑤ 허위 공시에 대한 조치

- 과학기술정보통신부장관은 심의위원회의 심의·의결 결과에 따라 정보보호 공시자의 고의 또는 과실로 허위 사실을 공시한 경우, 별도의 시정조치를 요구할 수 있음

- 시정조치 요구에 응하지 않아 공시가 취소되는 경우, 공시 혜택은 취소되며, 따라서 정보보호 및 개인정보보호 관리체계 인증 수수료의 할인받은 금액도 반납해야 함
  - 또한 한국거래소 상장공시시스템(KIND)에 공시한 경우 거래소 공시 규정에 따른 공시위반 제재 조치를 받을 수 있음

정보보호 공시 이행 혜택 및 연계 정책

1. 정보보호 및 개인정보보호 관리체계 인증 수수료 할인(자율공시에 한함.)

- 정보보호 현황을 공시한 경우에는 공시 시점부터 1년 내에 인증심사(최초·갱신·사후) 수수료 30% 할인 가능함

> **예** 2021년 3월 1일에 자율적으로 정보보호 공시를 이행할 경우, 2020년의 회계 내용으로 정보보호 현황을 작성하여 공시해야 하며, 혜택 효력은 2022년 2월 말까지 유지되고 효력 기간 안에 진행하는 최초 심사, 사후 심사, 갱신 심사에 모두 할인 혜택이 적용됨

- 정보보호 공시자가 정보보호 현황을 공시한 후 1년 이내에 정보보호 및 개인정보보호 관리체계 인증 심사 계약을 체결하였다면 인증심사 수수료 산정 내역서에서 '수수료 감면'란에 있는 정보보호 공시기업을 선택하여 심사기관에 제출하면 수수료를 30% 할인받을 수 있음

정보보호산업의 진흥에 관한 법률

제13조(정보보호 공시) ③ 제1항에 따라 정보보호 현황을 공개한 자가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항에 따른 정보보호 관리체계 인증을 받고자 하는 경우에는 납부하여야 할 수수료의 100분의 30에 해당하는 금액을 할인받을 수 있다.

정보보호 공시에 관한 고시

제9조(정보보호 관리체계인증 수수료 할인) ① 법 제13조제3항에 따른 정보보호 관리체계인증(정보보호 및 개인정보보호 관리체계인증 포함) 수수료 할인을 받고자 하는 정보보호 공시자는 다음 각 호의 요건을 충족하여야 한다.

1. 제3조에 따른 공시일 것
2. 제13조제1항에 따른 공시 취소 사유에 해당하지 않을 것

② 제1항에 따른 수수료 할인은 제5조제2항의 이행확인서 유효기간 내에 진행된 정보보호 관리체계인증의 최초심사, 사후심사, 갱신심사 등에 대한 인증 수수료에 대하여 적용한다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

제21조(수수료의 산정) ① 인증 수수료는 별표 6의 인증 수수료 산정 및 심사원 보수 기준을 적용하여 산정한다.

② 심사수행기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다.

③ 심사수행기관은 신청인이 다음 각 호의 어느 하나에 해당하는 경우 수수료를 감면 또는 조정할 수 있다.

1. 「중소기업기본법」제2조제2항에 따른 소기업
2. 제20조에 따른 인증심사 일부 생략 신청을 하는 경우
3. 「정보보호산업의 진흥에 관한 법률」제13조에 따라 정보보호 현황을 공시한 자
4. 그 밖에 신청인과 협의하여 수수료 조정이 필요하다고 판단되는 경우

2. 정보보호 투자 우수기업의 표시(자율·의무공시)

- 전자공시시스템(ISDS)에 정보보호 현황을 공시할 시 ISMS 인증을 획득하였거나 정보보호 준비도 평가 AA 등급 이상일 경우에는 “정보보호 투자 우수기업” 마크를 전자공시시스템에서 아래와 같이 별도로 표시하여, 기업이 정보보호 투자를 활발히 진행하고 있다는 것을 보여줄 수 있음

전자공시시스템(ISDS) 공시 예시

3. 정보보호 공시 우수 기관·단체의 선정(자율·의무공시)

- 공시 성실성 및 다양한 정보보호 노력 평가를 통해 정보보호 공시 우수 기관·단체를 선정하며 과학기술정보통신부장관에 의한 표창을 수여함

  - 표창을 받은 날로부터 1년 동안 「정보보호 공시에 관한 고시」에 따라 공시 내용의 사후 검증 대상 면제 등의 혜택을 받을 수 있음

Ⅳ FAQ

Q01 정보보호 공시는 언제까지 해야 하나요?

정보보호산업의 진흥에 관한 법률(이하 '정보보호산업법') 시행령 제8조제6항에 따라 매년 6월 30일까지 과학기술정보통신부장관이 운영하는 전자공시시스템(ISDS)에 정보보호 현황을 제출해야 합니다.
정보보호 현황은 공시년도의 직전년도(공시대상연도)에 해당하는 회계 및 인증 내용을 바탕으로 작성하며, 매년 정기적으로 공시를 이행하고 이용자, 투자자 보호를 목적으로 신속하게 정보를 전달하기 위해 신속하게 이행하는 것이 바람직합니다.

Q02 모든 기업은 반드시 공시를 해야 하나요?

정보보호산업법 시행령 제8조제1항의 기준을 충족하는 기업은 의무공시 대상으로 반드시 정보보호 공시를 해야 합니다.
의무공시 대상이 아니더라도 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자라면 누구나 자율적으로 정보보호 공시를 할 수 있습니다. 자율적으로 정보보호 현황 공시 이행한 기업은 정보보호 관리체계(ISMS) 인증수수료 30% 할인 혜택을 받을 수 있습니다.

Q03 글로벌 기업의 경우 공시 주체는 누구인가요??

글로벌 기업 본사 또는 국내 법인 중 국내 서비스의 제공 주체가 누구인지 판단하여 정보보호 공시 의무대상이 결정됩니다.
의무공시 대상이 아닌 글로벌 기업도 자율적으로 정보보호 공시를 할 수 있습니다.

Q04 ISDS와 KIND 두 곳에 같이 공시를 해야 하나요?

정보보호 공시는 과학기술정보통신부장관이 운영하는 전자공시시스템(이하 'ISDS')에 하는 것이 원칙입니다.
다만, 자율적으로 정보보호 공시를 하는 자가 유가증권·코스닥·코넥스시장 상장법인일 경우에는 ISDS 및 한국거래소 상장공시시스템(KIND)에 각각 공시 가능하며, 원하는 곳 한곳에만 공시도 가능합니다.

Q05 정보보호 현황을 허위로 공시할 경우 어떤 불이익을 받나요?

정보보호 공시자의 고의 또는 과실로 허위 사실을 공시할 경우, 불성실 공시로 판단하여 「정보보호 산업의 진흥에 관한 법률」 제13조제3항에 따른 정보보호 관리체계인증(ISMS) 수수료 감면 금액의 환수 조치 등 불이익 조치를 취할 수 있습니다.
또한 KIND에 자율공시한 경우, 한국거래소 공시 규정에 따라 공시위반 제재조치를 받을 수 있습니다.

Q06 투자액 산정을 위한 감가상각 적용 시, 내용연수에 대한 기준이 있나요?

내용연수에 대한 기준은 기업의 사규에 있는 기준을 적용하시면 됩니다. 또한 자산에 대한 감가상각 적용은 유·무형의 자산 모두를 포함합니다.

Q07 사무실에서 사용하는 PC나 네트워크, 스위치 같은 자산도 정보기술 관련 자산에 포함되나요?

공시 기관의 정보처리 시스템을 이용하거나 관리하기 위한 모든 IT 자산 및 비용은 정보기술부문자산/비용에 포함된다고 할 수 있습니다. 즉 사무실 출입을 위한 출입관리시스템이나 사무실 내외의 보안을 위한 영상정보처리 시스템(CCTV)도 정보기술/정보보호 부문투자로 볼 수 있습니다.* 그리고 보안문서를 별도의 통제된 공간, 즉 문서고를 조성하고 여기에 CCTV, 출입통제 시스템, 문서 반출입관리 시스템 등을 운영하면 이 시스템은 정보기술/정보보호부문 투자로 인정할 수 있습니다.

* 통신사 또는 전국에 지사를 보유한 기업들의 경우는 전산실에 설치된 출입관리시스템과 CCTV만 정보보호 투자로 인정

Q08 **정보처리 시스템을 외부 데이터센터에 위탁하여 운영하는 경우는 어떻게 투자비용을 구분하나요?**

정보처리 시스템을 외부 데이터센터에 두고 있을 경우 지불하는 비용을 정보기술 투자액으로 산정하면 됩니다. 이중 보안에 관련된 비용이 명확히 구분된다면 보안 관련 비용 부분을 정보보호부문 투자액으로도 산정할 수 있습니다.
보안관련 비용을 구분할 수 없더라도, 데이터센터를 서비스하는 기업이 정보보호 현황을 공시한 경우에는 그 기업의 정보보호부문에 대한 투자비율 만큼 전체 지불비용에서 정보보호 투자액으로 간주하여 산정할 수 있습니다.

Q09 **정보보호부문 관련 비용은 정보기술 관련 비용에 포함되나요?**

정보보호 비용은 모두 정보기술 비용에 포함됩니다. 예를 들면 물리보안서비스가 정보보호비용으로 인정되므로 이 비용은 당연히 정보기술비용으로도 인정됩니다. 그리고 인건비 산정에서도 정보보호 인력의 인건비는 정보기술 인력의 인건비에 포함됩니다. 인력 산정 또한 마찬가지로 정보보호 인력은 정보기술 인력에 포함됩니다.

Q10 **보안 전문업체로서 당사가 판매하고 있는 보안제품이나 서비스를 이용하는 경우, 이를 정보보호 투자액으로 산정할 수 있나요?**

비용원장이나 자산대장에 해당 제품이나 서비스 비용이 표시되어 있는 경우에는 인정됩니다. 그러나 표시되지 않는다면 정보보호 투자로 인정할 수 없습니다. 개발비 또한 자산대장이나 비용원장에 표시된다면 정보보호 투자로 인정됩니다. 단, 판매를 위한 생산비용, 용역계약에 의해 개발한 비용 등은 투자액으로 산정 불가능 합니다.

Q11 **라우터를 네트워크 접근 통제(방화벽처럼 활용) 전용으로 활용하고 있습니다. 정보보호 전용제품으로 인정받을 수 있나요?**

라우터의 본래의 기능은 정보보호 전용제품으로 볼 수 없기 때문에 정보보호 투자비용으로 인정하고 있지 않습니다.

Q12 **회사 지원으로 정보보안 관련 자격증을 취득하여 정보보안 업무에 투입한 직원들도 정보보호부문 인력으로 산정할 수 있나요?**

정보보호부문 인력 대상은 자격증 취득 유무와는 상관없습니다. 대상기업의 정보처리 시스템에 대하여 정보기술 또는 정보보호 관련 업무를 전담하는데 투입되었다면 정보기술/정보보호부문 인력으로 산정합니다.
그러나 대상기업의 정보시스템이 아닌 외주 용역에 의한 인력 파견으로 타 기업의 정보시스템을 위한 정보기술/보호 업무를 수행하고 있다면 대상기업의 정보기술/보호업무를 전담한다고 볼 수 없어 정보기술/보호부문 인력으로 산정할 수 없습니다. 다만 자격증 취득을 위한 회사의 지원에 대해서는 정보보호를 위한 활동으로 명기할 수 있습니다.

Q13 **보안담당자가 전산실이 아닌 타 부서에 배치되어 있을 경우에도 정보보호부문 인력으로 포함될 수 있나요?**

보안(정보보호) 업무를 명백하게 전담하고 있다면 소속된 부서 명칭은 상관없습니다. 다만 향후 사후검증에서 이를 입증하려면 대표자나 그에 상응하는 임원 (CISO 또는 CPO)의 서명이 있는 직무기술서를 준비하면 됩니다.

Q14 **국내에 한정하여 정보보호 투자나 인력을 산정하기 어려운 경우, 어떻게 내용을 작성할 수 있나요?**

재무제표, 자산대장 및 비용원장 등을 활용하여 정보기술/정보보호부문 투자 산정이 가능합니다. 인력 또한 국내 지사를 지원하는 인력에 대하여도 내부 산정 비율을 인정하여 산정이 가능합니다.
다만 해당 인력이 정보기술 또는 정보보호 업무를 전담하여야 하고, 단지 국내지사와 국외지사를 동시 지원하는 경우 회사 내부에서 산정하고 있는 지원 비율을 인정하여 산정할 수 있습니다.
일부 기업의 경우 글로벌 차원에서 정보보호 체계를 구축 및 운영 중에 있어 기업이 국내에 한정된 정보를 취합하는 것이 어려운 경우 정보보호 투자, 인력 수치를 작성하지 않아도 무방하나, '특기사항' 항목을 통해 정보보호에 대한 기업의 노력을 작성해야 합니다.

Q15 **정보시스템을 외부 데이터센터에 위탁하여 운영하는 경우, 외주 인력들은 정보기술/보호 부문 인력으로 포함할 수 있나요?**

정보처리 시스템을 외부 데이터센터에 두고 있을 경우, 해당 정보처리 시스템을 관리하는 인력(외주인력)도 대상기업의 정보시스템만 전담한다면 정보기술부문 인력으로 포함시킬 수 있습니다. 또한 보안담당은 정보보호부문 인력으로도 포함 가능합니다.
다만 대상 인력이 타 기업의 시스템도 공동으로 관리할 경우는 정보보호 현황 인력에 투입공수를 산정하여 대상기업을 위한 투입공수만을 포함시킬 수 있습니다. 이를 입증하기 위하여 위탁계약서(계약서상에 업무별로 투입공수가 명시되어 있을 경우) 등을 준비하면 됩니다.

Q16 **당사는 정보기술 인력과 정보보호 인력을 일정 기간 고객사에 파견하고 있습니다. 예를 들어, 3-5월까지 정보보호 인력을 외주용역으로 파견했다면 나머지 기간은 당사의 정보보호 인력으로 인정받을 수 있을까요?**

정보처리의 정보보호 인력으로 활용되다가 외주용역으로 활용되었다면 외주용역으로 활용된 기간을 제외한 기간은 정보보호 인원수로 인정될 수 있으며 연평균 인원수로 계산됩니다. 물론 그 해당기간의 인건비는 정보보호 투자액으로 인정받을 수 있습니다.

Q17 **정보기술부문 업무를 수행하는 인력이 타 업무(영업, 마케팅 등)를 겸임하고 있습니다. 주요 업무가 정보기술부문 업무라면(직무 기술서 상 정보기술부문 업무 비중이 90% 이상을 차지) 정보기술부문 인력에 포함되나요?**

정보기술부문 전담조직에 소속된 인원 또는 정보기술부분 업무를 전담(100%)하고 있는 인력에 대해서만 정보기술부문 인력으로 인정합니다. 위와 같은 경우에는 정보기술부문 인력에 포함되지 않습니다.

Q18 **우수정보보호 제품, 정보보호제품 성능평가 등도 정보보호 관련 인증, 평가, 점검 등에 관한 사항에 포함되나요?**

우수정보보호 제품, 정보보호제품 성능평가 등은 기업에서 생산하는 제품 및 서비스 등에 대한 인증이기 때문에 이를 기업 전체의 정보보호 관련 인증, 평가, 점검으로 보기에는 한계가 있습니다.
따라서, 제품 및 서비스에 대한 평가·인증은 정보보호 관련 인증, 평가, 점검 등에 관한 사항에 포함되지 않지만, 우수정보보호 제품, 정보보호제품 성능평가 제품을 개발 및 구매한 비용은 정보보호부문 투자 비용으로 인정됩니다.

Q19 **디자이너 인력은 정보기술부문 인력인가요?**

IT 기획·개발·운영·정보보호 등 정보기술 전담조직을 운영하는 경우에는 해당 부서 전체 인력을 정보기술부문 인력으로 산정합니다.
따라서, 제품팀, 개발팀 등 정보기술부문 조직에서 기획자, 개발자들과 함께 일하는 디자이너 직군은 정보기술부문 인력으로 분류합니다.

Q20 **의무대상 기준 中 이용자 수 100만은 어떻게 산정하나요?**

이용자수에 대한 의무대상 기준은 전년도 말 기준 직전 3개월간의 정보통신서비스 일일 평균 이용자 수 100만 명 이상입니다. 여러 가지 정보통신서비스(홈페이지 및 어플 등)를 제공할 경우에는 해당 서비스의 이용자 수를 모두 합하여 계산합니다. 산정 기준은 전년도 10월~12월의 순방문자수(UV)*의 일일 평균입니다.

* UV(Unique View) : IP 기준 1일 방문자 수(동일 IP로 동일 일에 수회 방문 시 1명으로 산정)

Q21 **의무대상 여부는 어떻게 알 수 있나요?**

매년 3월 첫째 주에 의무대상에 해당하는 기업리스트를 한국인터넷진흥원 대표 홈페이지 공지사항 등에 게시할 예정입니다. 해당 리스트를 확인하시면 됩니다.
확인 후, 의무대상에 해당하지 않는다고 생각하시는 기업은 의무 제외에 대한 소명자료를 3월 31일까지 정보보호 공시 담당자 메일*로 제출해주시면 됩니다.

* 한국인터넷진흥원 정보보호 공시 담당자 이메일 주소 : isds@kisa.or.kr

V 한눈에 보는 정보보호 공시 과정

순서		내용		비고
1	자료 준비	공시대상기간의 자산대장 및 비용원장, 외주용역비 내역, 정보기술 및 정보보호부문 인원 관련 인건비 내역		재무회계팀 협조 필요
		조직도, 원천징수이행상황명세서, 정보기술부문 전담조직 인원 수 및 업무내용, 정보보호부문 전담조직 인원 수 및 업무내용, 정보기술/보호부문 직무기술서, 상주/비상주 외주인력 현황		인사팀 협조 필요
		정보보호 관련 인증, 평가, 점검 증적자료		
		정보보호를 위한 활동 현황 증적자료		
2	정보기술 및 정보보호 내역 분류	투자	공시대상기간의 자산대장 및 비용원장, 외주용역비 내용, 관련 인건비 상에서 정보기술 및 정보보호 관련 내역 분류	
		인력	정보기술/보호부문 전담조직 인원 내역 및 직무 기술서를 확인 후, 정보기술 및 정보보호 전담인력 분류	
3	총 합계 산출	위 과정에서 분류된 내역을 정보기술 및 정보보호로 나누어 총 합계 산출		

순서		내용	비고
4	인증, 평가, 점검 및 정보보호 활동 현황 증적 취합	정보보호 관련 인증, 평가, 점검 증적자료 및 정보보호를 위한 활동 현황 증적자료를 확인하여 하나의 파일에 취합	
5	정보보호 현황 서식 작성	위에서 작업한 정보기술 및 정보보호 투자금액 총 합계와 인력, 인증, 평가, 점검, 정보보호 활동 현황 등을 정보보호 현황 서식에 기입 ※ 모든 산출 작업 자료들은 사후검증을 위하여 보관 필요	
6	최고경영자 직인	완성된 정보보호 현황 서식 및 사후검증 동의서에 정보보호 공시자의 최고경영자의 승인·결재 직인	
7	최종 제출	과학기술정보통신부 전자공시시스템(이하 'ISDS')에 입력, 불가피한 경우 한국인터넷진흥원에 전자파일 형태로 제출 * 한국인터넷진흥원 정보보호 공시 담당자 이메일 주소 : isds@kisa.or.kr	

첨부1 정보기술부문 및 정보보호부문 자산 분류표

대분류	중분류	소분류	설명
컴퓨팅 장비	서버 ※ OS 기준 구분	Unix	• 유닉스 OS(운영체제)를 사용하는 서버
		x86	• 윈도우(MS Windows) 및 리눅스 기반 OS(운영체제)를 사용하는 서버
		기타	• 상기 분류에서 제외된 서버 장비
	스토리지	스토리지	• 데이터가 저장되는 외장 스토리지
		NAS	• 네트워크 공유 스토리지
		기타	• 상기 분류에서 제외된 스토리지 장비
	백업 장비	테이프 라이브러리	• 다수의 테이프 카트리지를 가진 대용량 고속 백업용 장비
		VTL	• 가상 테이프 라이브러리(Virtual Tape Library), 가상화 기술을 통해 디스크를 테이프처럼 인식하여 데이터를 저장하는 데이터 백업 및 복구 장비
		기타	• 상기 분류에서 제외된 백업장비
	기타 컴퓨팅 장비	PC(사무용)	• 사무용으로 사용되는 중·소형 컴퓨터
		기타 입출력장치	• 스캐너, 프린터, 플로터, 팩스, 빔 프로젝터 등
		기반시설	• UPS, 항온 항습기, KVM 등의 기반시설
		기타	• 상기 분류에서 제외된 하드웨어
정보 통신 장비	교환설비		• 유선망: Voip교환기, BCN교환기, 지능망교환기, IP_PBX, IP기반 교환기, CMTS, Circuit 교환기(TDM등) • 무선망: 3G데이터, 4G교환기 (MME, MSC, IGS, AuC, PGW, SGW, IMS망, SMSC, AAA, 과금, HLR/HSS, MGW, TAS, EIR등), 부가서비스망, 2G, 3G음성 MSC교환기 (Circuit기반)
	전송설비		• 유선망: COT-RT, 광단국장비(가입자-국사), 국간전송장비, 라우터, 스위치, 방송저장장치, HFC망관련 전송장비 • 무선망: BSC, RNC, 교환국간 전송, 국사내 라우터, 라우터(백홀 라우터포함) ※ 가입자댁내 설비(모뎀, 셋탑박스, AP)와 기지국장비(BTS, RU, DU, e-NB 등)는 제외
	정보처리설비		• 망 관리 시스템 등

대분류	중분류	소분류	설명
네트워크 장비	전송장비		• 통신회선(광케이블등)을 통해 정보를 전송·처리할 수 있도록 하는 설비로 철도망, 우정망, 금융망 또는 지자체자가망 등 통신사망을 임대하지 않고 자체적으로 인터넷망을 구축하여 운영하는 기관만 해당 ※ WDM, ROADM, MSPP ,캐리어이더넷(PTN)장비 등
	스위치	L2	• 서로 다른 데이터링크 간을 MAC주소로 스위칭하는 소규모 워크그룹 스위치 장비
		L3	• 서로 다른 네트워크 간을 IP주소로 스위칭하는 장비로 라우팅 프로토콜을 수행하는 워크그룹 스위치, 또는 스위칭용량(Switching capacity) 720Gbps이하인 L3스위치(상세규격(스펙)에서 확인 가능)
		L4	• 서로 다른 네트워크 간을 서비스 포트로 스위칭하는 장비로 전송계층 정보(웹, FTP 등)에 따라 트래픽을 스위칭할 수 있어 부하분산(Load balancing)기능까지 제공하는 장비, 네트워크보안스위치도 해당
		백본	• 다수의 워크그룹 스위치 노드가 모이는 중심에 위치하는 스위치, 또는 스위칭용량 720Gbps이상의 L3스위치
		기타	• 상기 분류에서 제외된 스위칭 장비
	라우터		• 이기종의 네트워크(망)간의 연결을 위한 장비 • PSTN망, ATM망, 이더넷망 등을 연결하는 장비
	무선장비		• 일정공간에 WiFi서비스를 통한 인터넷 이용이 가능하도록 무선망을 구축하는 장비로 WiFiAP(무선공유기)등이 해당 ※ WiFiAP, AP컨트롤러(APC), WIPS, 무선랜인증장비 등
	기타 네트워크	VoIP용 장비	• IP망을 기반으로 음성 또는 영상 등 데이터통신을 제공하기 위한 장비 • IP교환기, VoIP용 게이트웨이, SBC(SessionBorderController), 콜센터상담어플(SW), 기타VoIP용장비 등을 포함
		네트워크 NMS	• 네트워크 운영 · 관리시스템(Network Management System). 이기종 네트워크 장비의 구성, 성능, 장애 정보를 통합 모니터링하기 위한 시스템
		기타	• 상기 분류에서 제외된 통신장비

대분류	중분류	소분류	설명
방송장비	영상장비	빔 프로젝트	• 빛을 이용하여 슬라이드나 동영상 이미지 등을 스크린에 비추는 장치로 촬영된 영상을 스크린에 표현
		방송 스토리지	• 촬영된 영상을 저장하고 관리하는 장치
		편집장치 (CG)	• 영상을 편집(자막, 그래픽 등) 할 수 있는 기기
		송출/ 수신장치	• 편집된 영상을 최종으로 분배하고 수신하여 모니터 등으로 표현하는 장비
		방송플랫폼 (인터넷 방송 시스템 포함)	• 컨텐츠와 서비스 등을 망, 네트워크, 통신 등을 이용하여 개발자/ 사업자가 빠르고 쉽게 주고받기 위한 장비와 S/W
		기타	• 상기 분류에서 제외된 방송용 영상장비
	음향 장비	방송용 음향 장비(SR 등)	• 공연, 강의 등의 음향정보 전달을 위해 설치되는(스피커, 앰프, 믹서, 프로세스 등) 장비
		비상 전관방송 (PA)	• 실/내외의 전 지역에 공지사항 방송, 일반방송, 비상통제 방송, 원격방송 등을 통하여 비상 상황 발생 시 안전지대 대피유도, 일반안내 및 음악(B.G.M)방송 등을 신속, 정확하게 동작 시키는 장비
		기타(회의용 시스템 등)	• 위의 분류에서 제외된 방송용 음향장비
소프트웨어	시스템 소프트웨어	운영체계	• 컴퓨터를 작동시키고 전반적인 동작을 제어 및 운영을 도맡아 관리하는 기본 소프트웨어
		통신 소프트웨어	• 컴퓨터 상호간에 접속하여 두개의 장치 사이에 다양한 방법으로 정보를 교환할 수 있게 하는 소프트웨어
		유틸리티 소프트웨어	• 사용자가 컴퓨터를 좀 더 편리하고 쉽게 사용할 수 있도록 도와주는 프로그램
		시스템관리 소프트웨어	• 네트워크를 관리하는 기능을 포함 여러 개의 네트워크가 묶인 대규모의 시스템에서 이기종 데이터베이스관리, 미들웨어 등에 이르는 다양한 기능을 체계적으로 관리하도록 하는 시스템
		미들웨어	• 클라이언트에서 서버에 있는 애플리케이션이나 자원을 불러오기 위해 클라이언트와 서버의 가운데 놓인 중간자

대분류	중분류	소분류	설명
소프트웨어	개발용 소프트웨어	프로그램 개발용 언어	• 컴퓨터가 인식할 수 있는 컴퓨터의 명령어를 논리적 순서에 맞게 프로그래머가 작성하는 프로그래밍 작업과정에서 사용되는 언어
		프로그램 및 콘텐츠개발용 도구	• 개발 생산성 및 품질향상을 도모하는 데 사용되는 각종 소프트웨어 및 각종 콘텐츠개발에 지원되는 도구
		프로젝트 관리용 소프트웨어	• 프로젝트 추진이나 개발 시 방생하는 모든 제반요소를 체계적으로 관리하기 위해 사용되는 소프트웨어
		DBMS	• 데이터를 효과적으로 이용할 수 있도록 정리, 보관하기 위한 기본 소프트웨어
	응용 소프트웨어	기업관리 소프트웨어	• 기업의 기간업무를 통합 관리해주는 소프트웨어
		과학용 소프트웨어	• 과학적 데이터의 처리나 과학적문제 등의 기술을 개발하고 지원하기 위한 소프트웨어
		산업용 소프트웨어	• 모든 분야의 생활적 활동의 전반적인 전체 산업을 구성하는 각 부문 및 각 업종을 지원하는 소프트웨어
	기타 소프트웨어		• 상기분류에서 제외된 소프트웨어
정보 보안 제품	네트워크 보안	웹 방화벽	• 다양한 형태의 웹 기반 해킹 및 유해트래픽을 실시간 감시하여 탐지하고 차단하는 웹 애플리케이션 보안 시스템
		네트워크 (시스템) 방화벽	• 외부의 불법 침입으로부터 내부의 정보자산을 보호하고 유해정보의 유입을 차단하기 위한 정책과 이를 지원하는 보안시스템
		침입방지시스템(IPS)	• 네트워크에서 공격 서명을 찾아내 자동으로 모종의 조치를 취하여 비정상적인 트래픽을 중단시키는 보안 솔루션
		DDoS 차단 시스템	• 대량의 트래픽을 전송하여 시스템을 마비시키는 디도스 공격 전용차단시스템
		통합보안 시스템 (UTM)	• 다중 위협에 대해 보호기능을 제공할 수 있는 포괄적인 보안 제품
		가상사설망 (VPN)	• 인터넷망 또는 공중망을 사용하여 둘 이상의 네트워크를 안전하게 연결하기 위하여 가상의 터널을 만들어 암호화된 데이터를 전송할 수 있도록 만든 네트워크

대분류	중분류	소분류	설명
정보 보안 제품	네트워크 보안	네트워크 접근제어 (NAC)	• 네트워크에 접근하는 접속단말의 보안성을 강제화할 수 있는 보안 인프라. 허가되지 않거나 악성코드에 감염된 PC 등이 네트워크에 접속되는 것을 차단해 시스템 전체를 보호하는 솔루션
		무선네크워크보안	• 무선을 이용하는 통신네트워크 상에서 인증, 키 교환 및 데이터 암호화 등을 통해 위협으로부터 보호하기 위한 기술
		가상화 (망분리)	• 조직에서 사용하는 망(네트워크)을 업무 및 내부용 망(인트라넷)과 외부망(인터넷)으로 구분하고 각 망을 격리
	시스템 (단말) 보안	시스템 접근통제 (PC방화벽 포함)	• 자료가 외부로 유출되는 것을 방지하기 위해 온라인을 통한 파일 유출방지, 감시 기능, SMTPMail, WebMail 등을 통한 파일 유출 방지, 감시기능, 프린터인쇄 모니터링 기능 등 자료 유출을 보안하는 다양한 기능을 함
		Anti 멀웨어	• 컴퓨터의 운영을 방해하거나, 정보를 유출 또는 불법적으로 접근권한을 취득하는 소프트웨어인 멀웨어를 방지함
		스팸차단 S/W	• 스팸을 방지하기 위해 스팸 차단 또는 필터링 기능을 제공하는 소프트웨어
		보안운영체제 (Secure OS)	• 컴퓨터 운영 체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위해 기존의 운영체제 내에 보안 기능이 추가된 운영체제
		APT대응	• APT공격에 대응하기 위한 프로그램 소프트웨어
		모바일 보안	• 모바일 서비스 상에 발생할 수 있는 위협으로부터 보호하기 위한 기술
	콘텐츠 (데이터)/ 정보유출 방지	DB보안 (접근통제)	• 데이터베이스 및 데이터베이스 내에 저장된 데이터를 인가되지 않은 변경, 파괴, 노출 및 비일관성을 발생시키는 사건으로부터 보호하는 기술
	보안	DB 암호	• 데이터의 실제 내용을 허가받지 않은 사람이 볼 수 없도록 은폐하기 위하여 데이터를 암호화하는 것
		보안 USB	• 사용자식별, 지정데이터 암복호화, 지정된 자료의 임의복제 방지, 분실 시 데이터 보호를 위한 삭제 등의 기능을 지원하는 보안 컨트롤러가 있는 휴대용 메모리 스틱
		디지털저작권 관리(DRM)	• 웹을 통해 유통되는 각종 디지털 콘텐츠의 안전 분배와 불법 복제 방지

대분류	중분류	소분류	설명
정보 보안 제품	보안	네트워크 DLP	• 사용자의 고의 또는 실수, 외부해킹, 멀웨어 등을 네트워크를 이용한 정보유출을 컨텐츠 수준에서 막는 기술
		단말 DLP	• 사용자의 고의 또는 실수, 외부해킹, 멀웨어 등을 네트워크를 이용한 정보유출을 단말 수준에서 막는 기술
	암호/인증	보안스마트카드	• 일반카드와는 달리 반도체 칩을 내장한 스마트카드
		H/W토큰(HSM)	• 전자 서명 생성키 등 비밀정보를 안전하게 저장 및 보관할 수 있고 기기 내부에 프로세스 및 암호 연산장치가 있어 전자 서명키 생성, 전자 서명 생성 및 검증 등이 가능한 장치
		일회용비밀번호(OTP)	• 로그인할 때마다 새로운 패스워드를 생성하는 보안 시스템
		공개키기반구조(PKI)	• 실체의 식별자와 공개키를 포함하는 정보로서 공개키 정보는 한 실체에 대한 데이터와 이 실체를 위한 공개키로 제한되며 인증기관, 실체, 공개키 또는 관련 알고리즘에 관한 다른 정적인 정보
		통합접근관리(EAM)/싱글 사인온(SSO)	• 통합접근관리: 인트라넷, 엑스트라넷 및 일반클라이언트/서버환경에서 자원의 접근인증과 이를 기반으로 자원에 대한접근권한을 부여 관리하는 통합인증관리솔루션 • 싱글사인온: 이기종의 시스템을 사용할 때마다 다른 사용자번호와 비밀번호를 입력하지 않고도 한번 인증만으로 전 시스템을 하나의 시스템처럼 사용할 수 있도록 하는 시스템
		통합계정관리(IM/IAM)	• ID와 패스워드를 종합적으로 관리해주는 역할 기반의 사용자 계정 관리 솔루션
	보안관리	통합보안관리(ESM)	• 방화벽, 침입탐지시스템, 가상사설망 등 각종 보안시스템 및 주요시스템 장비를 연동하여 효율적으로 운영할 수 있도록 하는 시스템
		위협관리시스템(TMS)	• 국내외 최신 취약성 정보와 보안 트렌드, 정밀 분석된 네트워크 트래픽 및 공격 형태를 상관 분석해 사이버 공격을 예측하고 판단하여 능동적으로 대응할 수 있는 체계적인 위협관제 및 대응 시스템
		패치관리시스템(PMS)	• 시스템의 보안 취약점을 보완하기 위하여 배포되는 보안 패치 파일을 원격에서 자동으로 설치 관리해주는 시스템
		위험관리시스템(RMS)	• 관리 대상 시스템의 잠재적인 위험도를 관리하며 위협 분석 기능뿐만 아니라 정보시스템의 취약성을 인식하고, 이로 인해 예상되는 손실을 분석하고 주요자산 평가 기능 등을 총체적으로 제공하는 시스템

대분류	중분류	소분류	설명
정보 보안 제품	보안 관리	백업/복구 관리 시스템	•자료 손실을 예방하기 위해 자료를 미리 다른 곳에 임시로 보관해 두었다가 원래 상태로 복구해주는 관리 시스템
		로그 관리/ 분석 시스템	•로그를 실시간 수집, 저장 및 분석하는 등의 작업을 위해 사용되어지는 시스템
		취약점 분석 시스템	•악성코드 민감도, 안전하지 않은 소프트웨어 설정, 열린 포트 같은 컴퓨터 시스템의 알려진 취약점들을 분석하기 위해 사용되어지는 시스템
		디지털 포렌식 시스템	•정보기기 내에 내장된 디지털자료가 법적증거가 되도록 자료를 수집, 보관, 분석, 보고용으로 사용 하는 시스템
	기타 정보보안제품		•상기분류에서 제외된 제품
물리보안 제품	CCTV	CCTV 시스템	•특정한 수신자에게만 서비스하는 것을 목적으로 하는 텔레비전 전송시스템, 카메라, 모니터, 디지털비디오녹화기(DVR), 네트워크로 구성된 시스템 ※ (예) 저장장치, 카메라, 주변장비 영상감시관제S/W 및 장비, 지능형솔루션, 액세서리
	바이오 인식	얼굴인식 시스템	•사람 얼굴의 대칭적인 구도, 생김새, 머리카락, 눈의 색상, 얼굴 근육의 움직임 등을 분석해 얼굴의 특징을 알아내는 대표적인 생체인식 기술
		지문인식 시스템	•지문 인식은 전용 센서를 이용해 지문의 디지털 영상을 획득하여 지문에 있는 다양한 패턴을 이용하여 신원을 확인하는 기술
		홍채인식 시스템	•홍채의 모양과 색, 망막모세혈관의 형태소 등을 분석해 사람을 인식하는 생체인식기술
		정맥인식 시스템	•손바닥이나 손가락에 흐르는 정맥을 이용해 본인 여부를 인식하는 생체인식 기술
		기타 (음성인식 및 기타)	•상기분류에서 제외된 시스템
	접근제어		•주요관공서, 군주요시설, 금융기관, 회사, 연구실 등의 보안유지가 요구되는 곳 또는 이용자의 출입관리가 요구되는 곳에서 IDCARD 등의 인식장비를 활용하여 관리하는 시스템 ※ (예) 카드&리더(번호/마그네틱), 시큐리티게이트 및 S/W 등
	알람모니터링		•온도, 압력, 방사선세기 등의 물리량이나 화학량을 검지하여 신호처리가 가능하도록 변화시키는 장치 ※ (예)적외선/레이저/진동/장력센서, 모션디텍터/침입 탐지장비 등
	기타 물리보안제품		•상기분류에서 제외된 제품

첨부2 정보보호 서비스 분류표

대분류	중분류	소분류	세부 항목
정보보호 서비스	정보보안 서비스	유지관리	• 제품업데이트, 기술지원 등
		보안성 지속 서비스	• 보안업데이트, 보안정책관리, 위협/사고분석, 보안기술 자문, 보안성 인증(KCMVP 등)효력 유지
		보안관제	• 원격관제 서비스 • 파견관제 서비스
		보안컨설팅	• 인증(ISO, ISMS 등) • 기반보호 • 진단 및 모의해킹 • 개인정보보호컨설팅 • 종합보안컨설팅 • 정보감사(내부정보유출방지컨설팅 등)
		교육/훈련	• 교육훈련 서비스
		인증서비스	• 공인/사설 인증서비스
	물리보안 서비스	• 출동보안서비스	
		• 영상보안서비스	
		• 기타보안서비스	

정보보호 공시 가이드라인

인 쇄 2021년 12월 인쇄
발 행 2021년 12월 발행

발 행 처 과학기술정보통신부, 한국인터넷진흥원

제 작 호정씨엔피(02-2277-4718)

정보보호 공시 가이드라인

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY