

정보보호 공시 가이드라인

Guidelines for Information Security Disclosure

2024. 3.



과학기술정보통신부
Ministry of Science and ICT

KISA **한국인터넷진흥원**
KOREA INTERNET & SECURITY AGENCY

정보보호 공시 가이드라인

Guidelines for
Information Security Disclosure

| 가이드라인 제·개정 이력

| 제·개정월 | 내역 |
|-----------|--|
| 2016. 08. | 정보보호 공시 가이드라인 제정 |
| 2019. 01. | 가이드라인 수정·보완 (사전점검 절차 의무화 폐지, 사후검증 대체 등) |
| 2021. 12. | 가이드라인 수정·보완 (정보보호 공시 의무화, 공시내용 양식 변경 등 정보보호산업법 및 하위법령 개정 내용 반영) |
| 2023. 01. | 가이드라인 수정·보완 (정보기술부문/정보보호부문 판단 기준 수립 등) |
| 2024. 03. | 가이드라인 수정·보완 (허위·불성실 공시 방지를 위한 정보보호산업법 및 하위법령 개정 내용 반영 등) |

CONTENTS

I

총칙

| | |
|--------------------------|----|
| 1. 제도 개요 | 06 |
| 2. 공시 항목 및 기준 | 10 |
| 3. 이행 절차 및 혜택 | 16 |
| 4. 공시내용 검증 방법 및 절차 | 25 |

II

공시내용 작성 방법

| | |
|---------------------------------|----|
| 1. 정보보호 투자 현황 산출 방법 | 32 |
| 2. 정보보호 인력 현황 산출 방법 | 51 |
| 3. 정보보호 인증·평가·점검 등에 관한 사항 | 62 |
| 4. 정보보호를 위한 활동 현황 | 64 |

III

자주 묻는 질문·응답 [FAQ]

68

첨부

| | |
|--|----|
| [첨부 1] 정보기술부문/정보보호부문 자산 분류표 | 72 |
| [첨부 2] 정보보호 서비스 분류표 | 78 |
| [첨부 3] 영업보고서를 작성하는 기간통신사업자 대상 정보기술부문 /정보보호부문 투자 산출 방법 | 79 |
| [첨부 4] 정보보호 최고책임자(CISO) 신고 접수 문의처 | 86 |

정보보호 공시
가이드라인



Guidelines for
Information Security Disclosure

총칙

-
- 제도 개요
 - 공시 항목 및 기준
 - 이행 절차 및 혜택
 - 공시내용 검증 방법 및 절차

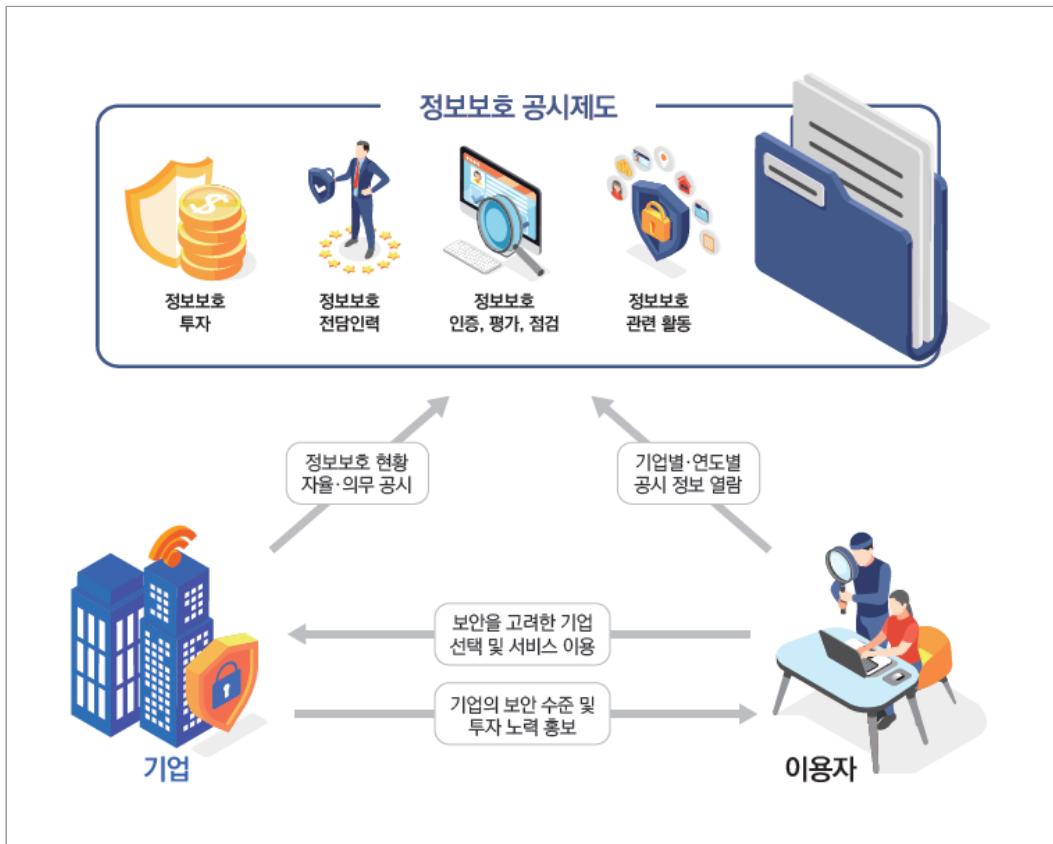
I 총칙

1 | 제도 개요

■ 목적

- 디지털 전환 과정에서 발생하는 사이버 침해사고, 디지털 대란 등이 기업의 경제적 피해, 대외 신뢰도 저하, 이용자 불편 등 기업 경영에 직·간접적인 영향을 끼치게 됨에 따라,
 - 정보통신 서비스 관련 기업뿐 아니라 이용자의 개인정보를 대량으로 보유한 전자상거래 기업 또는 중요 연구개발 정보를 보유한 첨단기업, 사회 기반시설 등 모든 기업에 정보보호가 핵심 경쟁력으로 부각됨.
- ※ IBM 보고서에 따르면 2021~2022년 2년 연속으로 제조업(24.8%)이 사이버 공격을 가장 많이 받는 업종으로 나타났으며, 그 다음으로 금융(18.9%), 서비스(14.6%), 에너지(10.7%) 순으로 나타남.
- 그러나 기업의 정보보호 현황은 위험관리(risk management)와 관련된 주요 정보이지만 그동안 시장에서 투명하게 공개되지 못하였으며, 이해관계자들은 해당 기업의 정보보호 현황을 알 수 없어 불충분한 정보로 서비스 이용과 투자 등 의사결정이 이루어짐.
 - 최근까지 많은 기업이 비용과 복잡성 등을 이유로 정보보호 문제에 관심을 갖지 않았으나, 사이버 공격 증가로 정보보호가 경영진의 핵심 이슈로 떠오름.

※ IBM 보고서에 따르면 2023년 데이터 유출로 인한 전세계 평균 비용은 445만 달러로 지난 3년간 15% 증가하였으며, 국내의 데이터 유출로 인한 평균 비용은 지난 3년간 19% 증가한 45억 3,600만 원으로 나타남.



- **정보보호** 공시제도는 이용자 보호 및 알권리를 보장하고 기업의 자발적인 **정보보호** 투자를 촉진하기 위한 제도로서,
 - (주주) 기업의 잠재적 재무상태 변화에 주요한 영향*을 미칠 수 있는 정보보호 현황에 대한 주주의 알권리를 확보함.
 * 기업의 중요 정보 유출, 징벌적·법정 손해배상제도 도입에 따른 강화된 배상책임, 소비자 신뢰도 저하 등으로 인한 큰 재무적 변동이 발생 가능함.
 - (이용자·국민) 기업 등이 보유하고 있는 다양한 정보의 보호 수준을 간접적으로 파악할 수 있도록 하여 이용자의 선택권을 강화함.
 - (기업) 기업 스스로 정보보호 수준을 객관적으로 파악하고, 이용자 등에게 정보보호 활동을 공시함으로써 법적 근거를 갖고 기업의 보안 투자 정도를 외부에 알릴 수 있는 기회로 활용함.

■ 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 통하여 사업 활동을 하는 영리·비영리 업체 모두 포함.

- (의무공시) 사업분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자(정보보호산업법 제13조제2항, 이하 '정보보호 공시 의무자'라 한다.)

참고

정보보호 공시 의무 대상 기준

| | |
|-------|--|
| 사업분야 | ▶ 회선설비 보유 기간통신사업자 ※「전기통신사업법」제6조제1항 |
| | ▶ 집적정보통신시설 사업자 ※「정보통신망법」제46조 |
| | ▶ 상급종합병원 ※「의료법」제3조의4 |
| | ▶ 클라우드컴퓨팅 서비스 제공자 ※「클라우드컴퓨팅법 시행령」제3조제1호 |
| 매출액 | ▶ 정보보호 최고책임자(CISO)*를 지정·신고하여야 하는 유가증권시장 및 코스닥시장 상장법인 중 매출액 3,000억 원 이상 |
| 이용자 수 | ▶ 정보통신 서비스 일일 평균 이용자 수** 100만 명 이상(전년도 말 직전 3개월간) |

* CISO: Chief Information Security Officer. 조직의 정보자산을 안정적으로 운영하는 데 필요한 정보보호 전략 및 정책을 수립하고, 관련 법·제도 준수, 보호관리 활동 수행, 위험에 따른 대책을 도출하고 실행하는 등 정보보안 관련 총괄 책임을지는 임원이나 관리자급 구성원을 가리킴(정보통신망법 제45조의3 참고).

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

참고

정보보호 공시 의무 예외 기준

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

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

※ 소기업의 경우 「중소기업 범위 및 확인에 관한 규정」에 따라 중소기업 현황 정보시스템을 통하여 발급받은 확인서 제출이 필요함.



법적 근거

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 정보통신 서비스를 이용하는자의 안전한 인터넷 이용을 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.

② 제1항에도 불구하고 정보통신 서비스를 이용하는자의 안전한 인터넷 이용을 위하여 정보보호 공시를 도입할 필요성이 있는 자로서 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는자는 제1항에 따른 정보보호 현황을 공시하여야 한다. 다만 다른 법률의 규정에 따라 정보보호 현황을 공시하는자는 제외한다.

「정보보호산업의 진흥에 관한 법률 시행령」 제8조(정보보호 공시) ① 법 제13조제2항 본문에서 '대통령령으로 정하는 기준에 해당하는자'란 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는자(이하 '정보보호 공시의무자'라 한다.)를 말한다.

1. 다음 각 목의 어느 하나에 해당하는자

- 가. 「전기통신사업법」 제6조제1항에 따라 등록한 기간통신사업자 중 같은 법 시행령 제11조에 따른 회선 설비 보유사업을 경영하는자
- 나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설 사업자
- 다. 「의료법」 제3조의4제1항에 따른 상급종합병원
- 라. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제3조제1호의 클라우드컴퓨팅 서비스를 제공하는자

2. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3제1항 본문에 따라 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고해야 하는 자로서 유가증권시장(「자본시장과 금융투자업에 관한 법률 시행령」 제176조의9제1항에 따른 유가증권시장을 말한다.) 또는 코스닥시장(대통령령 제24697호 자본시장과 금융투자업에 관한 법률 시행령 일부개정령 부칙 제8조에 따른 코스닥시장을 말한다.)에 상장된 주권을 발행한 법인 중 직전 사업연도의 매출액이 3,000억 원 이상인자

3. 전년도 말 기준 직전 3개월간 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 정보통신 서비스의 일일평균 이용자 수가 100만 명 이상인자

② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는자는 정보보호 공시의무자에서 제외한다.

1. 공공기관

- 2. 제1항제1호 또는 제3호에 해당하는자 중 「중소기업기본법 시행령」 제8조제1항에 따른 소기업
- 3. 「전자금융거래법」에 따른 금융회사
- 4. 「전자금융거래법」에 따른 전자금융업자로서 「통계법」 제22조제1항에 따라 통계청장이 고시하는 한국 표준산업분류에 따른 정보통신업이나 도매 및 소매업을 주된 업종으로 하지 않는자

2 | 공시 항목 및 기준

■ 공시 항목

- 「정보보호 공시에 관한 고시(이하 ‘고시’라 한다.)」[별표3] 정보보호 공시내용 양식(이하 ‘공시내용 양식’이라 한다.)에 따라 정보보호 투자 현황, 정보보호 인력 현황 등 4가지 항목별로 내용을 기재하여 최고경영자의 확인을 받음.

▣ 참고

고시 [별표3] 공시내용 양식

| | | | | | | | | | | | |
|-------------------------------------|---|---|----------------------|-------|-------|-------|--|--|--|--|--|
| 1. 정보보호 투자 현황 | 정보기술부문 투자액(A) | 정보보호부문 투자액(B)을 포함하여 산정 | | | | | | | | | |
| | 정보보호부문 투자액(B) | 정보기술부문 투자액(A) 중에서 정보보호와 관련하여 소요된 투자액 산정 | | | | | | | | | |
| | 주요 투자 항목* | 보안 솔루션 신규 도입 등 공시대상연도 정보보호부문 주요 투자 사항 작성 | | | | | | | | | |
| | B/A | 0.0%(소수점 첫째 자리까지 표기, 100%를 넘을 수 없음.) | | | | | | | | | |
| | 특기 사항* | 정보보호 투자 현황에 대한 세부설명 또는 참고할 만한 사항을 작성 | | | | | | | | | |
| 2. 정보보호 인력 현황 | 총 임직원 | 공시대상 기업의 내부인력 | | | | | | | | | |
| | 정보기술부문 인력(C) | 정보보호부문 전담인력(D)을 포함하여 산정(내부인력과 외주인력 모두 포함) | | | | | | | | | |
| | 정보보호부문 전담인력(D) | 내부인력 | 정규직과 계약직 모두 포함 | | | | | | | | |
| | | 외주인력 | 계약서 기반의 투입 공수로 인력 산정 | | | | | | | | |
| | | 계 | 정보보호부문 내부인력과 외주인력 합계 | | | | | | | | |
| 3. 정보보호 관련 인증·평가·점검 등에 관한 사항 | D/C | 0.0%(소수점 첫째 자리까지 표기, 100%를 넘을 수 없음.) | | | | | | | | | |
| | CISO·CPO 지정 현황 | 구분 | 직책 | 임원 여부 | 겸직 여부 | 주요 활동 | | | | | |
| | | CISO | 상무 | ○ | × | *건 | | | | | |
| | | CPO | 이사 | ○ | × | *건 | | | | | |
| | 특기 사항* | 정보보호 인력 현황에 대한 세부설명 또는 참고할 만한 사항을 작성 | | | | | | | | | |
| 4. 정보통신 서비스를 이용하는 자의 정보보호를 위한 활동 현황 | ISMS, ISO/IEC 27001 인증 등 공시대상연도에 유효한 사항 작성 | | | | | | | | | | |
| | KISA 주관 해킹 훈련 참여*, 제로트러스트 도입 준비, 정보 보호 교육, 정보보호 보험 가입 등 현황 작성 * 랜섬웨어, 디도스(DDoS), 해킹 메일 등 모의훈련 유형과 내용, 주관기관 등 기재 필요 | | | | | | | | | | |

■ 제출 내용

- 고시 및 정보보호 공시 가이드라인(이하 ‘가이드라인’이라 한다.)에 따라 작성된 공시내용 양식과 함께 공시내용 검증동의서(고시 [별표4])를 과학기술정보통신부 전자공시시스템(isds.kisa.or.kr)에 제출 및 공개하거나,
 - 회계법인이나 정보시스템 감리법인으로부터 사전점검을 받고 확인서(공시용, 조서용 2종)를 공시내용 양식과 함께 과학기술정보통신부 전자공시시스템(isds.kisa.or.kr)에 제출함.

※ 회계법인이나 정보시스템 감리법인으로부터 공시내용에 대하여 사전점검을 받고 확인서(공시용, 조서용 2종)를 제출한 기업은 공시내용 검증 대상에서 제외될 수 있음.

참고

정보보호 공시 제출 자료

① 정보보호 공시 사전점검 없이 자체적으로 공시를 진행하는 경우

1 정보보호 공시내용 양식

[별표3] 정보보호 공시내용 양식

| [회사명] 정보보호 현황 | | | | | | | | | | |
|--|--|----------|----------|----------|----------|----------|------|-----|--|--|
| 『정보보호사업의 진통에 관한 법률』 제13조, 같은 법 시행령 제8조 및 「정보보호 공시에 관한 고시」에 따라 다음 사항에 대해 공시합니다. | | | | | | | | | | |
| 작성 기준일 : 20... . | | | | | | | | | | |
| 1. 정보보호 부서 현황 | 정보기술부문 팀장자(A) 정보기술부문 부서장자(B) 국회 회장자(C) | | | | | | | | | |
| | 2. 소 부서 현황 총괄부원 정보기술부문 인력(C) 정보보호부문 내부현황 간접인력(D) | | | | | | | | | |
| 2. 정보보호 인력 현황 | D / C | | | | | | | | | |
| | CISO/CPO 직책 현황 <table border="1"><thead><tr><th>구분</th><th>직책</th><th>정원 여부</th><th>경력 여부</th><th>주교 활동</th></tr></thead><tbody><tr><td>CISO</td><td>CPO</td><td></td><td></td><td></td></tr></tbody></table> | 구분 | 직책 | 정원 여부 | 경력 여부 | 주교 활동 | CISO | CPO | | |
| 구분 | 직책 | 정원 여부 | 경력 여부 | 주교 활동 | | | | | | |
| CISO | CPO | | | | | | | | | |
| 첨부파일 1. 정보보호 관련 법률, 규정, 정침 등에 관한 서명 2. 정보통신서비스제공법 이용하는 차트 정보보호를 위한 활동 현황 | | | | | | | | | | |
| * 해당 항목의 작성은 공시 기관의 선택사항 | | | | | | | | | | |
| (회사명) 대표이사 ○○○은 상기 공시 내용에 거짓이 없음을 확인하였습니다. 0000. 00. 00. (회사 대표이사 직인) | | | | | | | | | | |
| ※ 작성 기준일 : 공시년도의 직전년도 마지막 날 | | | | | | | | | | |
| ※ 19년도에 정보보호 공시를 이행할 경우 작성 기준일은 '10년 12월 31일' | | | | | | | | | | |

2 정보보호 공시내용 검증 동의서

[별표4] 정보보호 공시내용 검증 동의서

| 정보보호 공시내용 검증 동의서 | |
|---|--|
| 과학기술정보통신부는 정보보호 현황을 제출한 법인에 대하여 공시내용 정정 및 사실 관계 증명을 위하여 「정보보호사업의 진통에 관한 법률」 제13조제4항, 「정보보호 공시에 관한 고시」 제10조에 의거, 검증을 진행할 수 있으며, ○○○은 검증 진행에 동의합니다. | |
| ○ 품지자료 수집·이용 목적 : 정보보호 현황의 확인 및 점검을 위한 용도로만 사용 ○ 보유 및 이용기간 : 공시 자료 제출 요구에 따른 자료 제출일로부터 3주간 보유하며, 이후 시제 없이 파기 | |
| □ 정보보호 공시 자료 제출 요구 내용 | |
| 1. 요구목적 - 공시 기업 정보보호 현황의 부정성·신뢰성 확인 | |
| 2. 요구항목 - 정보보호 공시 항목(부자액, 인력, 인증·평가·점검 사항, 정보보호 활동)의 관련 산출 근거 자료 등 - 회사의 회계정보와 관련하여 부정행위, 분개사실이 발생할 경우, 이를 과학기술정보통신부에 알림 | |
| 3. 요구방법 - 관련 자료 서면 제출 또는 현장방문을 통한 자료 제출 요구 | |
| (회사명) 대표이사 ○○○은 상기 내용에 동의합니다. 0000. 00. 00. (회사 대표이사) | |

② 정보보호 공시 사전점검 후 공시를 진행하는 경우

1 정보보호 공시내용 양식

[별표3] 정보보호 공시내용 양식

| [회사명] 정보보호 현황 | | | | | | | | | | |
|---|--|----------|----------|----------|----------|----------|------|-----|--|--|
| 『정보보호사업의 진통에 관한 법률』 제13조, 같은 법 시행령 제8조 및 「정보보호 공시에 관한 고시」에 따른 회사의 정보보호 실무 현황에 대한 공시입니다. | | | | | | | | | | |
| 작성 기준일 : 20... . | | | | | | | | | | |
| 1. 정보보호 부서 현황 | 정보기술부문 팀장자(A) 정보기술부문 부서장자(B) 국회 회장자(C) | | | | | | | | | |
| | 2. 소 부서 현황 총괄부원 정보기술부문 인력(C) 정보보호부문 내부현황 간접인력(D) | | | | | | | | | |
| 2. 정보보호 인력 현황 | D / C | | | | | | | | | |
| | CISO/CPO 직책 현황 <table border="1"><thead><tr><th>구분</th><th>직책</th><th>정원 여부</th><th>경력 여부</th><th>주교 활동</th></tr></thead><tbody><tr><td>CISO</td><td>CPO</td><td></td><td></td><td></td></tr></tbody></table> | 구분 | 직책 | 정원 여부 | 경력 여부 | 주교 활동 | CISO | CPO | | |
| 구분 | 직책 | 정원 여부 | 경력 여부 | 주교 활동 | | | | | | |
| CISO | CPO | | | | | | | | | |
| 첨부파일 1. 정보보호 관련 법률, 규정, 정침 등에 관한 서명 2. 정보통신서비스제공법 이용하는 차트 정보보호를 위한 활동 현황 | | | | | | | | | | |
| * 해당 항목의 작성은 공시 기관의 선택사항 | | | | | | | | | | |
| (회사명) 대표이사 ○○○은 상기 공시 내용에 거짓이 없음을 확인하였습니다. 0000. 00. 00. (회사 대표이사 직인) | | | | | | | | | | |
| ※ 작성 기준일 : 공시년도의 직전년도 마지막 날 | | | | | | | | | | |
| ※ 19년도에 정보보호 공시를 이행할 경우 작성 기준일은 '10년 12월 31일' | | | | | | | | | | |

2 사전점검확인서(공시용)

000기업

정보보호현황 사전점검 확인서
공시용

2020년 01월 01일 부터
2020년 12월 31일 까지

회계법인 또는
정보시스템
감리법인명

000기업

정보보호현황 사전점검 확인서
조서용

2020년 01월 01일 부터
2020년 12월 31일 까지

회계법인 또는
정보시스템
감리법인명

■ 정보기술부문 판단 기준

- ‘정보기술부문’이란 다음 각 활동을 위한 기업의 관리적·기술적 자산 및 서비스, 인력 및 조직을 말함.
 - 「전기통신사업법」제2조제2호에 따른 전기통신설비를 이용하는 것
 - 컴퓨터 등 정보처리능력을 가진 하드웨어와 소프트웨어, 이를 사용하기 위한 간접설비를 이용하는 것
 - 컴퓨터 등 정보처리능력을 가진 장치를 이용한 기술을 활용하여 정보를 수집·가공·저장·검색·송신·수신하는 것
 - 시스템 및 서비스 성능을 최적화하고 정상적 기능을 수행할 수 있도록 정기 또는 수시로 시스템을 유지하고 관리·운영하는 것
 - 정보보호부문 자산 및 서비스, 인력 및 조직을 이용하거나 운영하는 것
- ‘정보기술부문 투자액’은 기업회계기준에 따라 발생주의*에 의하여 정보기술부문에 소요된 모든 비용(공시대상연도의 1월 1일부터 12월 31일까지 발생한 비용***)의 합계를 말함. 여기에 포함될 수 있는 항목은 다음과 같음.

* 발생주의: 회계처리를 하는 방법의 하나로, 현금 유출입 시점에 관계 없이 거래나 그 밖에 경제적 가치가 창출·변형·교환·이전·소멸되는 시점에 거래를 기록하고 표시하는 것을 말함.

** 기업별 회계연도에 불구하고 정보의 적시성을 위하여 정해진 기간 동안 발생한 비용임.

- ① 인건비, ② 정보처리시스템 구입비 및 임차료, ③ 정보처리시스템 유지보수비, ④ 정보기술 서비스 이용료, ⑤ 정보기술 외주용역비, ⑥ 정보기술 컨설팅 비용, ⑦ 정보기술 교육·훈련비, ⑧ 통신회선 이용료, ⑨ 기타 정보기술 관련 비용 및 자산 감가상각비 등

※ 기업별 특성에 따라 비용원장 등에 표기되는 상세 계정명은 서로 다를 수 있음.

유의 사항

- ▶ (자산) 토지·건물·구축물·건설 중인 자산·차량운반구·인테리어 자산·각종 가구(의자, 책상 등)·영업권·회원권 관련 감가상각비 등은 투자액에 포함되지 않음.
- ▶ (비용) 광고·마케팅 비용, 건물·시설 이용료, 건물·시설 공사비, 전기·전화 등 각종 세금과 공과금 및 사업성 경비, 영업외비용 등은 정보기술부문 투자액에 포함되지 않음.

- 정보기술부문을 전담하지 않은 조직이 집행한 비용이라도 명백하게 정보기술부문과 관련하여 투자한 금액이면 정보기술부문 투자액에 포함됨.

참고

정보기술부문 항목별 세부 내용

| 항목 | 세부 내용 |
|----------------------------|---|
| 인건비 | 정보기술부문과 관련하여 기획·개발·운영·유지·보수를 수행하는 내부인력(정규직 및 계약직 포함)의 인건비 및 복리후생비 등 관련 경비 일체 ※ 계열회사의 직원이 사내에서 근무하는 대가로 계열회사에 지급한 비용은 인건비가 아닌 외주용역비로 처리함. |
| 정보처리시스템 구입비 및 임차료 | 정보기술부문과 관련하여 하드웨어·소프트웨어를 구입 또는 임차(리스)하는 데 소요되는 경비 일체 |
| 정보처리시스템 유지보수비 | 정보처리시스템의 성능을 최적화하고 정상적 기능을 수행할 수 있도록 정기 또는 수시로 정보처리시스템을 유지하고 관리하는 데 소요되는 경비 일체(정보 처리시스템 관련 소모품 교체 비용 포함) |
| 정보기술 서비스 이용료 | 정보처리시스템 및 정보기술부문과 관련하여 필요한 서비스를 이용하는 데 소요되는 경비 일체(소프트웨어 라이선스 비용, 기술이전·이용료, 정보이용료, 특허 사용료, 정보보호관제·인증·재해복구 등 정보보호 서비스 이용료 포함) |
| 정보기술 외주용역비 | 외부 주문 또는 제휴 등에 따라 정보처리시스템과 관련하여 기획·개발·운영·유지·보수의 일부 또는 전부의 업무를 외부업체에 위탁(아웃소싱)하여 수행하는 데 소요되는 경비 일체 |
| 정보기술 컨설팅 비용 | 정보처리시스템 및 정보기술부문과 관련하여 외부기관으로부터 자문·점검·분석·평가·인증·심사·연구·조사에 소요되는 경비 일체(감리비, 국제표준인증심사비, 품질인증심사비 등 포함) |
| 정보기술 교육·훈련비 | 정보처리시스템 및 정보기술부문과 관련하여 임직원의 교육, 직무훈련·연수 및 회의·행사에 소요되는 경비 일체 |
| 통신회선 이용료 | 정보처리시스템과 관련하여 정보의 송·수신과 정보처리시스템 간 접속·연계를 위하여 정보통신사업자(인터넷 서비스 제공자 포함)로부터 전용회선 등 통신회선을 이용하는 데 소요되는 경비 일체(재해복구센터용, 디도스 공격 대응용 통신회선 이용료 등 포함) |
| 기타 정보기술 관련 비용 및 자산 감가상각비 등 | 기타 '정보기술부문'과 관련하여 지출한 경비 및 전년도 말 잔존 내용연수가 남아 있는 유·무형자산 등의 당기 감가상각비 일체 |

유의 사항

- ▶ '정보기술부문'은 '정보보호부문'을 포함함. 따라서 '정보기술부문 투자액'은 '정보보호부문 투자액'보다 크거나 같아야 함.

- ‘정보기술부문 인력’은 정보기술부문 관련 다음 항목 중 어느 하나에 해당하는 내·외부 인력*을 말함.

* 내부인력은 입사·퇴사·인사 이동일을 기준으로 일수 계산한 월평균 인력 수를, 외주인력은 계약상 투입공수를 기준으로 월평균 인력 수를 계산함.

- 임직원 중 내부 규정에 따라 IT 기획·개발·운영 등 정보기술부문의 업무를 전담하는 조직에 소속된 정규직·계약직 근로자
- 정보기술부문을 전담하지 않은 조직에 소속된 근로자라고 하더라도 다른 업무를 겸임하지 않고 정보 기술부문 업무만을 전담하는 근로자(전담부서가 아니더라도 실제 정보기술 업무를 전담하고 있으면 정보기술부문 인력으로 인정)
- 외주인력 중 공시대상기업의 정보기술부문 업무를 적법한 절차에 의하여 수행하는 근로자

■ 정보보호부문 판단 기준

- ‘정보보호부문’이란 다음 각 활동을 위한 기업의 관리적·기술적·물리적 자산 및 서비스, 인력 및 조직, 인증·평가·점검, 내·외부 활동을 말함. 다만 인력 및 조직에서 기업의 출입 통제, 보안경비 등 물리보안 관련 인력은 제외함.
 - 정보의 수집·가공·저장·검색·송신·수신 중에 발생할 수 있는 정보의 훼손·변조·유출 등을 방지 및 복구하는 것
 - 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것
 - 그 밖에 사이버 안전을 위한 관리적·기술적·물리적 수단을 운영하는 것
- ※ 관리적·기술적·물리적 수단에는 △정보보호 계획의 수립 및 시행 등(관리적 수단), △암호기술, 접근통제, 백업체제 등(기술적 수단), △출입통제, 시건장치, 장비 고도화 등(물리적 수단) 다양한 형태와 방식이 있음.
- ‘정보보호부문 투자액’은 ‘정보기술부문 투자액’과 동일하게 기업회계기준에 따라 발생 주의에 의하여 정보보호부문에 소요된 모든 비용(공시대상연도의 1월 1일부터 12월 31일까지 발생한 비용)의 합계를 말함. 여기에 포함될 수 있는 항목은 다음과 같음.
 - ① 인건비, ② 정보보호시스템 구입비 및 임차료, ③ 정보보호시스템 유지보수비, ④ 정보보호 서비스 이용료, ⑤ 정보보호 외주용역비, ⑥ 정보보호 컨설팅 비용, ⑦ 정보보호 교육·훈련비, ⑧ 정보보호 관련 통신회선 이용료, ⑨ 기타 정보보호 관련 비용 및 자산 감가상각비 등
- ※ 기업별 특성에 따라 비용원장 등에 표기되는 상세 계정명은 서로 다를 수 있음.

참고**정보보호부문 항목별 세부 내용**

| 항목 | 세부 내용 |
|----------------------------|--|
| 인건비 | 정보보호부문과 관련하여 기획·개발·운영·유지·보수를 수행하는 내부인력(정규직 및 계약직 포함)의 인건비 및 복리후생비 등 관련 경비 일체 |
| 정보보호시스템 구입비 및 임차료 | 데이터 백업, 자료유출방지, 침입차단시스템 등 정보보호시스템과 관련하여 하드웨어·소프트웨어를 구입 또는 임차(리스)하는 데 소요되는 경비 일체 |
| 정보보호시스템 유지보수비 | 정보보호시스템의 성능을 최적화하고 정상적 기능을 수행할 수 있도록 정기 또는 수시로 정보보호시스템을 유지하고 관리하는 데 소요되는 경비 일체(정보보호 시스템 관련 소모품 교체 비용 포함) |
| 정보보호 서비스 이용료 | 정보보호관제·인증·재해복구 등 정보보호 서비스 이용료, 정보보호 소프트웨어 라이선스 비용, 정보보호기술 이전·이용료 등 정보보호시스템 및 정보보호부문과 관련하여 필요한 서비스를 이용하는 데 소요되는 경비 일체 |
| 정보보호 외주용역비 | 정보보호시스템과 관련하여 기획·개발·운영·유지·보수의 일부 또는 전부의 업무를 외부업체에 위탁(아웃소싱)하여 수행하는 데 소요되는 경비 일체 |
| 정보보호 컨설팅 비용 | 정보보호 표준 인증심사, 모의해킹 훈련 등 정보보호와 관련하여 외부기관으로부터 점검·분석·평가·인증·심사 등에 소요되는 경비 일체 |
| 정보보호 교육·훈련비 | 정보보호부문과 관련하여 임직원의 교육, 전담인력 직무훈련·연수 등에 소요되는 경비 일체 |
| 정보보호 관련 통신회선 이용료 | 재해복구센터 운영, 디도스 공격 대응 등과 관련하여 전용회선을 이용하는 데 소요되는 경비 일체 |
| 기타 정보보호 관련 비용 및 자산 감가상각비 등 | 기타 '정보보호부문'과 관련하여 지출한 경비 및 전년도 말 잔존 내용연수가 남아 있는 유·무형자산 등의 당기 감가상각비 일체 |

- ‘정보보호부문 전담인력’은 정보보호부문 관련 다음 항목 중 어느 하나에 해당하는 내·외부 인력*을 말하며, 기업의 출입통제·보안경비 등 물리보안 관련 인력은 제외함.

* 내부인력은 입사·퇴사·인사 이동일을 기준으로 일수 계산한 월평균 인력 수를, 외주인력은 계약상 투입공수를 기준으로 월평균 인력 수를 계산함.

- 임직원 중 내부 규정에 따라 정보보호 업무를 전담하는 조직에 소속된 정규직·계약직 근로자
- 정보보호부문을 전담하지 않은 조직에 소속된 근로자라고 하더라도 다른 업무를 겸임하지 않고 정보 보호부문 업무만을 수행하는 근로자
- 외주인력 중 사업자의 정보보호부문 업무를 적법한 절차에 의하여 수행하는 근로자

3 | 이행 절차 및 협택

■ 한눈에 보는 정보보호 공시 이행 절차

‘정보기술부문’은 포괄적으로, ‘정보보호부문’은 보수적으로 산정함.

* 정보기술부문과 정보보호부문 중 어느 하나에 해당하는지가 모호한 내용에 대해서는 정보기술부문은 포괄적으로, 정보보호부문은 보수적으로 산정함.

| 순서 | 내용 | | |
|----|--|----------|--|
| 1 | 협의체(TF팀) 구성 | | |
| 2 | 자료 준비 | 투자 | 정보보호 최고책임자(CISO) 주관하에 정보보호, 정보기술, 재무회계, 인사관리, 급여 담당, 공시 담당자 등으로 ‘정보보호 공시 협의체(TF팀)’ 구성·운영 |
| | | 인력 | 공시대상연도의 별도기준 감사보고서, 합계잔액시산표, 자산대장, 비용 원장, 외주용역비 내역, 정보기술부문/정보보호부문 전담인력 관련 인건비 내역 등 |
| | | 인증·평가·점검 | 원천징수이행상황신고서, 정보기술부문/정보보호부문 직무 기술서, 업무분장표, 외주인력 현황 |
| | | 활동 | 정보보호 관련 인증서, 결과보고서, 점검결과서 등 |
| 3 | 총 임직원 수 산정 | | 정보보호 관리 인력 수(직무 기술서, 업무분장표, 외주인력 현황 등)와 정보기술부문/정보보호부문 전담인력 수(별도기준 감사보고서, 합계잔액시산표, 자산대장, 비용 원장, 외주용역비 내역 등)의 합계로 산정 |
| 4 | 정보기술부문/정보보호부문 인력 산정 | | 정보보호 관리 인력 수(직무 기술서, 업무분장표, 외주인력 현황 등)와 정보기술부문/정보보호부문 전담인력 수(별도기준 감사보고서, 합계잔액시산표, 자산대장, 비용 원장, 외주용역비 내역 등)의 합계로 산정 |
| 5 | 정보기술부문/정보보호부문 투자 산정 | | ① 유·무형자산(감가상각비), ② 비용(자산과 인건비 제외), ③ 인건비(내부인력)의 합계로 정보기술부문/정보보호부문 투자액 산출 |
| 6 | 인증·평가·점검 및 정보보호 활동 현황 증적 취합 | | 정보보호 관련 인증·평가·점검 증적 자료 및 정보보호를 위한 활동 현황 증적 자료를 확인하여 하나의 파일에 취합 |
| 7 | 정보보호 현황 서식 작성 | | 위에서 작업한 정보기술부문/정보보호부문 투자액과 정보보호 활동 현황 등을 정보보호 현황 서식에 기입 ※ 모든 산출 작업 자료는 공시내용 검증을 위하여 보관이 필요함. |
| 8 | 최고경영자 확인 | | 완성된 정보보호 현황 서식 및 공시내용 검증 동의서에 정보보호 공시자의 최고경영자의 승인·결재 직인 |
| 9 | 정보보호 공시내용 입력·확인 | | 과학기술정보통신부 전자공시시스템에 입력·확인 |

■ 정보보호 공시 이행 절차

(1) 협의체 구성

- 기업의 경영 활동에 관련한 제반 자료 및 증빙을 수집·정리하여야 하기 때문에 CISO의 주관하에 정보보호, 정보기술, 재무회계, 인사관리, 급여담당, 공시 담당자 등으로 ‘정보보호 공시 협의체(TF팀)’ 구성·운영을 권고함.

▣ 참고

정보보호 공시 협의체 구성(안)

| 구분 | 세부 역할 |
|--------|---|
| 정보보호 | CISO - 정보보호 공시 협의체 총괄 업무 수행 |
| | 실무자 - 정보보호부문 인력, 자산, 투자내역 분류 및 정확성 검토 - 정보보호 인증·평가·점검 및 활동 내역 제공 - 정보보호 공시 이행 및 후속조치 관련 대응 |
| 정보기술 | - 정보기술부문 인력, 자산, 투자내역 분류 및 정확성 검토 |
| 재무회계 | - 공시대상연도 비용원장, 자산대장 및 당기 감가상각 내역 제공 - 퇴직급여산정(DB, DC), 사용권자산, 매출원가 회계처리 방법에 관한 회계처리 설명 등 지원 |
| 인사관리 | - 전사조직도, 부서별 업무분장표 - 정보기술부문/정보보호부문 인력별 직무기술서, 인별 인사정보(부서, 직무 등 자료 제공) |
| 급여담당 | - 정보기술부문/정보보호부문 인별 급여 등(급여, 상여, 인별 복리후생비, 인별 회계상 퇴직급여자료) 인건비의 자료 제공* - 무형자산 및 연구개발비 등 자본화된 인건비 대상 인력 리스트 |
| 공시 담당자 | - 기업공시 담당 |

* 기업의 보안 등의 사유로 인별 인건비를 제공하기 어려울 경우 인별 정보기술부문/정보보호부문의 인사정보를 기초로 정보기술부문/정보보호부문의 인건비를 산정한 후 공시에 활용할 수 있도록 하되, 그 상세 자료는 공시내용 검증 등을 위하여 보관함.

(2) 자료 준비

- 모든 자료는 정보보호 공시대상연도 1월 1일부터 12월 31일까지 발생하였거나 그 기간의 전부 또는 일부를 포함하는 활동을 기준으로 준비함.

 참고

정보보호 공시 항목별 필요 자료 및 검토 내용

| 공시 항목 | 세부 항목 | 필요 자료명(예시) | 검토 내용 |
|-----------------|---------------------------|--|---|
| 투자 현황 | 기초자료 | - 별도기준 감사보고서, 합계잔액 시산표 | - 정보기술부문/정보보호부문 관련 계정과목 및 상세 계정 확인 |
| | 비용 | - 비용원장, 주요 거래 계약서, 산출 내역서 등 | - 정보기술부문/정보보호부문 투자 유형별 금액 산정 |
| | 자산 | - 자산대장, 구매계약서 등 | - 정보기술부문/정보보호부문 자산별 당기 감가상각비 산정 |
| | 인건비 | - 연봉계약서, 급여대장 등 | - 정보기술부문/정보보호부문 내부 인력 확정 후 산정 |
| 인력 현황 | 총 임직원 | - 원천징수이행상황신고서(1~12월) | - 간이세액에 기입된 인원 수를 12개월 평균으로 산정 |
| | 정보기술부문/ 정보보호부문 내부인력 | - 정보기술부문/정보보호부문 인력 명단 - 개인별 업무분장표/직무기술서 | - 정보기술부문 담당인력 식별(전담·겸직 여부 확인) - 정보보호부문 담당인력 식별(전담·겸직 여부 확인) |
| | 정보기술부문/ 정보보호부문 외주인력 | - 정보기술부문/정보보호부문 외주 현황 및 계약서 | - 정보기술부문 외주 용역별 월평균 투입공수 - 정보보호부문 외주 용역별 월평균 투입공수 |
| | CISO·CPO 지정 현황 | - 인사명령·지정신고서 - 대내외 활동 기록 | - CISO·CPO의 임원 여부, 겸직 여부 확인 - CISO·CPO의 대내외 주요 활동 현황 (특기 사항) |
| 인증·평가· 점검 현황 | 정보보호 인증 | - 정보보호 관련 인증 신청서, 인증서 등 | - 인증명, 인증유효기간, 갱신여부 등 확인 |
| | 정보보호 평가 | - 정보보호 관련 평가 신청서, 결과 보고서 등 | - 평가명, 평가유효기간, 평가 등급 등 확인 |
| | 정보보호 점검 | - 정보보호 관련 점검결과서 등 | - 점검명, 점검기관, 유효기간, 결과 등 확인 |
| 활동 현황 | 투자 활성화 | - 활동 계획 품의서, 결과보고서 등 | - 정보보호 관련 정책 수립, 교육, 캠페인 등 내역 및 활동 횟수 확인 |
| | 임직원 인식 제고 | | |
| | 전담인력 관리 | | |
| | 이용자 보호 활동 | | |

(3) 정보보호 현황 작성 및 승인

- CISO 주관하에 정보보호, 정보기술, 재무회계, 인사관리, 급여담당, 공시 담당자 등이 협업하여 고시 [별표3] 공시내용 양식에 따라 정보보호 현황을 작성함.
 - 차후 공시내용 검증 대상에 선정되었을 경우를 대비하여 정보보호 현황 작성에 사용되었던 자료는 최소 1년 이상 별도 보관 또는 기록이 필요함.
- 정보보호 공시자의 최고경영자는 확정된 정보보호 현황을 최종적으로 확인하고 승인·결재함.
 - 최고경영자의 승인·결재를 통하여 CISO가 주관하여 공시하는 정보보호 현황은 기업의 책임하에 제공되는 사항임.

(4) 정보보호 공시내용 입력·수정

- 매년 6월 30일까지 최고경영자가 승인·결재한 정보보호 현황[‘정보보호 공시내용 양식 + 공시내용 검증 동의서’ 또는 ‘정보보호 공시내용 양식 + 사전점검확인서(공시용) + 사전점검확인서(조서용)’]을 과학기술정보통신부 전자공시시스템(isds.kisa.or.kr)*에 입력함(필수 사항).
 - 과학기술정보통신부 전자공시시스템에 입력한 자료 또는 기업이 입력한 수치에 누락이나 오기된 사항이 있는지 등을 확인하여야 함.
 - * 공시 기업 회원가입 및 이용방법 등 세부 사항은 과학기술정보통신부 전자공시시스템에 게시된 ‘정보보호 공시 종합포털 안내서’ 안내서를 참고함.
 - 정보보호 현황을 자율적으로 작성한 상장기업은 한국거래소 자율공시시스템(KIND, 공시유형: 자율공시/정보보호)에 정보보호 현황을 공시할 수 있음(선택 사항).
- ※ 유가증권시장 공시규정 시행세칙 제8조, 코스닥시장 공시규정 시행세칙 제13조, 코넥스시장 공시규정 시행세칙 제9조
- 정보보호 공시 의무자는 6월 말까지 정보보호 공시를 이행하지 않을 경우 최대 1천만 원 이하의 과태료가 부과됨.

- 6월 말 이후 정보보호 공시내용의 수정이 필요한 경우 고시 [별표3의2] 공시내용 수정 사유서 양식에 그 내용을 작성하여 제출하고, 전자공시시스템에 이미 입력된 자료 등을 수정하여야 함.



법적 근거

정보보호 공시에 관한 고시 제3조(공시방법 및 절차)

① 법 제13조제1항 또는 제2항에 따라 정보보호 공시를 하려는 자는 [별표3]의 양식에 따른 공시내용과 [별표4]의 양식에 따른 정보보호 공시내용 검증 동의서를 작성하여 영 제8조제5항에 따른 전자공시시스템(이하 “전자공시시스템”이라 한다)에 입력하여야 한다. 다만 회계법인 또는 정보시스템감리법인으로부터 공시내용 사전점검을 받은 기관·단체는 [별표4]를 제외하고, 사전점검 수행을 확인할 수 있는 확인서를 입력하여야 한다.

② 한국인터넷진흥원은 전자공시시스템에 입력된 공시내용에 최고경영자의 승인 누락이 있는지 등을 확인 한다.

③ 법 제13조제1항에 따라 공시하려는 자 중 「자본시장과 금융투자업에 관한 법률」 제159조에 따른 사업 보고서 제출대상 법인은 같은 법 제391조에 따라 공시내용을 한국거래소가 운영하는 전자공시시스템에 공시할 수 있다.

④ 제1항에서 제3항의 규정에 따라 공시를 이행한 자(이하 “정보보호 공시자”라 한다)는 정보통신 서비스 이용자가 언제든지 공시내용을 열람할 수 있도록 정보보호 공시자의 인터넷 홈페이지 등에 공시내용을 게시할 수 있다.

정보보호 공시에 관한 고시 제4조(공시내용의 변경)

① 정보보호 현황의 변동으로 인하여 공시내용의 수정이 필요한 경우, 정보보호 공시자는 변동사항 사유발생일 다음날까지 [별표3의2] 양식에 따른 수정 사유서를 작성하여 과학기술정보통신부장관에 신고하여야 한다.

② 제1항에 따른 공시내용의 변경에 관하여는 제3조의 규정을 준용한다.

예시 공시내용 수정 사유서

공시내용 수정 사유서

2024년 7월 30일

1. 수정대상 공시내용: '24년 정보보호 공시내용

2. 수정대상 공시내용 최초제출일: 2024년 6월 1일

3. 수정 사항

| 항목* | 수정사유 | 수정 전 | 수정 후 | |
|------------------------|---------------------------------|--|------------------|-----------------|
| 정보보호 투자 현황 | 정보기술부문 투자액 | - 산정 오류(2023년도 취득자산의 취득 가액만 반영) - 비용 누락(기존 공시 시 IT팀의 비용 원장만 검토) | 50,452,520원 | 65,581,652원 |
| | 정보보호부문 투자액 | - 산정 오류(2023년도 취득자산의 취득 가액만 반영) - 비용 누락(기존 공시 시 IT팀의 비용 원장만 검토) - 비용 과다산정(정보보호와 무관한 소프트웨어 및 솔루션 구매 비용 포함) | 1,025,548원 | 713,520원 |
| 정보보호 인력 현황 | 정보기술부문 인력 | - 정보보호부문 전담인력 미포함(1.5명) - 기존 공시한 정보기술부문 인력 중 2명이 정보기술부문 외 다른 업무(인사) 수행 | 5명 | 4.5명 |
| | 정보보호부문 전담인력 | - 정보보호부문 전담 외주인력 투입공수 오류(1명 → 0.5명), 내부인력은 동일 (1명) | 2명 | 1.5명 |
| | | - CPO 임명 내용 누락 | CPO 지정 현황 미기재 | CPO 지정 현황 기재 |
| 인증, 평가, 점검 등에 관한 사항 | - ISO 27001 인증서 누락 | 0건 | 1건 | |
| 정보보호를 위한 활동 현황 | - '내부회계관리 운영'은 정보보호 활동 에서 제외 | 5건 | 4건 | |

* 불필요한 항목 삭제 가능

OO기업 대표이사 OOO

(직인)

■ 제도 이행 혜택

(1) 정보보호 및 개인정보보호 관리체계 인증수수료 할인(자율공시에 한함)

- 자율공시 기업이 매년 6월 30일까지 정보보호 현황을 공시한 경우에는 공시 시점부터 1년 내에 정보보호 및 개인정보보호 관리체계(ISMS 또는 ISMS-P) 인증심사(최초·갱신·사후 심사) 수수료 30% 할인 가능함.
 - 인증심사 수수료 산정 내역에서 '수수료 감면'란에 있는 정보보호 공시기업을 선택하여 심사기관에 제출하면 수수료를 30% 할인받을 수 있음.
- ※ 2023년 3월 1일에 정보보호 공시를 자율적으로 이행할 경우 혜택 효력은 2024년 2월 말까지 유지되고 효력 기간 안에 진행하는 최초심사·사후심사·갱신심사에 모두 할인 혜택이 적용됨.



법적 근거

정보보호산업의 진흥에 관한 법률 제13조(정보보호 공시) ② 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. 법 제13조제1항에 따른 공시일 것
 2. 법 제41조제1항제1호의2에 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 [별표6]의 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)

- 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 보여 줄 수 있음.

예시 정보보호 투자 우수기업 표시

6

2022

기업명



우편 및 통신업

2022-06-21



법적 근거

정보보호 공시에 관한 고시 제7조(정보보호 투자 우수기업 표시) 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 자가 정보보호 공시를 한 경우에는 영 제8조제5항에 따른 전자공시시스템에 정보보호 투자 우수기업 표시를 부여할 수 있다.

1. 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」 제47조에 따른 정보보호 관리체계 인증을 받은 자
2. 법 제12조에 따른 정보보호 준비도 평가 AA등급 이상을 받은 자

(3) 정보보호 공시 우수 기관·단체의 선정(자율·의무공시)

- 공시 성실성 및 다양한 정보보호 노력 평가를 통하여 정보보호 공시 우수 기관·단체를 선정하며, 과학기술정보통신부장관에 의한 표창을 수여함.
 - 정보보호 공시 우수 기관·단체는 고시에 따라 전자공시시스템에서 아래와 같이 별도 우대 표시를 할 수 있으며, 표창을 받은 날로부터 1년 동안 공시내용 검증 대상 면제 등의 혜택을 받을 수 있음.

예시 정보보호 공시 우수기업 표시

5

2021



기업명



우편 및 통신업

2021-06-21



법적 근거

정보보호 공시에 관한 고시 제8조(정보보호 공시 우수 기관·단체 선정) ① 과학기술정보통신부장관은 정보보호 투자 확대와 성실공시 풍토조성을 위하여 노력한 정보보호 공시자에 대하여 정보보호 공시 우수 기관·단체로 선정할 수 있다.

② 과학기술정보통신부장관은 제1항에 따른 정보보호 공시 우수 기관 또는 단체에 대하여 각호의 혜택을 제공할 수 있다.

1. 정보보호 공시 우수 기관 또는 단체 증서 발급
 2. 영 제8조제5항에 따른 전자공시시스템 내 별도 우대 표시
 3. 「정보보호산업의 진흥에 관한 법률 시행규칙」(이하 '규칙'이라 한다.) 제3조의2에 따른 검증 면제
 4. 기타 과학기술정보통신부장관이 필요하다고 인정하는 사항
- ③ 제2항에 따른 정보보호 공시 우수 법인에 대한 혜택의 유효기간은 선정된 날부터 1년으로 한다.

(4) K-ESG 가이드라인 기본 진단항목 연계

- 정보보호 공시를 이행한 경우, K-ESG 가이드라인 사회 영역 정보보호 범주의 ‘정보보호 시스템 구축’ 항목 요건 일부를 충족함.

참고

K-ESG 가이드라인 주요 내용

| 구분 | 분류번호 | 영역 | 범주 | | | | | | | | | | | | | | | | | | | | |
|----------|---|-------|-------|-------|--|-----|--|-----|------------------------------------|-----|---------------------------------|-----|---|----------|-------|-------|-------|-------|----|-----|-----|-----|------|
| | S-8-1 | 사회 | 정보보호 | | | | | | | | | | | | | | | | | | | | |
| 항목 | 정보보호 시스템 구축 | | | | | | | | | | | | | | | | | | | | | | |
| 항목 설명 | <ul style="list-style-type: none"> 조직이 보유하고 있는 정보통신망 및 기타 정보자산 등의 안정성 이슈가 강조되고 있음. 이에 따라, 정보자산 해킹, 네트워크 침입 등의 외부공격과, 물리적/인적 오류로 인해 발생하는 장애에 대응할 수 있는 체계를 갖추고 있는지 확인 정보보호 최고책임자(CISO) 선임, 정보보호 시스템 인증, 모의해킹 등 취약성 분석, 정보보호 공시 이행 (의무 또는 자율), 정보보호 시스템 사고에 대비하기 위한 보험가입 여부 등을 점검 | | | | | | | | | | | | | | | | | | | | | | |
| 성과 점검 | <p>정보통신망 및 기타 정보자산 등을 체계적으로 관리하려는 조직의 노력 수준을 측정</p> <p>[데이터 원천] 정보보호 시스템 관리규정, 정보보호 추진 계획 및 결과, 정보보호 공시 내역 [데이터 기간] 직전 회계연도 [데이터 범위] N/A [데이터 산식] N/A</p> | | | | | | | | | | | | | | | | | | | | | | |
| 점검 기준 | <table border="1"> <tr> <td>요건1</td><td>등기임원이나 미등기임원(또는 이에 준하는 관리자급 구성원)을 정보보호 최고책임자(CISO)로 선임하고 있는 경우</td></tr> <tr> <td>요건2</td><td>정보보호 시스템의 안정성에 대해 제3자(또는 규제기관)의 인증을 획득하고 있는 경우</td></tr> <tr> <td>요건3</td><td>모의해킹 등 외부공격에 대한 취약성 분석을 실시하고 있는 경우</td></tr> <tr> <td>요건4</td><td>정보보호 공시(의무 또는 자율)사항을 이행하고 있는 경우</td></tr> <tr> <td>요건5</td><td>정보보호 시스템의 손상 또는 외부공격 등 정보보안 관련 사고에 대비하기 위한 보험에 가입하고 있는 경우</td></tr> </table> <p>점검 기준 적용방안(선택형)</p> <table border="1"> <tr> <th>1개 이하 총족</th><th>2개 총족</th><th>3개 총족</th><th>4개 총족</th><th>5개 총족</th></tr> <tr> <td>0점</td><td>25점</td><td>50점</td><td>75점</td><td>100점</td></tr> </table> | | | 요건1 | 등기임원이나 미등기임원(또는 이에 준하는 관리자급 구성원)을 정보보호 최고책임자(CISO)로 선임하고 있는 경우 | 요건2 | 정보보호 시스템의 안정성에 대해 제3자(또는 규제기관)의 인증을 획득하고 있는 경우 | 요건3 | 모의해킹 등 외부공격에 대한 취약성 분석을 실시하고 있는 경우 | 요건4 | 정보보호 공시(의무 또는 자율)사항을 이행하고 있는 경우 | 요건5 | 정보보호 시스템의 손상 또는 외부공격 등 정보보안 관련 사고에 대비하기 위한 보험에 가입하고 있는 경우 | 1개 이하 총족 | 2개 총족 | 3개 총족 | 4개 총족 | 5개 총족 | 0점 | 25점 | 50점 | 75점 | 100점 |
| 요건1 | 등기임원이나 미등기임원(또는 이에 준하는 관리자급 구성원)을 정보보호 최고책임자(CISO)로 선임하고 있는 경우 | | | | | | | | | | | | | | | | | | | | | | |
| 요건2 | 정보보호 시스템의 안정성에 대해 제3자(또는 규제기관)의 인증을 획득하고 있는 경우 | | | | | | | | | | | | | | | | | | | | | | |
| 요건3 | 모의해킹 등 외부공격에 대한 취약성 분석을 실시하고 있는 경우 | | | | | | | | | | | | | | | | | | | | | | |
| 요건4 | 정보보호 공시(의무 또는 자율)사항을 이행하고 있는 경우 | | | | | | | | | | | | | | | | | | | | | | |
| 요건5 | 정보보호 시스템의 손상 또는 외부공격 등 정보보안 관련 사고에 대비하기 위한 보험에 가입하고 있는 경우 | | | | | | | | | | | | | | | | | | | | | | |
| 1개 이하 총족 | 2개 총족 | 3개 총족 | 4개 총족 | 5개 총족 | | | | | | | | | | | | | | | | | | | |
| 0점 | 25점 | 50점 | 75점 | 100점 | | | | | | | | | | | | | | | | | | | |

4 | 공시내용 검증 방법 및 절차

■ 개요

- 정보보호 공시내용의 투명성과 신뢰성을 확보하기 위하여 과학기술정보통신부는 한국인터넷진흥원(이하 'KISA'라 한다.)을 통하여 공시 이행 기업의 공시 주요 내용의 정확성을 검증할 수 있음.
 - KISA 사전점검 지원을 받은 기업 또는 회계법인이나 정보시스템 감리법인으로부터 공시내용에 대하여 사전점검을 받고 사전점검 확인서(공시용, 조서용 2종)를 제출한 기업은 공시내용 검증 대상에서 제외될 수 있음.



법적 근거

정보보호산업의 진흥에 관한 법률 제13조(정보보호 공시) ④ 과학기술정보통신부장관은 제1항 또는 제2항에 따른 공시내용을 검증하고 공시내용이 사실과 다른 경우 수정을 요청할 수 있다.
⑤ 제4항에 따른 공시내용에 대한 검증 방법 및 절차 등 세부 사항은 과학기술정보통신부령으로 정한다.

정보보호산업의 진흥에 관한 법률 시행규칙 제3조의2(정보보호 공시내용의 검증 방법 및 절차) ① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원은 법 제13조제4항에 따라 같은 조 제1항 또는 제2항에 따른 공시 내용에 대한 검증을 연 1회 이상 실시할 수 있다.
② 한국인터넷진흥원은 법 제13조제1항 또는 제2항에 따라 정보보호 현황을 공시한 자(이하 이 조에서 '정보 보호공시자'라 한다.)에게 제1항에 따른 검증을 위하여 필요한 자료의 제출을 요청할 수 있다.
③ 한국인터넷진흥원은 제1항에 따른 검증을 위하여 정보보호·정보기술·회계 분야의 전문가로 구성된 공시 점검단을 운영할 수 있다.
④ 한국인터넷진흥원은 제1항에 따른 검증 결과 공시내용이 사실과 다른 경우에는 이를 과학기술정보통신부장관에게 보고하여야 한다.
⑤ 과학기술정보통신부장관은 제4항에 따라 보고받은 공시내용에 대한 검증 결과를 검토하여 공시내용의 수정이 필요하다고 인정하는 경우에는 해당 정보보호공시자에게 공시내용의 수정을 요청할 수 있다.
⑥ 제1항부터 제5항까지의 규정에 따른 정보보호 공시내용에 대한 검증 방법 및 절차, 수정 요청 등에 관한 세부 사항은 과학기술정보통신부장관이 정하여 고시한다.

정보보호 공시에 관한 고시 제10조(공시내용의 검증) ① 한국인터넷진흥원은 정보보호 공시자 중 다음 각 호의 어느 하나에 해당하는 자(이하 '검증대상자'라 한다.)에 대하여 검증을 수행할 수 있다.
1. 공시내용을 누락하였거나 영 제8조제6항에 따른 공시기한을 준수하지 않은 자
2. 공시내용에 오류가 있다고 인정할만한 사유가 있는 자
3. 그 밖에 한국인터넷진흥원이 정보보호 공시 신뢰성 확보를 위하여 검증이 필요하다고 인정한 자
② 제1항에도 불구하고 한국인터넷진흥원은 다음 각 호에 해당하는 자를 검증대상자에서 제외할 수 있다.

1. 제3조제1항 단서에 따라 사전점검을 수행하고 확인서를 제출한 정보보호 공시자
 2. 제8조제1항에 따른 정보보호 공시 우수 기관·단체
- ③ 한국인터넷진흥원은 공시내용 검증을 위하여 검증대상자에게 자료 제출을 요구하는 경우 서면으로 통지하여야 한다.
- ④ 한국인터넷진흥원은 규칙 제3조의2제1항에 따라 다음 각 호의 사항을 검증한다.
1. 공시내용의 누락 여부 및 미작성 사유
 2. 공시내용의 정확성
 3. 다른 법령 등에 따라 제출 또는 공개된 자료와의 상충성 등

■ 검증 세부 방법 및 절차

(1) 공시점검단 구성·운영

- KISA는 공시내용의 검증을 위하여 정보보호·정보기술·회계 분야의 전문성을 갖추고 정보보호 현황 자료에 대하여 판단 기준을 제시할 수 있는 전문가로 구성된 공시점검단을 운영함.

(2) 검증 대상 선정

- KISA는 ① 공시내용을 누락하였거나 영 제8조제6항에 따른 공시기한을 준수하지 않은 경우, ② 공시내용에 오류가 있다고 인정할 만한 사유가 있는 경우, ③ 그 밖에 KISA가 정보보호 공시 신뢰성을 확보하기 위하여 검증이 필요하다고 인정한 경우 중 어느 하나에 해당하는 기업에 대하여 공시내용 검증을 수행할 수 있음.
 - 다만 당해연도 사전점검을 수행하고 확인서를 제출한 기업이나 직전연도 정보보호 공시 우수기업은 검증에서 제외할 수 있음.

(3) 검증 실시

- 기업이 정보보호 현황을 공시하기 위하여 사용되었던 자료를 기초로 고시 및 가이드라인에 따라 정보보호 현황을 적정하게 산정하였는지 등을 확인하고 검토함.
 - 검증은 기업의 검증 자료 준비도에 따라 평균 2~4주 소요되며, 기업은 아래 참고에 나열된 정보보호 공시내용 검증 준비 자료를 기한 내에 제출하여야 함.

※ 검증 전, 검증 대상 개별 안내 및 공시내용 검증 준비 자료에 관한 집합교육을 실시할 수 있음.



법적 근거

정보보호 공시에 관한 고시 제10조(공시내용의 검증) ① 한국인터넷진흥원은 정보보호 공시자 중 다음 각 호의

어느 하나에 해당하는 자(이하 '검증대상자'라 한다.)에 대하여 검증을 수행할 수 있다.

1. 공시내용을 누락하였거나 영 제8조제6항에 따른 공시기한을 준수하지 않은 자
 2. 공시내용에 오류가 있다고 인정할 만한 사유가 있는 자
 3. 그 밖에 한국인터넷진흥원이 정보보호 공시 신뢰성 확보를 위하여 검증이 필요하다고 인정한 자
- ② 제1항에도 불구하고 한국인터넷진흥원은 다음 각 호에 해당하는 자를 검증대상자에서 제외할 수 있다.
1. 제3조제1항 단서에 따라 사전점검을 수행하고 확인서를 제출한 정보보호 공시자
 2. 제8조제1항에 따른 정보보호 공시 우수 기관·단체
- ③ 한국인터넷진흥원은 공시내용 검증을 위하여 검증대상자에게 자료 제출을 요구하는 경우 서면으로 통지하여야 한다.
- ④ 한국인터넷진흥원은 규칙 제3조의2제1항에 따라 다음 각 호의 사항을 검증한다.
1. 공시내용의 누락 여부 및 미작성 사유
 2. 공시내용의 정확성
 3. 다른 법령 등에 따라 제출 또는 공개된 자료와의 상충성 등

참고

정보보호 공시내용 검증 준비 자료

① 정보기술부문/정보보호부문 투자 현황

- 1) 정보보호 공시 투자 현황 산출자료 일체
- 2) 별도기준 감사보고서[별도재무제표의 재무상태표 및 주석 사항 중 유·무형자산(사용권자산 포함), 손익 계산서에서 매출원가, 판매비와 일반관리비]
- 3) 합계잔액시산표[유·무형자산, 매출원가, 판매비와 일반관리비 상세 계정(예: 통신비, 지급수수료, 소모품비 등)]
- 4) 비용원장 원본 및 분류내역: 공시대상연도 회계결산 완료된 자료
 - 공시대상연도 1월 1일부터 12월 31일까지의 비용원장(전표일자, 계정명, 부서명, 적요, 금액 등 표시)
 - 분류대상 계정의 비용원장별 정보기술부문/정보보호부문 분류내역 및 집계자료
 - 외주비 관련 상세 자료: 정보기술부문/정보보호부문 관련 외주비 내역(기안, 계약서 등)
- 5) 감가상각자산대장 원본 및 분류내역: 공시대상연도 회계결산 완료된 자료
 - 시산표상 정보기술부문/정보보호부문 검토 대상 자산으로 분류된 자산 계정의 자산대장(자산명, 취득일, 취득가액, 내용연수, 장부가액, 감가상각비 등 표시)
 - 분류대상 계정의 자산대장별 정보기술부문/정보보호부문 분류내역 및 집계자료

② 정보기술부문/정보보호부문 전담인력 현황

- 1) 정보기술부문/정보보호부문 조직 구분을 위한 근거자료
 - 전사 조직도
 - 조직별 주요 업무 설명 자료

- 2) 정보기술부문/정보보호부문 전담인력 현황 산정 및 인건비 비용 산정 근거자료(내부인력, 외주인력 포함)
- 정보기술부문/정보보호부문 전담인력 입·퇴사일 정보
 - 정보기술부문/정보보호부문 전담인력 R&R 자료(정보기술부문/정보보호부문 직무기술서)
 - 정보기술부문/정보보호부문 전담인력 급여, 상여, 퇴직급여, 복리후생비 등 인건비 자료
 - 정보기술부문/정보보호부문 외주인력(상주, 비상주) 외주인력 현황
- 3) 총 임직원 수 산정 근거자료
- 월별 원천징수이행상황 신고서(공시대상연도 전체 월별 간이세액 수)

③ 정보보호 인증·평가·점검 등에 관한 사항

정보보호 인증·평가·점검 등에 대한 증적 자료
(예) ISMS 인증, 클라우드 서비스 인증, ISO 27001 등 인증서류

④ 정보보호 활동 현황

정보보호 활동 증적 자료(정보보호 활동 증빙서류, 공식 기안 내용, 활동사진, 이미지 캡처본 등)

⑤ CISO·CPO 지정 현황

직책, 임원 여부, 겸직 여부 등에 대한 증적 자료

- CISO·CPO 지정 및 자격증빙(위촉장, 지정신고서 등) 제출

(4) 공시내용 검증 결과 확인 및 조치

- 검증 결과에서 허위공시 등으로 판단한 경우에는 그 내용을 심의위원회에 전달하여 공시 내용 수정 요청에 관한 사항을 최종 심의하고, 수정공시가 이루어질 수 있도록 기업을 지원함.
- 수정공시 대상 기업은 고시 [별표3] 정보보호 공시내용 양식 수정본과 [별표3의2] 공시 내용 수정사유서를 작성하여 전자공시시스템에 재입력하여야 함.
 - 공시 내용의 검증을 거부 또는 방해하거나 수정 요청에 따르지 않을 경우 최대 1천만 원 이하의 과태료가 부과됨.
- 수정공시 등 시정조치 요구에 응하지 않아 공시가 취소되는 경우 공시 혜택은 취소되며, 따라서 정보보호 관리체계 인증 수수료의 할인받은 금액도 반납하여야 함.
 - 한국거래소 상장공시시스템(KIND)에 공시한 경우 거래소 공시 규정에 따른 공시 위반 제재 조치를 받을 수 있음.



법적 근거

정보보호산업의 진흥에 관한 법률 제41조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제13조제2항을 위반하여 정보보호 현황을 공시하지 아니한 자
- 1의2. 제13조제4항에 따른 공시내용의 검증을 거부 또는 방해하거나 수정 요청에 따르지 아니한 자

정보보호 공시에 관한 고시 제13조(수정 요청) ① 과학기술정보통신부장관은 제11조제1항에 따른 심의 결과에 따라 공시내용의 수정이 필요하다고 인정하는 경우에는 해당 검증대상자에게 수정 요청 내용과 그 사유를 통지하여야 한다.

- ② 제1항에 따라 공시내용 수정 통지를 받은 검증대상자는 [별표3]의 양식에 수정한 공시내용 및 [별표3의 2] 양식에 따른 수정 사유서를 작성하여 전자공시시스템에 입력하여야 한다.
- ③ 한국인터넷진흥원은 제1항에 따른 수정 요청 내용대로 공시내용이 전자공시시스템에 입력되었는지 확인한다.

정보보호 공시
가이드라인



Guidelines for
Information Security Disclosure

공시내용 작성 방법

-
1. 정보보호 투자 현황 산출 방법
 2. 정보보호 인력 현황 산출 방법
 3. 정보보호 인증·평가·점검 등에 관한 사항
 4. 정보보호를 위한 활동 현황

II 공시내용 작성 방법

1 | 정보보호 투자 현황 산출 방법

■ 개요

- 정보기술부문/정보보호부문 투자액은 정보기술부문/정보보호부문 관련 ① 유·무형자산(감가상각비), ② 비용(자산의 감가상각비와 인건비 제외), ③ 인건비(내부인력)의 합계로 산출함.
 - 유·무형자산의 경우 자산대장 등을 활용하여 산출할 수 있으며, 당기 감가상각비를 투자액으로 산정함.
 - 비용의 경우 비용원장 등을 활용하여 산출할 수 있으며, 지급수수료·외주용역비 등 상세 계정 중에서 정보기술부문/정보보호부문 관련 비용을 투자액으로 인정함.
 - 인건비는 정보기술부문/정보보호부문 전담인력에 속하는 내부인력(정규직·계약직)의 급여, 상여, 퇴직급여, 복리후생비의 합계를 말함.

▣ 참고

정보보호 투자 현황 준비 자료

| 준비 자료 | 필요 내용 | 비고 |
|------------|---|-----------------|
| 조직도 | 공시대상연도의 조직도 | 정보기술·정보보호 조직 확인 |
| 별도기준 감사보고서 | 별도재무제표의 재무상태표 및 주석 사항의 유·무형자산(사용권 자산 포함), 손익계산서의 매출원가, 판매비와 일반관리비 | |

| 준비 자료 | 필요 내용 | 비고 |
|----------------------------|--|-----------------------------|
| 합계잔액시산표 | 유·무형자산, 매출원가, 판매비와 일반관리비 상세 계정(예: 통신비, 지급수수료, 소모품비 등) | |
| 공시대상연도 말 자산대장 | 유·무형자산으로 등록한 자산의 감가상각계상 대장(자산명, 취득일, 취득가액, 내용연수, 장부가액, 감가상각비 등 표시) | 공시대상 기간 감가상각비 |
| 공시대상 기간의 비용원장 | 공시대상연도 1월 1일부터 12월 31일까지의 비용원장(전표 일자, 계정명, 부서명, 적요, 금액 등 표시) | |
| 외주용역비 내역 | 정보기술부문/정보보호부문 외주비 상세 내역(기안서, 계약서 등) | 정보기술부문/ 정보보호부문 용역비 산정 |
| 정보기술부문/정보보호부문 인원 관련 인건비 | 공시대상연도에 근무한 정보기술부문/정보보호부문 인력의 급여, 상여, 퇴직급여, 복리후생비 합계 | |

■ 회계 정합성 검토

- 별도기준 감사보고서(세무조정계산서 포함, 이하 동일)를 바탕으로 자료를 작성할 때 가장 중요한 작성 원칙은 자료의 신뢰성과 완전성을 확보하는 것으로, 감사보고서상 자산 및 비용 합계와 합계잔액시산표(이하 ‘시산표’라 한다.)의 자산 및 비용 합계를 비교하여 신뢰성을 확보하여야 함.

- 투자액을 산정할 때 검토하는 시산표는 감사보고서상 계정보다 상세 계정들로 구성되므로 시산표와 감사보고서는 동일한 금액이어야 하며, 따라서 감사보고서와 시산표의 합계를 비교하여 동일한 자료인지 확인하는 작업이 우선됨.

※ 별도기준 감사보고서는 금융감독원 전자공시시스템(dart.fss.or.kr)에서 회사의 사업보고서를 조회한 후 첨부란의 ‘감사보고서’를 선택하며, 감사보고서 주석 사항의 유형자산 및 무형자산, 사용권자산의 장부가액, 감가상각비를 추출함. 사업보고서가 없는 회사는 외부감사 관련 ‘감사보고서’를 선택함.

※ 시산표는 과목 중 유·무형자산 및 사용권자산의 장부가액 및 감가상각비(매출원가 및 판매비와 일반관리비 포함), 감가상각비 외 비용과목(매출원가 및 판매비와 일반관리비 포함)을 추출함.

유의 사항

- 기간통신사업 매출액이 800억 원 이상으로 과학기술정보통신부로부터 영업보고서를 검증받는 기간통신 사업자는 일반적인 검토원칙을 준수하되 추가 자료 검토가 필요함(세부 내용은 [첨부 3] 참고).

- 감사보고서와 시산표를 통하여 자산 및 비용 금액을 비교한 후에는 시산표상 계정을 검토하여 정보기술부문/정보보호부문 대상 계정을 추출하여 해당 계정의 자산대장 및 비용원장의 합계금액이 시산표상 계정 금액과 일치하는지 비교함.
 - 정보기술부문/정보보호부문 금액 산정을 위해서는 시산표상 계정별 잔액보다 상세 내용이 필요하기 때문에 자산의 경우 자산대장 비용은 계정별 비용원장을 추가로 확인하여야 함.
 - 다만 검토 대상이 되는 자산대장이나 비용원장이 시산표상 금액과 일치하는지를 비교해 봄으로써 해당 계정이 모든 내용을 포함하는지 판단할 수 있게 되며, 이로써 자료의 완전성을 확보함.

※ 예를 들어, 시산표 계정 중 기계장치가 취득가액 10억 원인 경우 기계장치 자산대장 상 모든 자산(기계장치에 속하는 자산)의 취득가액 합계 금액이 10억 원인지를 비교하여야 기계장치 중 누락된 자산 없이 정보기술·정보보호 금액을 산정할 수 있음.

유의 사항

- ▶ CISO 주관하에 공시 자료를 작성하더라도 투자액 산정을 위해서는 회계 지식이 필수적으로 필요하므로 최고재무관리자(CFO) 및 회계 담당자의 확인하에 투자액이 산정되어야 함.
- 분야별로 전문부서의 책임자가 참여하여 투자 현황을 작성하고 CISO가 전체 공시 자료를 총괄 주관함. 이를 위하여 이 가이드라인에서도 정보보호 공시 이행을 위한 협의체를 구성하도록 권고하고 있음.

■ 자산 투자 현황

참고

정보기술부문/정보보호부문 투자액 집계표

| 구분 | 정보기술부문 투자액* | 정보보호부문 투자액 |
|-----------------|-------------|------------|
| ① 유·무형자산(감가상각비) | | |
| ② 비용(① 및 ③ 제외) | | |
| ③ 인건비(내부인력) | | |
| 합계 | | |

* 정보기술부문 투자액은 반드시 정보보호부문 투자액을 포함하여 산정함.

- 별도기준 감사보고서상 ① 유·무형자산 주석 사항의 자산별 취득가액, 장부가액, 감가상각비 등이 시산표상 유·무형자산(사용권자산 포함)의 계정별 취득가액, 장부가액, 감가상각비 등과 일치하는지 확인함.

※ 유·무형자산은 별도감사보고서상 주석 사항에 자산별로 상세 정보가 기재되어 있으므로 자산별(기계장치, 비품, 공구 비품 등) 금액과 시산표상 해당 자산계정의 금액이 일치하는지 검토함.

- 시산표상 재무상태표 유·무형자산의 △정보기술부문, △정보보호부문, △제외자산*을 분류 구분함(아래 시산표 예시 참고).

* 시산표상 자산명 자체가 제외 대상인 경우에 해당하며, 자산계정 특성상 정보기술·정보보호·제외자산이 명확히 구분되지 않으면 검토 대상으로 분류하여 자산대장에서 상세 검토함.

- (유형자산) 유형자산 중 토지, 건물, 구축물, 차량운반구, 인테리어 자산, 각종 가구(의자 책상 등), 건설 중인 자산은 검토 대상에서 일괄 제외되므로 산업별로 차이는 있으나 보통 기계장치, 공구비품, 전산비품 등이 검토 대상임.

※ 투자부동산은 투자목적의 유형자산으로 사용목적이 아닌 관계로 감가상각을 인식하지 않으므로 검토 제외 대상임.
그러나 사용권자산 계정은 유형자산과 동일한 기준을 적용하여 토지·건물 등 부동산 관련 사용권 자산은 제외하고, 기계장치·전산비품 등의 사용권 자산은 검토 대상임.

- (무형자산) 무형자산 중 영업권, 고객가치, 방송프로그램, 회원권, 건설 중인 자산은 검토 대상에서 제외됨.

※ 무형자산을 임차하여 사용권자산 계정이 무형자산 부문에서도 발생할 수 있으며, 유형자산과 마찬가지로 무형자산의 원칙을 준용하여 제외 대상과 검토 대상을 분류함.

- 회계팀에 유·무형자산 상각대장 및 사용권자산 상각대장 중 시산표상 제외자산 이외의 나머지를 요청하거나, 전체 상각대장 요청 시 제외자산은 별도로 분류함.

- 시산표상 검토 대상 유·무형자산을 분류한 후에는 해당 자산의 자산대장을 확보하여 자산대장에서 자산별로 ① 정보기술부문, ② 정보보호부문, ③ 제외(해당 없음)로 구분 표기하고, 해당 사유를 비고로 기재함.

- 자산별로 ① 정보기술부문, ② 정보보호부문, ③ 제외(해당 없음)로 구분하는 것은 기본적으로는 이 가이드라인에서 제시하고 있는 자산분류표 등을 참고하되, 자산분류표는 일반적인 사항을 제시하는 것이므로 분류표에 없는 자산의 경우 해당 부서를 통하여 자산의 성격을 규정할 필요가 있음.

※ 구분 표기 외에도 해당 사유의 기재를 요청하는 이유는 회사의 자료관리 차원에서도 필요하며, KISA의 공시내용 검증 시 대응하기 위하여 필수적으로 필요하기 때문임.

예시 감사보고서 및 시산표 정합성 검토

① 감사보고서 주석

10. 유형자산:

가. 당기 및 전기 중 유형자산의 변동 내역은 다음과 같습니다.

(1) 당기

| 구분 | 토지 | 건물및구축물 | 기계장치 | 건설중인자산 | 기타 | (단위: 백만원) 계 |
|--------------|-----------|--------------|--------------|------------|------------|--------------|
| 기초장부금액 | 7,800,435 | 19,087,134 | 43,749,609 | 13,994,259 | 1,535,487 | 86,166,924 |
| - 취득원가 | 7,801,259 | 28,992,675 | 146,778,918 | 13,994,259 | 3,535,985 | 201,103,096 |
| - 감가상각누계액 | -824 | -9,905,541 | -103,029,309 | - | -2,000,498 | -114,936,172 |
| 일반취득 및 자본적지출 | 5,295 | 4,385,819 | 31,501,402 | 1,339,173 | 607,076 | 37,838,765 |
| 감가상각 | -406 | ④ -1,614,006 | -18,016,803 | - | -532,894 | -20,164,109 |
| 처분_폐기 | -24,319 | -5,104 | -108,737 | - | -5,402 | -143,562 |
| 기타 | -11 | -12,027 | 9,842 | -25,930 | -2,867 | -30,993 |
| 기말장부금액 | 7,780,994 | ① 21,841,816 | 57,135,313 | 15,307,502 | 1,601,400 | 103,667,025 |
| - 취득원가 | 7,782,125 | 33,244,532 | 175,487,461 | 15,307,502 | 4,022,759 | 235,844,379 |
| - 감가상각누계액 | -1,131 | -11,402,716 | -118,352,148 | - | -2,421,359 | -132,177,354 |

11. 무형자산:

가. 당기 및 전기 중 무형자산의 변동 내역은 다음과 같습니다.

(1) 당기

| 구분 | 산업재산권 | 개발비 | 회원권 | 기타 | (단위: 백만원) 계 |
|-------------|-------------|----------|---------|------------|-------------|
| 기초장부금액 | 1,195,319 | 371,392 | 194,277 | 5,241,660 | 7,002,648 |
| 개별취득 | 286,963 | - | 4,329 | 3,610,518 | 3,901,810 |
| 내부개발에 의한 취득 | - | 193,708 | - | - | 193,708 |
| 상각 | ⑤ -218,754 | -321,608 | - | -1,851,408 | -2,391,770 |
| 처분_폐기 | -42,031 | - | - | -557 | -42,588 |
| 순상(환입) | - | - | -3,471 | - | -3,471 |
| 기타 | 4,744 | -6,582 | - | -1,043 | -2,881 |
| 기말장부금액 | ④ 1,226,241 | 236,910 | 195,135 | 6,999,170 | 8,657,456 |

12. 사용권자산

가. 사용권자산의 변동 내역은 다음과 같습니다.

(1) 당기

| 구분 | 토지 | 건물및구축물 | 기계장치 | 기타 | (단위: 백만원) 계 |
|--------|-------|---------|-----------|---------|-------------|
| 기초장부금액 | 2,593 | 144,615 | - | 188,236 | 405,873 |
| 일반취득 | 91 | 446,071 | 75,103 | 992 | 451,828 |
| 감가상각 | -405 | -80,085 | ⑥ -36,065 | -9,617 | -126,172 |
| 계약의 해지 | - | -28 | - | -1,131 | -1,159 |
| 기타 | - | -45 | - | - | -45 |
| 기말장부금액 | 2,279 | 510,528 | ③ 39,038 | 178,480 | 730,325 |

② 시산표

| *기준년도 | *회계정코드 | *회계정명 | 금액 | *구분 | 비고 |
|-------|----------|-------------------|--------------|-----|----|
| 2021 | 12301000 | 토지 | 7,782,125 | BS | 제외 |
| 2021 | 12302000 | 건물 | 32,244,532 | BS | 제외 |
| 2021 | 12303000 | 감가상각누계액 | -10,902,716 | BS | 제외 |
| 2021 | 12304000 | 구축물 | 1,000,000 | BS | 제외 |
| 2021 | 12305000 | 감가상각누계액 | ① -500,000 | BS | 제외 |
| 2021 | 12306000 | | 2,452,482 | BS | 검토 |
| 2021 | 12307000 | 산업재산권 | ④ -1,226,241 | BS | 검토 |
| 2021 | 12308000 | 상각누계액 | | BS | 검토 |
| 2021 | 12309000 | 사용권자산_기계장치 | ③ 75,103 | BS | 검토 |
| 2021 | 54410010 | 감가상각비_건물 | ④ -36,065 | BS | 검토 |
| 2021 | 84410010 | 감가상각비_구축물 | ④ -10,000 | PL | 제외 |
| 2021 | 54410030 | 무형자산상각비_산업재산권 | ⑤ -218,754 | PL | 검토 |
| 2021 | 83241000 | 감가상각비_사용권자산(기계장치) | ⑥ -36,065 | PL | 검토 |

유의 사항

- ▶ 검토 대상 자산 상각대장에 누락이 없는지 확인하기 위하여 유·무형자산 상각대장 및 사용권자산 상각대장의 취득가액, 장부가액, 감가상각비, 감가상각누계액이 시산표 금액과 일치하는지 확인하여야 함.
- ▶ 정보기술·정보보호 대상 설비 등의 임차 관련 사용권자산의 감가상각비는 정보기술부문/정보보호부문 투자액에 포함되어야 함. 다만 토지, 건물, 구축물, 차량운반구의 임차 관련 사용권자산의 감가상각비는 제외함.
- ▶ 사용권자산 중 검토 대상 자산이 있는 경우 해당 자산에 대한 투자액은 사용권자산에 대한 감가상각비로 자산대장 검토 시 별도 산정되므로 비용원장 검토 시 관련 비용 중복하여 산정되지 않도록 주의가 필요함.

- 유·무형자산 상각대장 및 사용권자산 상각대장상 자산명별로 △정보기술부문, △정보보호부문, △제외자산을 분류하고 정보기술부문/정보보호부문으로 분류된 자산의 감가상각비 합계액을 유·무형자산의 투자액으로 확정함.
 - 정보보호부문 자산에 대한 투자액을 산정할 때 정보보호 전용 제품만을 인정하고 있어, 정보보호 기능을 별도로 분리·산정할 수 없는 유형자산의 투자금액(감가상각비)은 정보보호부문 투자로 인정하지 않음.

유의 사항

- ▶ 정보보호부문 자산이 다른 자산의 부속품으로 포함되어 자산대장상 별도 자산으로 분류되지 않는다면 정보보호부문 자산으로 인정하지 않음.
- ▶ 시산표상 동일한 기계장치 계정이더라도 자산대장상에서는 자산에 따라 정보기술부문/정보보호부문/제외로 분류될 수 있으며, 정보보호부문 자산이 회사의 자산 분류 정책에 따라 다른 자산의 부속품으로 포함되어 자산대장상 별도 자산으로 분류되지 않는다면 해당 자산은 정보보호부문 자산으로 인정하지 않음.

참고

정보기술부문/정보보호부문 자산 분류

| | |
|-----------------|---|
| 정보기술부문 자산 인정 | 사용부서와 관계 없이 회사 내 모든 PC와 부속장치, 모니터, 프린터, 복합기, TV(모니터 대용), 의료정보시스템, 원격회의 시스템(소프트웨어), 스캐너, 태블릿 등 [첨부 1] 참고 |
| 정보보호부문 자산 인정 | 문서파쇄기(세단기), 노트북 케이블 락, 모니터 보안경, 보안 USB 등 물리적 보안 제품(CCTV*, 바이오인식, 접근제어, 알람모니터링 등) * 본사에서 통제·관리하는 시스템 및 전산실 보안용 설비는 정보보호투자로 인정하나, 단순 대리점, 공장 등 출입 감시용 및 단순 판매 목적은 제외(정보보호 자산의 입증 책임은 회사에 있음.) |
| | 재해·재난 등에 따른 서비스 중단을 대비하여 구축하는 백업 서버 등의 재해복구시스템. 다만 원격지 소산이 아닌 일반 백업 투자는 정보보호부문으로 인정하지 않음. |
| | 「정보보호산업의 진흥에 관한 법률」에 따라 지정된 우수 정보보호 제품 |

| | |
|------------------|---|
| 정보기술부문 자산 불인정 | 영상·음향 장비(전산실 외), 조명 장비, 의료기기 등 |
| 정보보호부문 자산 불인정 | 물리적 망분리를 위한 PC 등 정보보호 기능이 일부 내재된 제품 및 정보보호 전용제품이 아니지만 정보보호를 목적으로 구입한 제품* * 물리적 망분리를 위한 PC 등은 정보보호 자산은 아니지만 정보기술에는 포함 |

예시 정보기술부문/정보보호부문 자산 분류

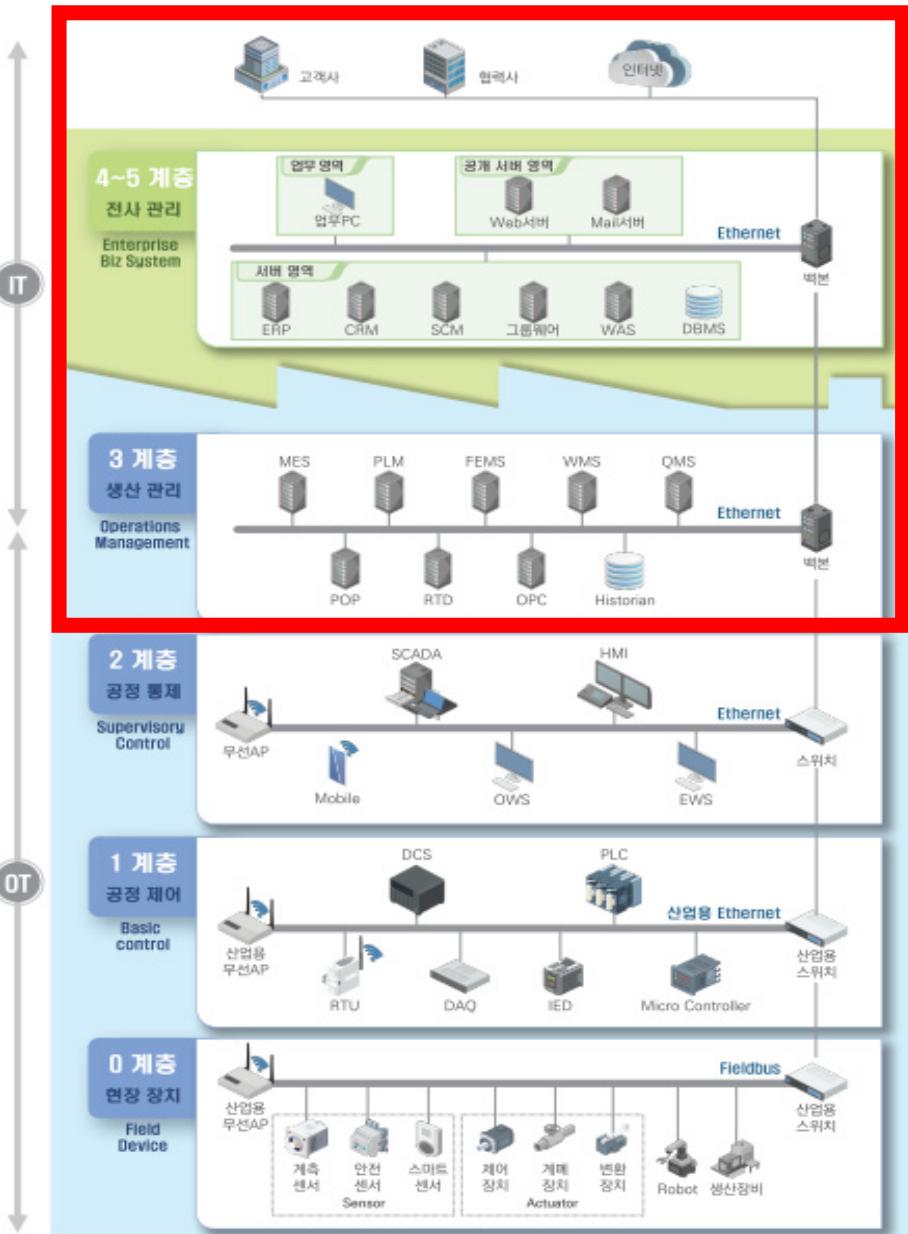
| 자산명 | 자산 계정 | 취득일 | 취득 가액 | 감가 상각비 | 감가 누계액 | 자산 분류 | | |
|-------------------|----------|---------------|--------|--------|--------|-------|-------|----|
| | | | | | | 정보 기술 | 정보 보호 | 제외 |
| 노트북 | 공기구 비품 | 2022. 1. 1. | 1,000 | 500 | 500 | ○ | | |
| 서버 | 공기구 비품 | 2020. 12. 31. | 5,000 | 1,000 | 2,000 | ○ | | |
| 소프트웨어 자산관리 솔루션 | 무형-소프트웨어 | 2021. 6. 30. | 200 | 40 | 60 | ○ | | |
| 스위치 | 비품-전산 장비 | 2019. 1. 1. | 500 | 100 | 400 | ○ | | |
| 방화벽 | 비품-전산 장비 | 2020. 9. 1. | 600 | 120 | 280 | ○ | ○ | |
| DB 암호화 | 무형-소프트웨어 | 2021. 5. 1. | 300 | 60 | 100 | ○ | ○ | |
| 본사 건물 | 유형-건물 | 1990. 1. 1. | 10,000 | 250 | 8,000 | | | ○ |
| 합계 | | | 17,600 | 2,070 | 11,340 | | | |

- 스마트공장* 등 Operation Technology의 경우 정보보안 대상 범위 중요성 등을 종합적으로 고려하여 전사관리 및 공장별 생산관리체계까지의 자산(3~5계층 하드웨어·소프트웨어)만을 정보기술부문으로 판단함.

* 스마트공장은 제품 기획·개발부터 양산까지, 주문에서부터 완제품 출하까지, 제조 관련 모든 과정을 말하며, 응용 시스템뿐 아니라 현장 자동화와 제어자동화 영역까지 공장 운영의 모든 부문을 포함함.

참고

스마트공장 내 정보기술부문/정보보호부문 자산



※ 계층별 서비스 예시 및 보안 요구 사항 등에 대한 세부 내용은 스마트공장 사이버 보안 가이드(2019. 12.), 스마트 공장 보안모델 해설서(2022. 12.) 참고

■ 비용 투자 현황

참고

정보기술부문/정보보호부문 투자액 집계표

| 구분 | 정보기술부문 투자액* | 정보보호부문 투자액 |
|-----------------|-------------|------------|
| ① 유·무형자산(감가상각비) | | |
| ② 비용(① 및 ③ 제외) | | |
| ③ 인건비(내부인력) | | |
| 합계 | | |

* 정보기술부문 투자액은 반드시 정보보호부문 투자액을 포함하여 산정함.

- 자산 투자 현황 산출방법과 마찬가지로 별도기준 감사보고서와 시산표의 계정과목별 일치 여부를 확인한 뒤 시산표에서 매출원가, 판매비와 일반관리비 항목 중 정보기술부문 /정보보호부문 관련 비용이 포함될 수 있는 상세 계정을 검토함.

- 기업의 회계계정 분류체계에 따라 다를 수 있지만 포함될 수 있는 상세 계정*으로 통신비, 지급임차료, 전산유지비, 전산용품 구입비, 사무용품비, 소모품비, 지급수수료, 외주용역비, 보험료, 수선비, 교육·훈련비, 경상연구개발비 등이 정보기술부문/정보보호부문에 포함될 수 있는 항목임.

* 회사별로 다양한 비용 계정이 있을 수 있으므로 회사별 계정 목록을 고려하여 비용 산정 시 누락이 없도록 주의가 필요함.

- 상세 계정 중 판단이 어려운 계정은 비용원장의 적요 등을 검토하여 정보기술부문/정보보호부문 해당 여부를 판단함.

유의 사항

- ▶ 매출원가는 복잡한 과정을 거쳐 시간 차이를 두고 원가로 인식됨. 그 과정에서 당해연도에 즉시 비용 처리되는 비용(당기 매출원가)도 존재하고 재고자산(기말제품)으로 자산화되었다가 다음해 매출원가(다음해 기초 제품)으로 처리되는 경우 등이 있어 시기별로 명확히 분류하는 것이 어려움.
- ▶ 따라서 당해연도 발생한 제조원가를 당해연도 정보기술부문 및 정보보호부문 검토 대상으로 포함함.

- 인건비성 경비(급여, 상여, 퇴직급여, 복리후생비 등)와 감가상각비, 영업외손익(기타 수익, 기타 비용, 금융수익, 금융 비용, 손상차손), 사업성 경비는 비용 투자 현황을 작성할 때 정보기술부문/정보보호부문 검토 대상에서 제외함.

- 인건비성 경비(급여, 상여, 퇴직급여, 복리후생비 등)는 정보기술부문/정보보호부문 인력이 확정된 후 별도로 인별 인건비를 산정하기 때문에 비용 투자 현황을 작성할 때 제외함.
 - 감가상각비는 자산 투자 현황을 작성할 때 자산대장에서 별도 추출하므로 비용 투자 현황을 작성할 때 제외함.
 - 영업외손익 중 기타 수익과 기타 비용은 주로 유형자산 처분이익, 임대료수익, 배당금수익 등 성격이며, 금융수익과 금융 비용은 이자수익, 이자 비용, 외환손익 등 금융 활동과 관련된 손익으로 정보기술부문 /정보보호부문 검토 대상에서 제외함.
 - 유·무형자산 손상차손은 영업외비용으로 회계처리하기 때문에 정보기술부문/정보보호부문 검토 대상에서 제외함.
 - 그 밖에 비용 성격상 투자금액에 산정하지 않는 계정*으로 회의비, 식사비, 접대비, 교통비, 출장비, 물류비, 잡비, 차량유지비, 광고선전비, 각종 마케팅 관련 비용, 제세공과금, 대손상각비, 포장비 등은 검토 대상에서 일괄 제외함.
- * 정보기술부서 또는 정보보호부서에서 발생한 비용이더라도 위의 비용은 정보기술부문/정보보호부문 투자금액으로 보지 않음.

유의 사항

- ▶ 최초 별도기준 감사보고서와 시산표를 요청할 때 모든 비용에 대한 비용원장을 요청할 수도 있으나 자료 양이 방대하므로 우선 감사보고서와 시산표를 비교하여 완전성을 확보한 후 시산표 내에서 검토 대상 비용 계정을 분류하여 해당 비용에 대한 비용원장만 요청하는 것이 효율적임(최초 자료를 요청할 때 향후 추가 검토 대상 비용에 대하여 비용원장 추가 요청할 수 있음을 안내하는 것을 주천함).
- ▶ 비용 중 검토 대상 비용 계정의 비용원장을 확보하면 비용 계정별 연중 발생금액 합계금액이 시산표와 일치하는지 한번 더 확인하여 자료의 신뢰성을 확보함.

- 시산표에서 계정이 확정되면 비용원장 추출 후 내역(계정, 적요, 부서 등)을 확인하여 정보 기술부문/정보보호부문으로 분류하며, 정보보호부문 투자는 반드시 정보기술부문 투자에 포함하여 산정함.

- 실제 발생 내용에 따라 분류하되, 적요가 불분명한 경우 정보기술부서에서 발생된 비용은 정보기술부문 투자로 분류하고, 정보보호부서에서 발생된 불분명한 비용일 경우 정보보호부문 투자로 보지 않음.

※ 예를 들어, 정보기술부서에서 소모품비의 적요가 없어 어떤 소모품을 구입하였는지가 불분명할 경우 포괄적으로 정보 기술부문 투자에 포함하고, 정보보호부서에서 발생된 소모품비이고 적요란이 불분명한 경우 정보보호부문 투자에는 포함하지 않음. 다만 다른 증빙을 통하여 소명 가능할 경우 정보보호부문 투자로 인정함.

- 어느 부서가 사용한 비용인지보다 해당 비용이 정보기술이나 정보보호를 위한 비용인지가 중요하며, 어느 부서가 사용하더라도 인정되는 비용으로는 PC(노트북 포함) 등 사용료(리스료) 및 유지보수 비용, IT 소모품 비용, IT 서비스 비용(클라우드 사용료, 전용회선료, 도메인 등록 비용, 인증서 비용)* 등을 예로 들 수 있음.

* 통신요금 중 전화요금, 영업성 문자 비용, TV 수신료, 뱅킹수수료 등은 제외함.

* 네트워크 장비 관련 비용은 포함되나, 네트워크 구축 및 공사 비용은 아래 범위 참고

참고

네트워크 공사의 유형 및 정보기술부문 인정 범위

| 비용/자산 범위 | 정보기술부문 여부 |
|--------------------|-----------|
| 회계상 구축물 처리 | 불인정 |
| 네트워크 장치 구입 및 설치 용역 | 인정 |
| 통신케이블 공사 | 불인정 |
| 단순 자리 배치 등 공사 | 불인정 |

예시

비용 원장 분류

| 전표일 | 상세 계정 | 적요 | 사용부서 | 금액 | 정보 기술 | 정보 보호 | 제외 |
|-------------|-------|---------------|------|-----|-------|-------|----|
| 2022. 1. 3. | 지급수수료 | 복합기 사용료 | IT팀 | XXX | ○ | | |
| 2022. 1. 4. | 지급수수료 | 복합기 사용료 | 영업팀 | XXX | ○ | | |
| 2022. 1. 4. | 외주용역비 | ERP 운영유지비(1월) | IT팀 | XXX | ○ | | |
| 2022. 1. 5. | 지급수수료 | 회계감사료 | 회계팀 | XXX | | | ○ |
| 2022. 2. 2. | 외주용역비 | ISMS 컨설팅 비용 | 보안팀 | XXX | ○ | ○ | |
| 2022. 2. 5. | 소모품비 | 백신 사용료 | 보안팀 | XXX | ○ | ○ | |
| 2022. 2. 5. | 소모품비 | (빈 칸) | IT팀 | XXX | ○ | | |
| 2022. 2. 5. | 소모품비 | (빈 칸) | 보안팀 | XXX | ○ | × | |
| 2022. 2. 6. | 통신비 | 전용회선료 | IT팀 | XXX | ○ | | |
| 2022. 3. 1. | 소모품비 | 인쇄용지 | 총무팀 | XXX | | | ○ |
| 2022. 3. 2. | 소모품비 | 인쇄용지 | 보안팀 | XXX | | | ○ |
| ... | | | | | | | |

* IT팀에서 소모품비로 분류하였으나 적요에 내역이 없거나 판단하기 어려울 경우 정보기술부문 투자로 분류하고, 보안팀에서 소모품비로 분류하였으나 적요가 없을 경우 정보보호로 분류하지 않음.

- 외주용역비의 경우 용역의 성격·내용 등을 파악하여 정보기술부문/정보보호부문 투자액을 산정함. 외주용역비의 경우 외부인력과 매핑하여 유의미한 의미를 가지는지 검토함으로써 인력과 비용의 신뢰성을 향상시킬 필요가 있음.

* 예를 들어, A사는 B사와 영업전산시스템 개발 용역을 체결하였으며 당해연도 B사 외주인력은 12M 동안 10명이었음 (외주인력 총 10명). 시장에서 대략 개발자의 1MM은 1천만 원 수준이라면 회사의 외주용역비는 약 12억 원 ($12M \times 10명 \times 1천만 원$) 수준과 유사한지 비교하여 용역비가 유의미하게 낮거나 높은 경우 외주인력 및 외주용역비가 잘못 산정되었을 가능성이 크므로 재검토할 필요 있음.

- 정보보호부문 관련 외주용역비는 보안관제, 보안컨설팅, 보안성 지속 서비스* 및 유지보수 등이 있음.

* 보안성 지속 서비스: 보안업데이트, 보안정책관리, 위협·사고분석, 보안기술 자문, 보안성 인증(KCMVP 등) 효력 유지 등
※ 정보보호 업무를 수행하는 전문 서비스 기업 목록은 KISA 또는 정보보호산업진흥포털(ksecurity.or.kr)에서 확인할 수 있음.

- 하나의 계약에 정보기술부문과 정보보호부문 통합 서비스를 제공받을 경우 계약서 상세 내역에 별도 구분 가능할 경우 분리할 수 있으며, 정보기술부문/정보보호부문 상세 내역이 없을 경우 정보기술부문으로만 분류함.

* 서비스 제공업체가 정보보호 공시를 한 경우에 한하여 '외부 정보기술 서비스 이용대가'에 서비스 제공업체의 '정보기술 부문 투자 대비 정보보호 투자 비율'을 곱하여 산정하는 것이 가능함.

* 예를 들어, A사가 B호스팅 업체의 호스팅 서비스를 이용하면서 서비스 이용에 따른 대가로 1,000만 원을 지불하였고, B호스팅 업체의 정보기술 투자 대비 정보보호 투자비율이 10%였다면 A사의 정보보호부문 투자액은 자체 정보보호 투자액에 100만 원($=1,000만 원 \times 10\%$)으로 집계 가능함.

- 공시 기업이 IDC 또는 클라우드 서비스를 제공받을 때 해당 서비스 제공업체의 계약서 또는 정산서에 정보보호 투자금액을 구분할 수 있을 경우 그 금액을 정보기술부문과 정보보호부문 투자액으로 산정함.

* 예를 들어, 정보기술부문(IT 인프라 운영)과 정보보호부문(보안관제)에 해당하는 업무가 계약서 상세 내역에 공수기준으로 분리되어 있다면 정보보호 부문에 공수비율만큼 분류 가능함.

유의 사항

- ▶ IDC의 코로케이션, 호스팅 서비스는 정보기술부문으로 인정되나, 단순 상면만 임대하는 파킹 서비스 이용료는 인정하지 않음.
※ 코로케이션: 네트워크접속+상면, 호스팅 서비스: 서버+네트워크접속, 파킹 서비스: 상면만 임대
- ▶ IDC 및 클라우드 서비스 제공사업자의 경우 모든 이용자에게 영향을 주는 일반적인 정보보호 투자와는 달리, 특정 고객사를 대상으로 하는 옵션 또는 추가 판매를 목적으로 하는 보안 솔루션에 대한 투자는 정보보호부문으로 인정하지 않음.

- 그룹사 간 경비절감을 위한 공동구매를 지주사 등에서 일괄 수행한 후 구매분담률만큼 부담하는 경우에는 서비스가 아닌 비용 공동구매이므로 구매분담률만큼 각자 투자액으로 산정함.
 - 비용 공동구매가 아닌 셰어드 서비스(shared service)*를 사용하는 기업의 경우 기본적으로 양사 간 합의된 내용으로 진행함.
 - 합의 내용이 없고 서비스 사용자별 투자금액 및 인력 구분이 어려울 때 서비스 제공사에서 서비스를 제공하기 위하여 투입된 인력·자산·비용 등 모든 정보기술부문/정보보호부문을 공시하고, 그룹사는 청구된 비용(서비스 비용)만을 정보기술 또는 정보보호로 분류함.
- * 셰어드 서비스: 이 가이드라인에서 의미하는 셰어드 서비스는 기업 간 공용으로 사용할 수 있는 IT 부문의 기능이나 서비스를 중앙화하여 SI(시스템 통합) 회사와 같은 서비스 제공자가 정보기술·정보보호 부문의 투자를 주도적으로 수행하고, 각 서비스 사용자에게 비용을 청구하여 제공하는 서비스를 의미함.

유의 사항

- ▶ 그룹사 간 경비절감을 위하여 지주사 등에서 공동구매를 일괄 수행한 후 구매 분담률만큼 부담하는 방식을 셰어드 서비스라고 하는 경우도 있으나, 해당거래는 단순 공동구매 형태임.
- ▶ 이러한 경우에는 공동구매를 일괄 수행한 지주사 등이 서비스 제공사로 보기 어려우므로 지주사 등 공동구매 사업자가 모두 공시하는 방법을 인정하지 않고 공동구매 분담률만큼 각 그룹사가 투자액을 인식하는 방안만 인정함.

예시 셰어드 서비스 관련 산정

- ① 서비스 제공자가 서비스 사용자별로 투입하는 투자액 및 인력의 공수를 구분할 수 있고, 서비스 사용자가 사용자의 투자금액 및 투입공수 인력을 사용자가 공시하기로 양쪽이 합의한 경우
 - 서비스 사용자와 서비스 제공자가 합의하여 공시하기로 한 각 사의 투자액 및 인력을 공시함.
※ 이 경우 서비스 제공자는 해당 인원 수와 인건비를 공시에서 제외함. 다만 협의 내용은 적절한 증빙자료로 문서화되어야 함.

(①-1) 서비스 사용자가 서비스 제공자에 인력배분을 요청하여 서로 합의한 경우

- 예를 들어, 서비스 사용자가 서비스 제공자에게 인력배분을 요청하여 서비스 제공자가 투입한 정보기술 인력 100명 중 서비스 사용자 사용분 60명을 제공할 것을 합의하였을 때, 서비스 제공자는 자사사용분 40명 및 인건비 40을 인식하고 서비스 사용자는 60을 인식함.

- 제공 서비스 기준으로 서비스 제공자가 정보기술부문 비용·자산을 각각 100원씩 투입하였고, 서비스 이용자가 해당 서비스 제공 대가로 180원을 청구하였다면 아래와 같이 각각 공시함.

| 구분 | 서비스 제공자 (그룹사 SI 제공업체) | 서비스 사용자 (그룹사) | |
|----------|--------------------------|---------------------|---|
| 수익 | 그룹사 청구 매출 인식 180 | | |
| 인원 수 | 40 | 60 | |
| 투자 금액 | 인건비 | 40(인원 수 40에 대한 인건비) | |
| | 비용 | 100 | 지급수수료 180 인식(자산, 인력, 비용의 청구 금액을 정보기술로 인식) |
| | 자산 | 100 | 0(*) |
| | 계 | 240 | 180 |

※ (주의 사항) 회계상 서비스 이용자는 지급수수료로 포함하여 계상하고 있으므로 별도 자산의 감가상각비로 계상할 경우 투자금액이 이중으로 발생될 수 있음.

② 서비스 제공자가 서비스 사용자별 투자금액 및 인력 구분이 어려운 경우 또는 서비스 관련 투자 금액과 인력이 서비스 제공자의 소유로 판단한 경우

- 서비스 제공자가 세어드 서비스를 제공하기 위하여 투입된 인력·자산·비용 등 모든 정보기술부문/정보 보호부문을 공시하고, 서비스 사용자는 청구된 비용(서비스 비용)만을 정보기술 또는 정보보호로 분류함.
- 예를 들어, 제공 서비스 기준으로 서비스 제공자가 정보기술부문 인력 100명, 정보기술부문 인건비·비용·자산을 각각 100원씩 투입하였고 서비스 이용자가 해당 서비스 제공 대가로 180원을 청구하였다면 아래와 같이 각각 공시함.

| 구분 | 서비스 제공자 (그룹사 SI 제공업체) | 서비스 사용자 (그룹사) | |
|----------|--------------------------|-----------------------|---|
| 수익 | 그룹사 청구 매출 인식 180 | | |
| 인원 수 | 100(그룹사 업무수행 인력 60 포함) | | |
| 투자 금액 | 인건비 | 100(인원 수 100에 대한 인건비) | |
| | 비용 | 100 | 지급수수료 180 인식(자산, 인력, 비용의 청구 금액을 정보기술로 인식) |
| | 자산 | 100 | |
| | 계 | 300 | 180 |

※ (주의 사항) 서비스 제공자가 세어드 서비스를 제공하기 위하여 소비한 자산 및 비용(인건비 제외)은 서비스 제공자의 투자액으로 공시되며, 서비스 사용자는 지급수수료만 공시대상임.

- 사용권자산에 대하여 자산 투자 현황을 작성할 때 감가상각비로 투자액을 인식하였음에도 불구하고 비용 투자 현황을 작성할 때 지급수수료나 임차료 계정을 통하여 이중으로 투자액을 산정하는 오류가 생기지 않도록 주의하여야 함.
- 일반적으로 사용권자산 대상 임차료 등 비용은 제외로 분류하고, 회사의 재무회계부서나 회계전문가와 협의하여 사용권자산 대상 비용이 무엇인지 검토하는 것이 이중 계상방지를 위한 실무적 접근 방법임.

유의 사항

- ▶ 리스 회계처리 대상 지급임차료의 경우 지급 시점에 비용으로 회계처리하고, 결산시점에 리스부채와 지급 임차료를 상계 처리함. 지급임차료 성격이 정보기술부문(또는 정보보호부문) 항목일 경우 차감된 지급 임차료(대변금액 또는 음수의 차변금액)도 동일하게 분류하여 상계처리되도록 함. 그 이유는 사용권자산의 감가상각비도 정보기술부문(또는 정보보호부문)으로 분류되므로 리스부채 조정 관련 임차료 비용이 차감되지 않을 경우 이중 계상될 수 있음.

(관련 분개)

- 지급임차료 지급 시
(차변) 지급임차료 XXX / (대변) 미지급금 XXX
- 결산 시 지급임차료의 리스부채 차감
(차변) 리스부채 XXX / (대변) 지급임차료 XXX

아래와 같이 지급임차료를 정보기술로 분류하였다면, 리스부채 상계처리 관련 지급임차료 마이너스 분개도 정보기술로 분류하여야 함.

| 전표일 | 상세 계정 | 적요 | 사용부서 | 금액 | 정보 기술 | 정보 보호 |
|--------------|-------|------------------|------|-----------|-------|-------|
| 2022. 2. 1. | 지급임차료 | 전용회선 임차료 | IT팀 | 100,000 | ○ | |
| 2022. 3. 31. | 지급임차료 | 리스부채 상계 -전용회선 | IT팀 | (100,000) | ○ | |

※ 리스부채 상계전표가 계약별(예: 전용회선 임차료과 같이 상세 단위별)로 구분되지 않을 경우 리스회계처리 관련 최초 비용 발생 전표를 정보기술(또는 정보보호)에서 제외하는 방안도 고려 가능함.

■ 내부인력 인건비 투자 현황

참고

정보기술부문/정보보호부문 투자액 집계표

| 구분 | 정보기술부문 투자액* | 정보보호부문 투자액 |
|-----------------|-------------|------------|
| ① 유·무형자산(감가상각비) | | |
| ② 비용(① 및 ③ 제외) | | |
| ③ 인건비(내부인력) | | |
| 합계 | | |

* 정보기술부문 투자액은 반드시 정보보호부문 투자액을 포함하여 산정함.

- 인건비는 급여, 상여, 퇴직급여, 복리후생비 등 손익계산서에 반영된 인건비성 경비로 구성됨.

- 내부인력의 정보기술부문/정보보호부문 전담인력이 확정된 후 해당 인력의 손익계산서상에 반영된 비용으로 인별 총급여(급여, 상여, 수당 등 근로소득으로 신고된 총 급여), 퇴직급여*, 복리후생비**등의 합을 정보기술부문 /정보보호부문 투자로 봄.

* 퇴직급여는 근로기준법상 1년 이상 근속 임직원을 대상으로 하므로 보통 회계적으로도 1년 이상 근속자에 대해서만 퇴직급여를 설정하고 있음.

** 4대 보험 회사부담분(근로자 부담분은 제외), 인별 귀속이 가능한 급여성 복리후생비(상품권, 스톡옵션, 우리사주, 기타 유가증권 등)

- 급여·상여 등은 인별 연봉계약서 또는 급여대장과 일치하여야 하며, 손익계산서상 비용(인건비)으로 처리된 항목이어야 함. 연말정산 시 지급받는 총 급여 자료에 기초할 경우 급여담당자는 공시대상 회계기간의 귀속연도를 확인할 필요가 있음.

※ 공시대상 회계기간과 회계상 회계연도가 다를 경우 회사 지급분을 반영하기 위하여 급여담당자에게 공시대상연도 (1~12월)에 반영된 급여만을 추출하도록 요청이 필요함.

예시

개인별 인건비 산출내역

| 사번 | 이름 | 부서 | 업무 | 급여 | 상여 | 퇴직 급여 | 4대보험 (회사) | 기타 |
|---------|-----|-------|------|--------|-------|----------|--------------|-----|
| 1975012 | 김○○ | IDC센터 | 프로그램 | 65,000 | 7,400 | 3,400 | 1,500 | 500 |
| 2005145 | 이△△ | 보안팀 | 보안관제 | 45,000 | 4,340 | 1,340 | 1,200 | 100 |
| : | : | : | : | : | : | : | : | : |

예시 인건비 집계내역

| 투자 구분 | 대상자 수 | 급여 (a) | 상여 (b) | 퇴직급여 (c) | 복리후생비(d) | | 총인건비 (a+b+c+d) |
|-------|-------|--------|--------|----------|----------|-------|-------------------|
| | | | | | 4대 보험 | 기타 복리 | |
| 정보기술 | 33 | 000 | 000 | 000 | 000 | 000 | 0,000 |
| 정보보호 | 8 | 000 | 000 | 000 | 000 | 000 | 0,000 |
| 합계 | 41 | 000 | 000 | 000 | 000 | 000 | 0,000 |

- 급여담당의 협의체 참여자는 충분한 정보보호 공시에 대한 이해가 있어야 하며, 급여 담당자가 직접 관련 인건비의 데이터를 추출하고 그 총액만을 집계에 사용함. 추후 사전 또는 공시내용을 검증할 때 상세 자료를 검증단에게 제출할 수 있도록 자료관리가 필요함.
 - 인별 급여자료를 기초로 산정하는 것이 원칙이나, 기업 조직의 정보기술 조직과 정보보호 조직이 전담하고 있고, 회계상 부서별 인건비가 구분될 경우 비용원장상 부서별 인건비를 기초로 투자액을 산정할 수 있음.
- 당기 중 인별 업무분장이 변경되어 정보기술·정보보호 업무가 변경될 경우 인건비도 업무 투입일수에 따라 안분계산하여 투자액에 반영함.

예시 인별 업무분장 변경 시 인건비 분류

① 김XX님의 인건비가 52,000천 원, 4월 14일 IT 부서에서 정보보호 부서로 업무 변경되고, 9월 10일자로 총무팀으로 업무 변경 시 아래와 같이 인건비를 산정함.

| 이름 | 부서 | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 계 | 연평균 | 정보기술 | 정보보호 |
|-----|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|--------|-------|------|------|
| 김홍길 | IT부서 | 1,000 | 1,000 | 1,000 | 0.467 | | | | | | | | | 3,467 | 0.289 | 0 | |
| | 정보보호 | | | 0.533 | 1,000 | 1,000 | 1,000 | 1,000 | 0.323 | | | | | 4,856 | 0.405 | 0 | 0 |
| | 총무팀 | | | | | | | | 0.677 | 1,000 | 1,000 | 1,000 | 1,000 | 3,677 | 0.306 | | |
| | 계 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 12,000 | 1,000 | | |

※ 인건비 배부의 정확성을 위하여 계상 인원 수는 최대 소수점 사용

- 4월 인원 수: 4월 14일 부서 이동 시 IT 부서는 0.467(14÷30), 정보보호부서는 0.533(16÷30)
- 9월 인원 수: 9월 10일 부서 이동 시 정보보호부서는 0.323(10÷31), 총무팀은 0.677(21÷31)

② 이에 따른 최종 김XX님의 인건비 배부 결과는 아래와 같음.

| 구분 | 연평균 | 금액 | 수식(인건비 × 부문연평균인원수/연평균인원수) |
|------|-------|------------|--------------------------------------|
| 정보기술 | 0.694 | 36,064,516 | $52,000 \times (0.289+0.405) \div 1$ |
| 정보보호 | 0.405 | 21,042,294 | $52,000 \times 0.405 \div 1$ |
| 제외 | 0.306 | 15,935,484 | $52,000 \times 0.306 \div 1$ |

※ 정보기술: 정보보호가 포함된 연평균 인원 수(정보기술 + 정보보호)

유의 사항

- ▶ 회계상 자본화 요건을 충족하는 무형자산 등으로 인건비가 포함될 경우 자산화 후 자산의 사용시점에 감가상각비로 회계처리되면서 자산의 투자로 인식되므로 관련 인건비는 정보기술부문/정보보호부문 투자에서 제외함.

※ 예를 들어, 소프트웨어를 개발 중인 회사가 그 인원의 인건비를 비용 회계처리하지 않고 ‘건설 중인 자산’ 등으로 회계처리할 경우 관련 인건비는 정보기술부문/정보보호부문 인건비로 보지 않음. 그 이유는 개발이 완료될 경우 무형자산(소프트웨어)으로 대체되고, 관련 소프트웨어의 감가상각비는 정보기술·정보보호 투자로 인식하기 때문에 소프트웨어에 포함된 인건비가 정보기술·정보보호 투자로 이중 계산될 수 있음.

- ▶ 회계상 경상연구개발비로 인건비가 포함될 경우 경상연구개발비의 성격에 따라 정보기술부문/정보보호부문 투자로 산정되므로, 관련 인건비는 인건비 항목의 투자에서 제외함.

※ 회사에서 프로젝트를 구성하고, 그 프로젝트에서 발생된 인건비와 경비 등을 경상연구개발비로 회계처리할 경우 경상연구개발비의 성격에 따라 정보기술부문/정보보호부문으로 분류하기 때문에 경상연구개발비에 포함된 인건비는 인건비가 아닌 경상연구개발비 항목으로 분류하여야 이중 계상되지 않음.

- 확정된 내부인력이 확정기여형(DC형)인지 확정급여형(DB형)인지 퇴직보험의 유형을 확인하여 인별 퇴직급여를 산정함.

- 확정기여형인 경우 손익계산서상 퇴직급여를 사외적립과 동시에 비용 처리하기 때문에 관련 비용을 퇴직급여로 산정함.

| | |
|------------------------|---|
| 확정기여형 퇴직연금 (DC형) | 회사가 매년 연간 임금총액의 일정비율(1/12 이상)을 적립하고, 근로자가 적립금을 운용하는 방식. 국제회계기준을 적용하는 회사는 근로자에게 당해연도 기여만큼을 근로자에게 지급하는 동시에 의무가 없어지기 때문에 불입금액만큼 퇴직급여로 계상함. |
|------------------------|---|

- 확정급여형인 경우 손익계산서상 퇴직급여는 계리평가보고서를 기초로 산정하며, 회계부서 담당자와 급여담당자가 협의하여 아래 항목을 퇴직급여로 산정함.

※ 다만 일반 기업회계기준으로 재무제표를 작성할 경우 퇴직급여 산정방식으로 인별 퇴직급여를 산정함(퇴직급여충당부채 증감액 기준).

| | |
|------------------------|--|
| 확정급여형 퇴직연금 (DB형) | 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. |
|------------------------|--|

* DB형일 경우 퇴직급여 구성항목: 당기근무원가, 과거근무원가, 확정급여부채에 대한 이자원가, 사외적립자산에 대한 기대수익, 자산인식 상한효과에 대한 이자원가

* DB형일 경우 퇴직급여 제외항목: 투자는 당기손익으로 구성된 항목에 한하므로 자본항목인 재측정요소 등은 제외함.

예시 DB형 계리평가보고서

| 사번 | 기초퇴직급여채무 | 당기근무원가 | 이자원가 | 기말 퇴직급여채무 | 그룹 | 연령 | 성별 |
|--------|-------------|------------|-----------|-------------|-----|----|----|
| A00001 | 10,000,000 | 1,200,000 | 84,000 | 11,284,000 | 일반직 | 25 | 남자 |
| A00002 | 20,000,000 | 2,400,000 | 168,000 | 22,568,000 | 일반직 | 32 | 여자 |
| A00003 | 30,000,000 | 3,600,000 | 252,000 | 33,852,000 | 일반직 | 35 | 남자 |
| A00004 | 40,000,000 | 4,800,000 | 336,000 | 45,136,000 | 일반직 | 32 | 여자 |
| A00005 | 50,000,000 | 6,000,000 | 420,000 | 56,420,000 | 일반직 | 21 | 여자 |
| A00006 | 60,000,000 | 7,200,000 | 504,000 | 67,704,000 | 일반직 | 36 | 여자 |
| A00007 | 70,000,000 | 8,400,000 | 588,000 | 78,988,000 | 일반직 | 45 | 남자 |
| A00008 | 80,000,000 | 9,600,000 | 672,000 | 90,272,000 | 일반직 | 51 | 남자 |
| A00009 | 90,000,000 | 10,800,000 | 756,000 | 101,556,000 | 임원 | 47 | 남자 |
| A00010 | 100,000,000 | 12,000,000 | 840,000 | 112,840,000 | 임원 | 48 | 여자 |
| 합계 | 550,000,000 | 66,000,000 | 4,620,000 | 620,620,000 | | | |

- ▶ A0001번부터 A00010번 모두 정보기술에 해당하는 인력일 경우 당기 확정급여형 퇴직급여에 해당하는 금액은 당기근무원가 및 이자원가의 합인 70,620,000원으로 기말 퇴직급여채무 620,620,000원이 아님을 주의하여야 함.

유의 사항

- ▶ 퇴직금은 실제 퇴직 시 일시 지급되나, 입사 후 1년 이후부터 근무 기간 동안 매년 비용으로 미리 인식하는 것으로, 정보기술·정보보호 인건비는 매년 인식되는 손익계산서상 비용을 의미함. 따라서 실제 퇴직 시 그 동안 비용으로 인식하였던 퇴직급여를 일시에 지급하더라도 퇴직시점에 실제 지급한 퇴직급여를 인건비로 포함하지 않아야 이종으로 인식하지 않을 수 있으므로 주의가 필요함.
- ▶ 확정급여형인 경우 회사별로 인사팀이나 회계팀에서 주관하여 보관하므로 주무부서를 파악하여 정보보호·정보기술 인력을 제공한 후 해당 인력에 대한 손익계산서상 퇴직급여 구성항목의 합계를 정보기술부문/정보보호부문별로 산정해 줄 것을 요청하여야 함.

■ 특기 사항

- 정보보호 투자비중(%)에 대한 업종별·규모별 착시효과 완화 등을 위하여 이용자 등을 대상으로 기업별로 정보보호부문 투자 현황에 대하여 설명 또는 그 밖의 노력 사항을 서술형으로 작성 가능함.(자율기재 사항)
 - 합병 또는 분할로 인한 자산 등의 변동으로 전년 대비 정보기술부문/정보보호부문 투자 현황의 변동 폭이 큰 경우 그 사유를 특기 사항에 기재할 것을 권고함.
 - 국내외 관계사가 정보보호시스템 등을 공동으로 이용하는 등의 상황으로 국내 정보보호 투자액을 별도로 구분 및 작성하기 어려운 경우 '특기 사항' 항목을 통하여 정보보호에 대한 기업의 노력을 작성하여야 함.

예시 정보보호 투자 현황 내 특기 사항 작성 내용

- ① 제조기업으로 개인정보 미취급 등의 사유로 다른 분야 대비 투자 금액이 낮으나, ○○시스템 도입으로 랜섬웨어 등 공격으로부터 정보보안에 최선을 다함.
- ② 신산업 R&D 등을 위한 IT 투자 규모 확대로 공시해당연도 정보보호 예산 비율이 낮아 보이나, 투자 금액 규모로는 전년 대비 ○○% 상승함.
- ③ 당사는 동종업계 평균 투자액 대비 ○○억 원 이상 추가 투자하여 IT 업계 수준으로 랜섬웨어·해킹 등 잠재적인 사이버 공격 등에 대비함.
- ④ A회사의 경우 국내외 관계사가 정보보호시스템 등을 공동으로 이용하고 있고, 이에 대한 글로벌 차원의 정보보호 투자를 시행하고 있으며, 안정적인 서비스를 제공하기 위하여 정보기술 예산의 약 ○%를 정보보호 예산으로 투자 중임.
- ⑤ 제로트러스트 프로그램 확장, 오픈소스 보안 강화, 보안 인력 양성 등 정보보호를 위하여 △년간 ○○○억 달러를 투자함.
- ⑥ 한국 내 ○○ 서비스 제공을 위하여 본사는 △△의 기간통신 서비스와 정보보호 시설 등을 활용하고 있어 정보보호 투자 현황 또한 그에 준함.

2 | 정보보호 인력 현황 산출 방법

■ 개요

▣ 참고 공시내용 양식 내 정보보호 인력 현황

| 구분 | 인원 수 | 참고 |
|-------------------|--------|---|
| 총 임직원(내부인력) | 101.5명 | 원천징수이행상황신고서 월평균 간이세액 |
| 정보기술부문 인력(C) | 43.5명 | 정보보호부문 전담인력(D) 포함 (내부인력, 외주인력 모두 포함) |
| 정보보호부문 전담인력(D) | 내부인력 | 내부인력(정규직+계약직) |
| | 외주인력 | 외주인력(상주+비상주 등) |
| | 계 | 내부인력+외주인력 |
| D/C | 9.7% | 정보기술부문 인력(C) 대비 정보보호부문 전담인력(D) 비율 |

- 정보기술부문 인력과 정보보호부문 전담인력은 다시 내부인력과 외주인력으로 나누어 산출하여 합산하며, 정보보호부문 내부인력은 정보기술부문 내부인력에 포함되고 정보보호부문 외주인력도 정보기술부문 외주인력에 포함됨.
- 정보기술부문 인력은 정보기술부문 업무를 전담하는 내부인력(정규직·계약직)과 외부인력(상주, 비상주, 사내파견, 외부전담)의 공시대상연도 인원으로 산정하고, 정보보호부문 전담인력도 마찬가지로 정보보호부문 업무를 전담하는 공시대상연도 내부인력과 외주인력 인원으로 산정함.
- 내부인력은 조직도·업무분장표·직무기술서를 바탕으로 산출하며, 해당 자료를 통하여 내부인력이 명확히 정보기술부문/정보보호부문 업무만을 하는지 확인이 필요함(내부인력 산정 후 해당 인력의 인건비를 산정하여 투자액에 포함).
- 정보기술부문/정보보호부문 업무와 그 밖의 업무(총무·인사 등)를 겸직하는 경우에는 정보기술부문/정보보호부문 내부인력에서 제외함.
 - 정보기술부문 업무와 정보보호부문 업무를 겸직하는 인력은 정보기술부문 인력에만 포함함.
 - 정보기술부문 업무와 그 밖의 업무(총무·인사 등)를 겸직하는 인력은 제외함.
- 외주인력은 외주 용역 계약을 검토하여 정보기술부문/정보보호부문 용역으로 구분하고, 용역 계약서에 명시된 투입공수나 보고서 등에 표시된 투입공수를 해당 용역의 투입공수로 인정하여 월평균(총 투입공수/12)으로 산정함.
 - 외주인력 산정에는 장기·단기 상관 없이 모든 IT 관련 외주 용역이 포함됨.
 - 외주인력 인건비는 외주용역비에 포함되어 있으므로 내부인력 인건비와 같이 별도로 구분하여 산정할 필요 없음(비용원장에서 외주용역비를 정보기술 용역과 정보보호 용역으로 구분하여 해당 투자액으로 산입함).
- 정보기술부문 인력 대비 정보보호부문 인력의 비율은 정보기술부문 전담인력과 정보보호부문 전담인력을 각각 합산하고, 정보보호부문 전담인력(D)을 정보기술부문 인력(C)으로 나누어 산정함.

참고**정보보호 인력 현황 산식**

$$\text{정보기술부문 인력 대비} \quad \text{정보보호부문 전담인력(D)} \\ \text{정보보호부문 인력 비율(D/C)} = \frac{\text{정보보호부문 전담인력(D)}}{\text{정보기술부문 인력(C)}} \times 100 \\ (\text{단위: 명}) \quad (\text{단위: 명})$$

- 총 임직원(내부인력), 정보기술부문 인력, 정보보호부문 전담인력을 산정하기 위한 기초 자료로 ① 원천징수이행상황신고서(월평균 간이세액), ② 조직도, ③ 정보기술부문/정보보호부문 직무기술서 또는 업무분장표 등이 필요함.

 참고**정보보호 인력 현황 준비 자료**

| 준비 자료 | 필요 내용 | 비고 |
|------------------------|--|------------------------|
| 원천징수이행상황신고서 | 공시대상연도의 월평균 간이세액 (1~12월) | 총 임직원 수 산정 |
| 조직도 | 조직별 직무기술 | 정보기술·정보보호 조직 확인 |
| 정보기술부문/정보보호부문 직무기술서 | 정보기술부문/정보보호부문 내부인력의 직무정보 | 정보기술·정보보호 직무 확인 |
| 정보기술부문/정보보호부문 업무분장표 | 정보기술부문/정보보호부문 내부인력의 부서, 직무, 입사일, 퇴사일 정보 | 정보기술·정보보호 전담인력 확인 |
| 상주·비상주 외주인력 현황 | 용역명과 월평균 투입공수(M/M) | 외주 용역 계약서, 계약 내용 포함 |

■ 총 임직원 산정

- 총 임직원 수는 정보보호 공시자의 내부인력만을 대상으로 하며, 원천징수이행상황신고서상 근로소득 간이세액 인원을 월별로 평균하고, 소수점 첫째 자리 아래는 첫째 자리까지 반올림한 인원으로 산정함.

- 회사의 월별 원천징수이행상황신고서를 확보할 때 주의할 점은 회사의 급여지급 원칙과 일치하는 원천징수이행상황신고서를 기준으로 하여야 함.

※ 예를 들어, 1월 근무 시 1월 급여(상여나 수당 아닌 급여)를 지급하는 회사의 경우 원천징수이행상황신고서상 귀속 연월과 지급연월이 모두 1월인 원천징수이행상황신고서상 근로소득 간이세액 근로자 수를 산정하며, 1월 근무 2월 급여를 지급하는 회사의 경우 원천징수이행상황신고서상 귀속연월은 1월, 지급연월은 2월인 원천징수이행상황신고서상 근로소득 간이세액 근로자 수를 산정함.

예시 원천징수이행상황신고서

| ① 신고구분 | | | | <input type="checkbox"/> 원천징수이행상황신고서 | | | ⑥ 귀속연월 | | 년 월 | | | | | |
|----------------------------|----------------------------|------|----------------------|--------------------------------------|----------|--------------------------------------|---------------------------|-----|-----------------|---------------------|--------------|-----|-----|-------|
| 매월 | 반기 | 수정 | 연말 | 소득 처분 | 판급 신청 | <input type="checkbox"/> 원천징수세액환급신청서 | ⑦ 지급연월 | | 년 월 | | | | | |
| 원 천 징 수 외부자 | 법인명(상호) 사업자(주민) 등록번호 | | | 대표자(성명) 사업장 소재지 | | | 일괄납부 여부 전화번호 전자우편주소 | | | 여, 부 | | | | |
| | | | | | | | | | | @ | | | | |
| 1. 원천징수 명세 및 납부세액 (단위 : 원) | | | | | | | | | | | | | | |
| 소득자 소득구분 | | 코드 | 원천징수 명세 | | | | | | ⑤ 당별 조정 판급내역 | 남부 세액 | | | | |
| | | | 소득 기금 (기부금 포함) | | 징수세액 | | | | | ⑥ 소득세 등 (기부세 포함) | ⑦ 국어증 특별세 | | | |
| 개인 거주자 비거 | 근로소득 | 간이세액 | A01 | | | | | | | | | | | |
| | | 중도퇴사 | A02 | | | | | | | | | | | |
| | | 일용근로 | A03 | | | | | | | | | | | |
| | | 연말정산 | A04 | | | | | | | | | | | |
| | | 가감계 | A10 | | | | | | | | | | | |
| | 사업소득 | 회칙소득 | A20 | | | | | | | | | | | |
| | | 매출징수 | A25 | | | | | | | | | | | |
| | | 연말정산 | A26 | | | | | | | | | | | |
| | | 가감계 | A30 | | | | | | | | | | | |
| | | 기타소득 | A40 | | | | | | | | | | | |
| 연 | 매출징수 | A45 | | | | | | | | | | | | |
| | 구분 | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 월평균 |
| 간이세액 | 104 | 106 | 107 | 106 | 100 | 100 | 100 | 101 | 101 | 104 | 101 | 100 | 89 | 101.5 |

- 법인의 본점 외의 지점, 영업소 또는 기타사업장(공장 등)이 별도 사업장으로 신고납부하는 경우에는 사업장별로 원천징수이행상황신고서(명세서)상 간이세액 인원 수를 월평균하여 총 임직원 수를 산정함.

예시 총 임직원 수 산정

| 구분 | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 월평균 |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-------|
| 본사 | 104 | 106 | 107 | 106 | 100 | 100 | 100 | 101 | 104 | 101 | 100 | 89 | 101.5 |
| A지사 | 47 | 49 | 49 | 50 | 50 | 51 | 51 | 51 | 50 | 51 | 51 | 52 | 50.2 |
| B공장 | 263 | 265 | 263 | 263 | 265 | 265 | 245 | 244 | 245 | 246 | 250 | 252 | 255.5 |
| 총합 | 414 | 420 | 419 | 419 | 415 | 416 | 396 | 396 | 399 | 398 | 401 | 393 | 407.2 |

■ 정보기술부문/ 정보보호부문 전담인력 산정

(1) 정보기술부문/정보보호부문 내부인력

- 정보기술부문 내부인력은 정규직과 계약직을 포함하며, 직무기술서상 정보기술부문

업무를 전담(정보보호부문 업무 포함)하는 내부인력을 정보기술부문 내부인력으로 인정함.

참고

내부인력 요건

| 구분 | | | 세부 내용 |
|------------------|-----|----------------|---|
| 내 부 인 력 | 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 단시간 근로자 보호 등에 관한 법률」 제2조제1호에 따른 '기간제 근로자' 중 1년 이상 계약된 근로자 |

* 기간의 정함이 없는 계약직(무기계약직)의 경우 일반계약직과 달리 기간의 정함이 없지만 본래 소속이 계약직군에 포함되기 때문에 계약직으로 인정함.

참고

정보기술부문/정보보호부문 주요 업무

| 부문 | 주요 업무 | 업무 상세 내용 |
|-----------------------|--------------------|---|
| 정보 기술 부문 | IT 기획 및 관리 | ○ IT 전략 수립·관리 및 IT 관련 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 프로젝트 관리 및 통합품질관리시스템 운영 |
| | | ○ 형상관리정책 수립·운영 및 프로그램 형상 관리 |
| | | ○ 테스트방법론과 테스트계획 관리 및 테스트품질관리 |
| | | ○ IT 감사 및 IT 감리 기획·실시 등 |
| IT 개발 및 유지보수 | IT 개발 및 유지보수 | ○ 전산개발 범위와 처리기능 정의, 개발 세부계획 수립 |
| | | ○ 시스템 상세 업무요건 정의 및 시스템 인터페이스·데이터 분석 |
| | | ○ 입출력자료, 업무처리 단위별 프로그램, 오류코드 등 설계 |
| | | ○ 프로그램 구현 및 산출물 작성 |
| | | ○ 테스트 수행 |
| | | ○ 프로그램 이행 및 시스템 적용 |
| | | ○ 프로그램 유지보수 등 |
| IT 운영 및 보수정비 | 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 |

| 부문 | 주요 업무 | 업무 상세 내용 |
|----------------|-----------------|--|
| | | <ul style="list-style-type: none"> ○ 단말기, 주변기기 등 업무용 전산기기 배정 설치·운영 ○ 전산기기 자산 관리 및 장애 관리(보수정비 포함) ○ 단말기, 자동화기기, 인터넷, 콜센터 등 채널 통합시스템 관리·운영 ○ 대내외 시스템 간 연계(인터페이스)·중계시스템 관리·운영 ○ 전산센터(종합상황실 포함) 운영 및 전산백업·소산매체 관리·운영 ○ 재해복구센터(전산 백업시스템 포함) 관리·운영 ○ IT 업무지속성 계획 수립·관리 및 업무지속성 훈련 실시 ○ 시스템 모니터링 등 IT 서비스 관리 시스템(ITSM) 운영 ○ 센터집중처리·배치 처리, 보고서 추출 등 일괄전산작업 처리 등 |
| | 정보보호 기획 및 관리 | <ul style="list-style-type: none"> ○ 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(법규 준수 포함) 관리 ○ 취약점 분석·평가 및 이행 계획 수립 |
| 정보 보호 부문 | 개발 및 유지보수 | <ul style="list-style-type: none"> ○ 정보시스템 개발 시 정보보호 요구 사항 정의 ○ 정보보호 요구 사항 검토 및 시험, 개선조치 이행 ○ 정보시스템 및 정보보호시스템 시험 운영 ○ 정보시스템 소스 프로그램 이력 관리 ○ 정보시스템 및 정보보호 시스템 운영 이관 및 통제절차 이행 ○ 정보보호 아키텍처 유지관리 ○ 취약점 분석·평가 시행 |
| | 정보보호 운영 | <ul style="list-style-type: none"> ○ 정보기술부문 관련 보안성 검토 ○ 모의해킹, 디도스 대응훈련 등 비상대응훈련 실시 ○ 침해시도에 대한 실시간 보안 관제 및 통합보안관제시스템 운영 ○ 외부 직원 출입통제 및 노트북, USB 등 반출·입 통제 시스템 구축·운영 ○ 침해방지·대응시스템 구축·운영 ○ 시스템 접근 통제, 권한 관리 및 사용자 인증 관련 시스템 구축·운영 ○ 고객 정보 보호 및 정보 유출 방지 시스템 구축·운영 등 |

- 정보기술부문/정보보호부문 전담 내부인력 산정은 회사의 조직도를 통하여 부서별 직무를 파악한 후 개인별 직무를 구분하며, 개인별 월평균 인력 수(공시대상연도에 입사·퇴사한 경우에는 일할계산)를 산출하여 정보기술부문/정보보호부문의 내부인력에 산입함.
 - 정보기술부문/정보보호부문 직무와 전혀 무관한 부서(회계, 마케팅, 인사, 구매, 경영기획 등)는 인력 산정 시 먼저 제외하여야도 무방함.

예시 인력별 정보기술부문/정보보호부문 인력 현황

| 조직명 | 직급 | 성명/사번 | 수행 업무 | 직무 | 직렬 | 입사일 | 퇴사일 | 정보 기술 | 정보 보호 | 제외 |
|-----|----|-------|--------------------|------------|----|-----|-----|-------|-------|----|
| IT팀 | 부장 | 김○○ | 유지보수 총괄 | IT | | | | ○ | | |
| IT팀 | 과장 | 박□□ | 시스템 모니터링 | 보안 | | | | ○ | ○ | |
| IT팀 | 사원 | 이△△ | 장애 처리 | IT | | | | ○ | | |
| IT팀 | 사원 | 정□□ | 장애 처리 및 인사 관리 | IT 및 인사 | | | | | | ○ |
| IT팀 | 사원 | 최△△ | 시스템 모니터링 및 장애처리 | IT 및 보안 | | | | ○ | | |
| : | : | : | : | : | : | | | : | : | |

* 입사일과 퇴사일은 공시대상연도에 근무한 이력을 파악하기 위한 것으로, 이를 바탕으로 월평균 인력 수를 산정할 수 있음.

유의 사항

- 내부인력이 정보기술 업무와 정보보호 업무를 겸직하는 경우에는 정보기술부문 내부인력으로만 인정되고, 정보기술부문/정보보호부문 업무와 그 밖의 업무(총무·인사 등)를 겸직하는 경우에는 정보기술부문/정보보호부문 내부인력에서 제외함.

- 정보보호 공시자가 내부 규정에 따라 IT 기획·개발·운영·정보보호 등 정보기술 전담조직을 운영하는 경우에는 해당 부서 전체 인력을 정보기술부문 인력으로 산정할 수 있음.
- 정보기술부문/정보보호부문 전담부서 소속 인력이 아니더라도 정보기술부문/정보보호부문 업무를 전담(100%)하는 인력은 최고경영자 또는 임원급(CISO)이 확인(결재·서명 등)한 기업의 공식 문서(직무기술서 등)를 근거로 정보기술부문/정보보호부문 인력에 포함 시킬 수 있음.
- 정보기술부문/정보보호부문 인력이 매월 동일한 인원으로 유지되지 않고 신규 입사, 부서 이동, 퇴사 등의 사유로 변경이 발생한 경우에는 변동일자에 따라 일할계산하여 12개월 간의 월평균 인력 수를 산정함.

※ 인력 수는 무한소수점으로 계산한 후, 최종 공시내용 양식 작성 시 소수점 첫째 자릿수로 반올림하여 산정 필요[예: 정보기술부문 인력(소수점 첫째 자릿수) = 정보기술부문/정보보호부문 내주인력 무한소수점 + 정보기술부문/정보보호부문 외주인력 무한소수점]

예시 인력별 정보기술부문/정보보호부문 월평균 근무일수 산출

| 성명/사번 (A) | 직무 (B) | 직렬 (C) | 입사일 (D) | 퇴사일 (E) | 월평균 근무일수 | 정보 기술 | 정보 보호 | 제외 |
|--------------|-----------|-----------|------------|-------------|-------------|----------|----------|----|
| 김○○ | IT | | 2011. 2 1. | | 1.00 | ○ | | |
| 이□□ | IT | | 2015. 2 1. | | 1.00 | | | |
| 박□□ | 보안 | | 2021. 2 1. | | 0.92* | ○ | ○ | |
| 이△△ | IT | | 2018. 9 1. | 2021. 9. 1. | 0.67* | ○ | | |
| 정○○ | 총무 | | 2020. 2 1. | | 1.00 | | | ○ |
| : | : | : | | | : | : | : | |

예시 정보기술부문/정보보호부문 내부인력 산정

| 구분 | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 월평균 |
|--------|------|----|----|----|----|----|----|----|----|-----|-----|------|-------|
| 정보기술부문 | 31.5 | 32 | 32 | 32 | 32 | 33 | 33 | 33 | 33 | 33 | 33 | 32.2 | 32.4명 |
| 정보보호부문 | 5.5 | 5 | 5 | 6 | 5 | 4 | 4 | 5 | 6 | 6 | 5 | 5.2 | 5.1명 |

참고

정보기술부문/정보보호부문 내부인력 산정 방법

- ① 월평균 근무일수는 일할계산으로 산출하며, 엑셀을 이용하여 산출한다면 ① (DAYS('2021-12-31', D3)+1)/365=334/365=0.92이고, ② (DAYS(E4, '2021-01-01')+1)/365=244/365=0.67와 같이 두 산술식을 이용하여 월평균 근무일수를 쉽게 산출할 수 있음.
- ② 정보보호부문 인원 중 1월 16일 입사하여 12월 5일 퇴사한 자가 있는 경우 1월에는 0.5(16/31)명으로 산정하며, 2~11월은 1명, 12월은 0.2(5/31)명으로 산정함. 또한 정보보호부문 인력은 정보기술부문 인력에도 포함됨.

- 내부인력이 정보기술부문/정보보호부문 관련 업무를 하고 있다고 하여도 외주계약에 따라 고객사의 IT 서비스를 목적으로 근무하는 직원(통상 계약서에 투입인력으로 확정된 경우)은 당사의 정보기술부문/정보보호부문 전담인력으로 포함하지 않음.
 - 다만 특정 프로젝트 계약 기간이 종료되어 기업 내부 IT 업무(정보기술부문/정보보호부문)를 수행한 인력은 해당 기간만큼 정보기술부문/정보보호부문 인력에 산입할 수 있음(인건비도 해당 기간만큼 산입함).

(2) 정보기술부문/정보보호부문 외주인력

- 정보기술부문 인력 및 정보보호부문 외주인력은 기업에 상주·비상주 인력 등을 모두 포함하며, 공시대상연도의 월평균 투입공수로 산정함.
 - 외주인력이란 기업과 외부주문, 하도급 계약 등에 따라 업무를 처리하는 업체에 소속된 상시 종업원으로서 파견 근로자 및 사내하도급 근로자를 포함함.



관련 근거

「근로기준법」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. '근로자'란 직업의 종류와 관계 없이 임금을 목적으로 사업이나 사업장에 근로를 제공하는 사람을 말한다.
- 2.~8. (생략)
9. '단시간 근로자'란 1주 동안의 소정근로시간이 그 사업장에서 같은 종류의 업무에 종사하는 통상 근로자의 1주 동안의 소정근로시간에 비하여 짧은 근로자를 말한다.

「기간제 및 단시간 근로자 보호 등에 관한 법률」 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. '기간제 근로자'라 함은 기간의 정함이 있는 근로계약(이하 '기간제 근로계약'이라 한다.)을 체결한 근로자를 말한다.

「파견 근로자 보호 등에 관한 법률」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

- 1.~4. (생략)
5. '파견 근로자'란 파견사업주가 고용한 근로자로서 근로자 파견의 대상이 되는 사람을 말한다.

사내하도급 근로자 고용안정 및 근로조건 보호 가이드라인 II. 정의

- 1.~3. (생략)
4. '사내하도급 근로자'란 수급사업주가 사내하도급계약을 이행하기 위하여 고용한 근로자를 말한다.

- 외주 용역 계약을 통하여 정보보호 공시자의 정보기술부문/정보보호부문 업무를 상시 전담하는 상주·비상주 인력, 시스템 개발이나 보안 컨설팅 등의 단기 외주 용역 인력 등을 투입공수 기반 정보기술부문/정보보호부문 전담인력으로 산정함.

- 1년 미만의 단기외주 용역도 투입공수를 정보기술부문/정보보호부문 외주인력에 포함시킬 수 있음.

유의 사항

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

예시 외주 용역별 정보기술부문/정보보호부문 산정

| 공시 기업 | | 협력 사명 | 용역명/ 수행 업무 | 정보 기술 | 정보 보호 | 월별 인원 수 | | | | | | | | | | | |
|----------|-----|----------|------------------|----------|----------|---------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 담당 부서 | 담당자 | | | | | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 |
| A팀 | 김○○ | B회사 | 일반 IT 업무 | ○ | | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| C팀 | 이□□ | B회사 | 보안 업무 | ○ | ○ | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 |
| C팀 | 이△△ | D회사 | 보안 관제 | ○ | ○ | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 |

예시 정보기술부문/정보보호부문 외주인력 산정

| 구분 | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 월평균 |
|--------|------|------|------|------|------|------|------|------|------|------|------|------|-------|
| 정보기술부문 | 13.5 | 13.5 | 13.5 | 13.5 | 13.5 | 13.5 | 13.5 | 14.5 | 14.5 | 14.5 | 14.5 | 14.5 | 13.9명 |
| 정보보호부문 | 3.5 | 3.5 | 3.5 | 3.5 | 3.5 | 3.5 | 3.5 | 4.5 | 4.5 | 4.5 | 4.5 | 4.5 | 3.9명 |

- 계약에 투입인력이 확정되거나 일반 외주 및 SI, 세어드 서비스 제공자가 제공 서비스에 대한 월평균 투입공수 정보를 제공하는 경우 외주인력으로 산정이 가능함.

※ 세어드 서비스 관련 인력 산정방법 참고(p.44~45)

■ CISO·CPO 지정 현황

- 기업별 CISO와 개인정보보호 책임자(CPO)의 직책, 임원 여부, 겸직 여부 및 대표적인 내·외부 활동 건수 등을 작성함.
 - ‘특기 사항’을 활용하여 공시대상연도의 CISO·CPO의 정보보호 관련 대표적인 대내외 발표, 학술지 기고, 위원회 운영, 외부 자문, 자격 취득 등 상세 활동을 기재할 수 있음.

예시 CISO·CPO 지정 현황 작성

| CISO·CPO 지정 현황 | 구분 | 직책 | 임원 여부 | 겸직 여부 | 주요 활동 |
|-------------------|---|----|-------|-------|-------|
| CISO | 본부장 | ○ | × | 5건 | |
| CPO | 실장 | × | CIO | 3건 | |
| 특기 사항 | CISO 주요 활동: △△제도 개선 자문위원 참여(○○. ○○. ~ ○○. ○○.) CPO 주요 활동: ■■학술 발표(주제: -----) | | | | |

- CISO·CPO가 정보기술부문/정보보호부문이 아닌 총무·인사 등 다른 업무를 겸직하고 있는 경우 정보보호 전담인력으로 포함되지 않음.

유의 사항

- ▶ 정보보호 공시에서의 겸직 여부는 CISO·CPO가 CISO 또는 CPO 직무 외의 다른 업무를 수행하는가에 따라 ○, X를 기입하여야 함.
- ▶ 「정보통신망 이용촉진 및 정보보호에 관한 법률 시행령」 제36조의7(정보보호 최고책임자 지정 및 겸직금지 등)에 따르는 겸직 기준 내용과 무관함.

참고

CISO·CPO 지정·신고 관련 주요 정보

- ① CISO 신고 관련 문의 사항은 지역별 전파관리소([첨부 4] 참고)를 통하여 문의 가능
 - 중앙전파관리소 홈페이지: www.crms.go.kr(상단메뉴 업무안내 - 방송통신사업 등록관리 - 정보보호 최고책임자 지정신고)
- ② CISO 지정·신고 관련 법령
 - 「정보통신망 이용촉진 및 정보보호에 관한 법률」 제45조의3(정보보호 최고책임자의 지정 등 *), 제76조 (과태료 부과)
 - 「정보통신망 이용촉진 및 정보보호에 관한 법률 시행령」 제36조의7(정보보호 최고책임자 지정 및 겸직 금지 등), 제36조의8(정보보호 최고책임자의 신고 방법 및 절차)
 - 정보통신망 이용촉진 및 정보보호에 관한 법률 시행규칙 제2조(정보보호 최고책임자 지정·신고 등)

■ 특기 사항(선택)

- 정보보호 인력 비중(%)에 대한 업종별·규모별 착시효과 완화 등을 위하여 이용자 등을 대상으로 기업별로 전담부서(팀) 편성 여부, 정보보호 인력 현황 등에 대하여 설명 또는

참고 사항을 서술형으로 작성 가능함(자율기재 사항).

- 국내외 관계사가 정보보호시스템 등을 공동으로 이용하는 등의 상황으로 인하여 국내 정보보호 인력을 별도 구분 및 작성이 어려운 경우 ‘특기 사항’ 항목을 통하여 정보보호에 대한 기업의 노력을 작성하여야 함.

예시 정보보호 인력 현황 내 특기 사항 작성 내용

- ① 당사의 정보보호 업무는 정보기술부문 인력이 겸임하여 수행하고 있어, 전담인력 규모가 상대적으로 낮음.
- ② 전문적이고 안전한 정보보호 서비스를 제공하고자 정보보호부문 인력을 자체 운영하지 않고, IT 전문 기업의 ○○ 서비스 이용계약을 체결하여 운영 중임.
- ③ 정보기술·정보보호 겸직 업무 구성으로 인하여 정보보호 전담인력을 0명으로 기재하였으며, 물리보안 (출입통제 등)을 위한 업무도 △△명이 별도로 수행 중임.
- ④ 당사는 디지털전략 및 정보보호 전담부서를 각각 편성하여 전담인력 XX명 배치하고, 디지털 전환을 빠르게 실행하기 위하여 노력함.
- ⑤ A회사의 경우 글로벌 차원에서 정보보호 체계를 구축 및 운영 중에 있음.
- ⑥ 전세계 ○○개 지역에서 ○○개 이상 서비스를 제공하기 위하여 약 ○○명의 정보보안 전문가를 활용하여 사이버 공격 위험에 대비함.
- ⑦ 한국 내 ○○ 서비스 제공을 위하여 본사는 △△에게 정보기술부문/정보보호부문을 아웃소싱하고 있어 전담인력의 규모와 수준이 △△에 준함.

3 | 정보보호 인증·평가·점검 등에 관한 사항

- 정보보호 및 개인정보보호 관리체계 인증, 정보보호 준비도 평가, 클라우드 보안(CSAP) 인증 등 기업이 취득한 국내외 정보보호 관련 주요 인증·평가·점검을 위한 기업의 노력을 작성함.

- 정보보호 관련 인증·평가·점검 등을 취득하지 않은 경우 공시내용 양식의 ‘3. 정보보호 관련 인증·평가·점검 등에 관한 사항’ 문항에 ‘해당 사항 없음’으로 표기함.

※ 국제인증 제도에는 ISO/IEC 27001, ISO/IEC 27017, CSA STAR, SOC 등이 있음.

- 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(의무, 임의)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.

참고

국내외 정보보호 관련 인증 현황

| 인증 종류 | 인증제도 설명 | 비고 |
|------------------------|---|----|
| 정보보호 및 개인정보보호 관리체계 인증서 | <ul style="list-style-type: none"> - 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증 기준에 적합함을 증명하는 제도 * 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(과학기술정보통신부, 개인정보 보호위원회 고시) | 국내 |
| 클라우드 서비스 보안인증서 | <ul style="list-style-type: none"> - 클라우드컴퓨팅 서비스 사업자가 제공하는 서비스에 대하여 정보보호 기준의 준수 여부를 평가·인증하는 제도 * 클라우드컴퓨팅 서비스 정보보호에 관한 기준(과학기술정보통신부 고시) | 국내 |
| 정보보호 준비도 등급 평가서 | <ul style="list-style-type: none"> - 보안투자 비율 및 인력 조직 확충, 법규 준수 등 기업의 정보보호 준비 수준을 평가하여 일정 등급을 부여하는 제도 * AAA~B 5등급, 개인정보보호 지표 만족 시 인증마크에 'P' 부여 | 국내 |
| 데이터베이스 품질 인증서(데이터보안) | <ul style="list-style-type: none"> - 기업·기관에서 중요 데이터나 개인정보가 저장된 데이터베이스를 대상으로 데이터보안에 대한 기술요소 전반을 심사·심의하는 제도 * 데이터베이스 접근 제어, 암호화, 작업결재, 취약점 분석 | 국내 |
| ISO/IEC 27001 | <ul style="list-style-type: none"> - 국제표준화기구(ISO)·국제전기기술위원회(IEC)에서 제정한 정보보호 관리 체계 국제규격 인증 | 국외 |
| ISO/IEC 27701 | <ul style="list-style-type: none"> - 국제표준화기구·국제전기기술위원회에서 제정한 EU GDPR 등 전세계의 개인정보보호 요구 사항을 충족하는 글로벌 개인정보 관리체계 국제규격 인증 | 국외 |
| ISO/IEC 27799 | <ul style="list-style-type: none"> - 국제표준화기구·국제전기기술위원회에서 제정한 의료정보보호 관리체계 국제규격 인증 | 국외 |
| ISO/IEC 27017 | <ul style="list-style-type: none"> - 국제표준화기구·국제전기기술위원회에서 제정한 클라우드 서비스 정보보호 관리체계 국제규격 인증 | 국외 |
| CSA STAR | <ul style="list-style-type: none"> - 영국표준협회와 미국 클라우드시큐리티 얼라이언스가 공동으로 평가하는 클라우드 서비스 정보보호 인증 | 국외 |
| FedRAMP | <ul style="list-style-type: none"> - 클라우드 제품·서비스에 대한 보안평가, 인증 및 지속적인 모니터링에 대한 표준화된 연방 보안 인증 프로그램 | 국외 |
| SOC | <ul style="list-style-type: none"> - 국제인증업무 기준에 따라 서비스의 안정성과 내부 통제 수준을 평가하는 제도 | 국외 |

예시**정보보호 관련 인증·평가·점검 등에 관한 사항 작성**

| 공시 항목 | 공시내용 |
|---------------------------------|--|
| 정보보호 관련 인증·평가·점검 등에 관한 사항 | <ul style="list-style-type: none"> ○ 정보보호 및 개인정보보호 관리체계 인증(유효기간: ○○○○. ○○. ○○.~○○○○. ○○. ○○.) <ul style="list-style-type: none"> - △△ 서비스의 정보보호 및 개인정보보호를 위한 일련의 활동이 인증 기준에 적합함을 보증 ○ 클라우드 서비스 보안 인증 <ul style="list-style-type: none"> - □□ 데이터 센터 각 운영에 대한 안정성 확보 및 서비스 제공 ○ ISO/IEC 27001 <ul style="list-style-type: none"> - 정보보호 수준의 지속적인 개선 및 이용자 요구 사항 충족을 보장하는 국제인증 ○ SOC 2, 3 <ul style="list-style-type: none"> - 이용자의 개인정보보 중점을 두고 서비스 안정성과 내부 통제 수준을 평가하는 국제인증 * SOC 3의 경우 국내에 ○○개 기관만 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*) 참여 등 협력 활동, 사이버 위기 대응을 위한 모의훈련 참여, 업무지속계획(BCP**) 수립, 제로트러스트(Zero Trust)*** 도입·운영 등이 정보보호 활동에 해당함.

* C-TAS: KISA에서 운영 중인 사이버 위협정보의 수집·분석 및 공유 플랫폼(일반회원과 공유회원으로 구분)

** BCP: Business Continuity Plan. 재난 발생 시 업무 연속성을 유지하기 위한 계획으로, 랜섬웨어 등 사이버 공격 예방 대책, 사고 시 확산단계별 대응계획 등 반영

*** Zero Trust: ‘신뢰할 수 있는 네트워크’라는 개념 자체를 배제하며, 기업망 내·외부에 언제나 공격자가 존재할 수 있고, 명확한 인증 과정을 거치기 전까지는 모든 사용자·기기 및 네트워크 트래픽을 신뢰하지 않으며, 인증 후에도 끊임없이 신뢰성을 검증함으로써 기업의 정보 자산을 보호할 수 있는 보안 모델

- 사이버 위기 대응을 위한 모의훈련을 실시한 경우 모의훈련 유형(자체, 외부)과 내용(랜섬웨어, 디도스 해킹메일 등) 및 주관기관(공공, 민간) 등을 같이 기재함.
 - 제로트러스트를 도입 또는 운영하는 기업은 제로트러스트 단계[준비, 계획(설계), 구현(도입), 운영, 피드백 및 개선] 및 활용 내용 등을 기재함.
- 「개인정보보호법 시행령」 제30조, 제48조의2에서 규정하고 있는 개인정보의 안전성 확보 조치를 위한 활동 등 공시대상연도에 수행한 내·외부 활동도 공시 가능함.

| 구분 | 정보보호 활동 세부 내용 |
|-----------------|--|
| 개인정보의 안전성 확보 조치 | 1. 개인정보를 안전하게 처리하기 위한 내부 관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위치·변조 방지를 위한 조치 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 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(수행 주기)를 표기하고, 각 세부 활동 건수를 집계하여 정보보호 활동 공시 자료를 작성함.
 - 정보보호 활동 내역이 없는 경우에는 공시내용 양식의 '4. 정보통신 서비스를 이용하는 자의 정보보호를 위한 활동 현황' 문항에 '해당 사항 없음'으로 표기함.

예시 정보통신 서비스 이용자의 정보보호를 위한 활동

| 구분 | 정보보호 활동 세부 내역 | 건수 |
|-----------------------------|--|----|
| 정보보호 투자 활성화 실적 및 정보보호 관련 활동 | <ul style="list-style-type: none"> ○ 사이버 위협 정보 분석공유 시스템(C-TAS) 참여(일반 또는 공유회원) ○ 업무지속계획 수립 ○ 정보보안 업무규칙, 기본지침 등 보안정책 2건 개정 및 공급망 보안정책 1건 제정 ○ 제로트러스트 아키텍처 도입을 위한 자산·기기 및 워크플로 점검 ○ 국내외 정보보호 기업과 양해각서(MOU) 체결 ○ 정보보호 관련 수상 내역(ICT 대상, 공시 우수기업 지정) ○ 사이버 위협 배상책임보험 가입 ○ 정보보호 관련 국내외 콘퍼런스 참가(세션 발표, 전시 부스 설치 등) | 8건 |
| 임직원의 정보보호 인식 제고 교육 및 지원 | <ul style="list-style-type: none"> ○ 사이버 위기대응 ○○모의훈련 실시(자체 점검, KISA 주관 훈련 등) ※ 랜섬웨어, 디도스, 해킹 메일 등 모의훈련 유형과 내용, 주관기관 등 기재 필요 ○ 임직원 정보보호 및 개인정보보호 수준 진단 ○ 월별 임직원 보안의식 제고 활동 추진(정보보호의 날, 자가진단 등) ○ 임직원 대상 사내 정기 정보보호 교육과정 개설(상·하반기) | 4건 |
| 정보보호 전담인력 관리 활동 | <ul style="list-style-type: none"> ○ 사내 우수보안사례 발굴 및 내부 시상(월 1회) ○ 정보보호 공모(모의해킹대응대회 등), 세미나 개최 등 지원 ○ 취약점 제보 및 보상제도 도입 | 3건 |
| 이용자 정보보호 인식 제고 활동 | <ul style="list-style-type: none"> ○ 정보보호 취약계층 대상 보안인식 제고 캠페인 실시(3회) ○ 이용자 참여형 정보보호 콘텐츠 마련 ○ 정보보호 생활 실천 수칙 마련 및 배포 ○ 대표 홈페이지 팝업 및 공지 사항 내 보안 실천 수칙 게시(상·하반기 2회) | 4건 |
| 계 | 19건 | |

자주 묻는 질문·응답

[FAQ]

III 자주 묻는 질문·응답 [FAQ]

Q1

모든 기업은 반드시 정보보호 공시를 해야 하나요?

Q2

의무대상 여부는 어떻게 알 수 있나요?

Q3

의무대상 기준 중 일평균 이용자 수 100만은 어떻게 산정하나요?

Q4

글로벌 기업의 경우 공시 주체는 누구인가요?

Q5

정보보호 현황 산출 시 전사의 자산대장, 비용원장이 꼭 필요한가요?

Q6

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

Q7

정보보호 공시는 언제까지 해야 하나요?

Q8

ISDS와 KIND 두 곳에 같이 공시해야 하나요?

Q9

회계법인 또는 정보시스템 감리법인의 사전점검은 필수인가요?

Q10

네트워크 유지보수 용역을 제공받고 있으며, 정기 점검 월 1회 및 원격으로 언제든지 대응 조건일 경우 외주인력은 어떻게 산정되나요?

Q1

모든 기업은 반드시 정보보호 공시를 해야 하나요?

A

「정보보호산업법 시행령」 제8조제1항의 기준을 충족하는 기업은 정보보호 공시 의무자로 반드시 정보보호 공시를 하여야 합니다.

정보보호 공시 의무자가 아니더라도 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자라면 누구나 자율적으로 정보보호 공시를 할 수 있습니다.

정보보호 현황 공시를 자율적으로 이행한 기업은 ISMS 인증 수수료 30% 할인 등 혜택을 받을 수 있습니다(정보보호 공시 의무자는 할인 미해당).

Q2

의무대상 여부는 어떻게 알 수 있나요?

A

매년 4월 중 정보보호 공시 의무자 대상(안)을 KISA 대표 홈페이지, ISDS 공지 사항 등에 게시할 예정입니다(게시 일정 변동 가능).

확인 후, 의무대상 기준에 해당하지 않는다고 생각하는 기업은 의무 제외에 대한 소명 자료를 안내 기일까지 정보보호 공시 담당자 메일*로 제출하면 내용 검토 후 개별 회신하여 드립니다.

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

Q3

의무대상 기준 중 일평균 이용자 수 100만은 어떻게 산정하나요?

A

이용자 수에 대한 의무대상 기준은 전년도 말 기준 직전 3개월간 정보통신 서비스 일평균 이용자 수 100만 명 이상입니다.

여러 가지 정보통신 서비스(홈페이지 및 앱 등)를 제공할 경우에는 해당 서비스의 이용자 수를 모두 합하여 계산합니다.

산정 기준은 전년도 10~12월의 순방문자 수(UV)*의 일일 평균입니다.

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

Q4

글로벌 기업의 경우 공시 주체는 누구인가요?

A

글로벌 기업 본사 또는 국내법인 중 국내 서비스의 제공 주체가 누구인지를 판단하여 정보보호 공시 의무대상이 결정됩니다.

의무공시 대상이 아닌 글로벌 기업도 자율적으로 정보보호 공시를 할 수 있습니다.

글로벌 차원에서 정보보호 체계를 구축·운영 중 기업이 국내에 한정된 정보를 취합하는 것이 어려운 경우 정보보호 투자, 인력 수치를 작성하지 않아도 무방하나, ‘특기 사항’ 항목을 통하여 정보보호에 대한 기업의 노력을 작성하여야 합니다.

Q5

정보보호 현황 산출 시 전사의 자산대장, 비용원장이 꼭 필요한가요?

A

원칙적으로 전사의 자산대장과 비용원장을 협조받아 정보보호 현황을 산출하는 것을 권합니다.

다만 영업비밀 등을 이유로 유관부서에서 전사의 자료 협조가 어렵다면 영업비·광고선전비 등 명백히 정보기술부문/정보보호부문에 해당되지 않는 내용만 제외하고 진행할 수 있습니다.

Q6

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

A

우수정보보호 제품, 정보보호제품 성능평가 등은 기업에서 생산하는 제품·서비스 등에 대한 인증이기 때문에 이를 기업 전체의 정보보호 관련 인증·평가·점검으로 보기에는 한계가 있습니다.

따라서 제품·서비스에 대한 인증과 평가는 정보보호 관련 인증·평가·점검 등에 관한 사항에 포함되지 않지만, 우수정보보호 제품, 정보보호제품 성능평가 제품을 개발·구매한 비용은 정보보호부문 투자 비용으로 인정됩니다.

Q7

정보보호 공시는 언제까지 해야 하나요?

A

「정보보호산업의 진흥에 관한 법률 시행령」 제8조제6항에 따라 매년 6월 30일까지 과학기술정보통신부장관이 운영하는 ISDS에 정보보호 현황을 제출하여야 합니다.

정보보호 현황은 공시연도의 직전연도(공시대상연도)에 해당하는 회계 및 인증 내용을 바탕으로 작성하며, 매년 정기적으로 공시를 이행하고 이용자·투자자 보호를 목적으로 정보를 신속하게 전달하기 위하여 신속하게 이행하는 것이 바람직합니다.

Q8

ISDS와 KIND 두 곳에 같이 공시해야 하나요?

A

과학기술정보통신부장관이 운영하는 ISDS에 하는 것이 원칙입니다.
다만 자율적으로 정보보호 공시를 하는 자가 유가증권·코스닥·코넥스시장 상장법인일 경우에는 ISDS·KIND에 각각 공시 가능하며, 원하는 곳 한 곳에만 공시도 가능합니다
(정보보호 공시 의무자는 ISDS 필수 공시).

Q9

회계법인 또는 정보시스템 감리법인의 사전점검은 필수인가요?

A

회계법인 또는 정보시스템 감리법인의 사전점검 절차는 기업의 선택 사항입니다.
사전점검 유무에 따라 제출하여야 할 자료가 서로 다른 점을 유의하여야 하며, 사전점검을 받아 확인서 2종을 제출한 경우 당해연도 공시내용 검증 대상에서 제외될 수 있습니다.

Q10

네트워크 유지보수 용역을 제공받고 있으며, 정기 점검 월 1회 및 원격으로 언제든지 대응 조건일 경우 외주인력은 어떻게 산정되나요?

A

시스템 유지보수 용역의 경우 MM 없이 월 정기점검 및 원격대응 조건이 많은데, 이 경우 월 정기점검 기록이 있거나 원격대응 시간 등 객관적인 기록이 있는 경우 해당 기록을 토대로 외주인력 일수를 산정할 수 있습니다. 다만 객관적인 기록이 없는 경우에는 제외합니다.

첨부 1

정보기술부문/정보보호부문 자산 분류표

※ 정보보호 공시의 '정보기술부문'은 '정보보호부문'을 포함함에 따라 모든 정보보호부문 자산은 정보기술 부문 자산에 포함하여 산정

| 대분류 | 중분류 | 소분류 | 설명 |
|--------|------------------|------------------|--|
| 컴퓨팅 장비 | 서버 * OS 기준 구분 | Unix | · 유닉스 OS(운영체제)를 사용하는 서버 |
| | | Windows | · 윈도우 OS를 사용하는 서버 |
| | | Linux | · 리눅스 기반 OS를 사용하는 서버 |
| | | 기타 | · 위의 분류에서 제외된 서버 장비 |
| | 스토리지 | 스토리지 | · 데이터가 저장되는 외장 스토리지(HDD, SSD 등) |
| | | NAS | · 네트워크 공유 스토리지 |
| | | 기타 | · 위의 분류에서 제외된 스토리지 장비 |
| | 백업 장비 | 클라우드백업 | · 공용 클라우드백업(AWS, Axure 등), 온-프레미스 클라우드백업, 하이브리드 클라우드 백업 등 |
| | | 디스크기반 | · NAS 기반, 스토리지영업네트워크(SAN) 기반, 직접연결스토리지 (DAS) 기반 백업 등 |
| | | VTL | · 가상 테이프 라이브러리(Virtual Tape Library), 가상화 기술을 통하여 디스크를 테이프처럼 인식하여 데이터를 저장하는 데이터 백업 및 복구 장비 |
| | | 테이프 라이브러리 | · 다수의 테이프 카트리지를 가진 대용량 고속 백업용 장비 |
| | | 기타 | · 위의 분류에서 제외된 백업 장비 |
| | 기반시설 | 영상·음향설비 (전산실) | · 전산실에서 사용되는 프로젝트, 화상회의, 음향설비 등 |
| | | 소방설비 (전산실) | · 전산실에서 사용되는 스프링클러, 가스소화설비, 하론 등 |
| | | 전원·공조장치 | · 정보시스템을 구성하는 하드웨어·소프트웨어와 함께 활용되는 UPS, 항온 항습기 등 |
| | 기타 컴퓨팅 장비 | PC (사무용) | · 사무용으로 사용되는 개인용 데스크탑, 노트북 등 |
| | | 입출력장치 | · 스캐너, 프린터, 플로터, 팩스 등 |
| | | 기타 | · 위의 분류에서 제외된 하드웨어 |

| 대분류 | 중분류 | 소분류 | 설명 |
|------------------|----------|-----|---|
| 정보 통신 장비 | 교환설비 | | <ul style="list-style-type: none"> 유선망: Voip교환기, BCN교환기, 지능망교환기, IP_PBX, IP 기반교환기, CMTS, Circuit교환기(TDM 등) 무선망: 3G데이터, 4G교환기(MME, MSC, IGS, AuC, PGW, SGW, IMS망, SMSC, AAA, 과금, HLR/HSS, MGW, TAS, EIR 등), 5G교환기(NSA/SA교환, VSGW,VPGW 등), 부가 서비스망, 3G음성 MSC교환기(Circuit 기반) |
| | 전송설비 | | <ul style="list-style-type: none"> 유선망: COT-RT, 광단국 장비(가입자-국사), 국간 전송 장비, 라우터, 스위치, 방송저저장장치, HFC망 관련 전송 장비 무선망: BSC, RNC, 기지국-교환국 간 전송, 교환국 간 전송, 기지국 간 전송(백홀, 프런트홀 등) <p>* 가입자액 내 설비(모뎀, 셋톱박스, AP)와 기지국 장비(BTS, RU, DU, e-NB 등)는 제외</p> |
| | 정보처리설비 | | <ul style="list-style-type: none"> 망 관리 시스템(NMS), 통신설비관리 서버 등 |
| 네트워크 장비 | 전송장비 | | <ul style="list-style-type: none"> 통신회선(광케이블 등)을 통하여 정보를 전송·처리할 수 있도록 하는 설비 <p>* 고속 광전송 네트워크 장비: WDM, DWDM, ROADM 등 * 패킷 기반 전송 장비: PTN, MPLS 등</p> |
| | 스위치 | L2 | <ul style="list-style-type: none"> 서로 다른 데이터링크 간 MAC 주소로 스위칭하는 소규모 워크 그룹 스위치 장비 |
| | | L3 | <ul style="list-style-type: none"> 서로 다른 네트워크 간 IP 주소로 스위칭하는 장비로 라우팅 프로토콜을 수행하는 워크그룹 스위치, 또는 스위칭 용량(switching capacity) 720Gbps 이하인 L3스위치(상세 규격에서 확인 가능) |
| | | L4 | <ul style="list-style-type: none"> 서로 다른 네트워크 간 서비스 포트로 스위칭하는 장비로 전송계층 정보(웹, FTP 등)에 따라 트래픽을 스위칭할 수 있어 부하분산 (load balancing) 기능까지 제공하는 장비, 네트워크 보안 스위치도 해당 |
| | | 백본 | <ul style="list-style-type: none"> 다수의 워크그룹 스위치 노드가 모이는 중심에 위치하는 스위치, 또는 스위칭 용량 720Gbps 이상의 L3 스위치 |
| | | 기타 | <ul style="list-style-type: none"> 위의 분류에서 제외된 스위칭 장비 |
| | 라우터 | | <ul style="list-style-type: none"> 이기종의 네트워크(망) 간 연결을 위한 장비 PSTN망·ATM망·이더넷망 등을 연결하는 장비 |
| | 무선 장비 | | <ul style="list-style-type: none"> 일정 공간에 WiFi 서비스를 통한 인터넷 이용이 가능하도록 무선망을 구축하는 장비로 WiFiAP(무선공유기) 등이 해당 <p>* WiFiAP, AP 컨트롤러(APC), WIPS, 무선랜 인증 장비 등</p> |
| 기타 네트워크 장비 | VoIP용 장비 | | <ul style="list-style-type: none"> IP망을 기반으로 음성 또는 영상 등 데이터통신을 제공하기 위한 장비 IP 교환기, VoIP용 게이트웨이, SBC(Session Border Controller), 콜센터 상담앱(소프트웨어), 그 밖의 VoIP용 장비 등 포함 |

| 대분류 | 중분류 | 소분류 | 설명 |
|-------------|--------------|-------------------------|---|
| | | 네트워크 NMS | <ul style="list-style-type: none"> 네트워크 운영·관리시스템(network management system). 이기종 네트워크 장비의 구성·성능·장애 정보를 통합 모니터링 하기 위한 시스템 |
| | | 기타 | <ul style="list-style-type: none"> 위의 분류에서 제외된 통신 장비 |
| 소프트웨어 | 시스템 소프트웨어 | 운영체계 | <ul style="list-style-type: none"> 컴퓨터를 작동시키고 전반적인 동작을 제어·운영을 도맡아 관리하는 기본 소프트웨어 |
| | | 통신 소프트웨어 | <ul style="list-style-type: none"> 컴퓨터 상호간 접속하여 2개 장치 사이에 다양한 방법으로 정보를 교환할 수 있게 하는 소프트웨어 |
| | | 유ти리티 소프트웨어 | <ul style="list-style-type: none"> 사용자가 컴퓨터를 좀 더 편리하고 쉽게 사용할 수 있도록 도와 주는 프로그램 |
| | | 시스템관리 소프트웨어 | <ul style="list-style-type: none"> 네트워크를 관리하는 기능을 포함하여 여러 개의 네트워크가 묶인 대규모의 시스템에서 이기종 데이터베이스 관리, 미들웨어 등에 이르는 다양한 기능을 체계적으로 관리하도록 하는 시스템 |
| | | 미들웨어 | <ul style="list-style-type: none"> 클라이언트에서 서버에 있는 애플리케이션이나 자원을 불러오기 위하여 클라이언트와 서버의 가운데 놓인 중간자 |
| | 개발용 소프트웨어 | 프로그램 개발용 언어 | <ul style="list-style-type: none"> 컴퓨터가 인식할 수 있는 컴퓨터의 명령어를 논리적 순서에 맞게 프로그래머가 작성하는 프로그래밍 작업 과정에서 사용되는 언어 |
| | | 프로그램 및 콘텐츠 개발용 도구 | <ul style="list-style-type: none"> 개발 생산성 및 품질을 향상하는데 사용되는 각종 소프트웨어 및 콘텐츠 개발에 지원되는 도구 |
| | | 프로젝트 관리용 소프트웨어 | <ul style="list-style-type: none"> 프로젝트를 추진하거나 개발할 때 발생하는 모든 요소를 체계적으로 관리하기 위하여 사용되는 소프트웨어 |
| | | DBMS | <ul style="list-style-type: none"> 데이터를 효과적으로 이용할 수 있도록 정리·보관하기 위한 기본 소프트웨어 |
| | 응용 소프트웨어 | 기업관리 소프트웨어 | <ul style="list-style-type: none"> 기업의 기간업무를 통합 관리해 주는 소프트웨어 |
| | | 과학용 소프트웨어 | <ul style="list-style-type: none"> 과학적 데이터의 처리나 과학적 문제 등의 기술을 개발하고 지원하기 위한 소프트웨어 |
| | | 산업용 소프트웨어 | <ul style="list-style-type: none"> 모든 분야의 생활 활동의 전반적인 전체 산업을 구성하는 각 부문·업종을 지원하는 소프트웨어 |
| | 기타 소프트웨어 | | <ul style="list-style-type: none"> 위의 분류에서 제외된 소프트웨어 |
| 정보 보안 제품 | 네트워크 보안 | 웹 방화벽 | <ul style="list-style-type: none"> 다양한 형태의 웹 기반 해킹 및 유해 트래픽을 실시간 감시하여 탐지하고 차단하는 웹 애플리케이션 보안 시스템 |
| | | 네트워크 (시스템) 방화벽 | <ul style="list-style-type: none"> 외부의 불법 침입으로부터 내부의 정보자산을 보호하고 유해 정보의 유입을 차단하기 위한 정책과 이를 지원하는 보안시스템 |
| | | 침입방지시스템 (IPS) | <ul style="list-style-type: none"> 네트워크에서 공격 서명을 찾아내 자동으로 조치를 취하여 비정상적인 트래픽을 차단시키는 보안 솔루션 |

| 대분류 | 중분류 | 소분류 | 설명 |
|-----------------------------------|-----|-------------------------------|--|
| 시스템 (단말) 보안 | | 디도스 차단 시스템 | · 대량의 트래픽을 전송하여 시스템을 마비시키는 디도스 공격 전용 차단시스템 |
| | | 통합보안시스템 (UTM) | · 다중 위협에 대하여 보호기능을 제공할 수 있는 포괄적인 보안 제품 |
| | | 가상사설망 (VPN) | · 인터넷망 또는 공중망을 사용하여 2개 이상의 네트워크를 안전하게 연결하기 위하여 가상의 터널을 만들어 암호화된 데이터를 전송할 수 있도록 만든 네트워크 |
| | | 네트워크 접근제어 (NAC) | · 네트워크에 접근하는 접속단말의 보안성을 강제화할 수 있는 보안 인프라. 허가되지 않거나 악성코드에 감염된 PC 등이 네트워크에 접속되는 것을 차단하여 시스템 전체를 보호하는 솔루션 |
| | | 무선 네트워크 보안 | · 무선을 이용하는 통신 네트워크상에서 인증, 키 교환 및 데이터 암호화 등을 통하여 위협으로부터 보호하기 위한 기술 |
| | | 가상화 (망 분리) | · 조직에서 사용하는 망(네트워크)을 업무 및 내부용 망(인트라넷)과 외부망(인터넷)으로 구분하고 각 망을 격리 |
| 콘텐츠 (데이터)/ 정보유출 방지 보안 | | 시스템 접근통제 (PC 방화벽 포함) | · 자료가 외부로 유출되는 것을 방지하기 위하여 온라인을 통한 파일 유출방지, 감시 기능, SMTPMail, WebMail 등을 통한 파일 유출 방지, 감시기능, 프린터 인쇄 모니터링 기능 등 자료 유출을 보안하는 다양한 기능 |
| | | 안티멀웨어 (anti-malware) | · 컴퓨터의 운영을 방해하거나 정보를 유출 또는 불법적으로 접근 권한을 취득하는 소프트웨어인 멀웨어 방지 |
| | | 스팸차단 소프트웨어 | · 스팸을 방지하기 위하여 스팸 차단 또는 필터링 기능을 제공하는 소프트웨어 |
| | | 보안운영체제 (Secure OS) | · 컴퓨터 운영 체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 기존 운영체제 내에 보안 기능이 추가된 운영체제 |
| | | APT 대응 | · APT 공격에 대응하기 위한 프로그램 소프트웨어 |
| | | 모바일 보안 | · 모바일 서비스상 발생할 수 있는 위협으로부터 보호하기 위한 기술 |
| | | 데이터베이스 보안 (접근통제) | · 데이터베이스 및 데이터베이스 내에 저장된 데이터를 인가되지 않은 변경·파괴·노출 및 비밀관성을 발생시키는 사건으로부터 보호하는 기술 |
| | | 데이터베이스 암호 | · 데이터의 실제 내용을 허가받지 않은 사람이 볼 수 없도록 은폐하기 위하여 데이터를 암호화하는 것 |
| | | 보안 USB | · 사용자 식별, 지정 데이터 암복호화, 지정된 자료의 임의복제 방지, 분실 시 데이터 보호를 위한 삭제 등의 기능을 지원하는 보안 컨트롤러가 있는 휴대용 메모리 스틱 |
| | | 디지털 저작권관리 (DRM) | · 웹을 통하여 유통되는 각종 디지털 콘텐츠의 안전 분배와 불법 복제 방지 |

| 대분류 | 중분류 | 소분류 | 설명 |
|-------|-------|------------------------------------|---|
| 암호/인증 | | 네트워크 DLP | <ul style="list-style-type: none"> 사용자의 고의 또는 실수, 외부해킹, 멀웨어 등을 네트워크를 이용한 정보 유출을 콘텐츠 수준에서 막는 기술 |
| | | 단말 DLP | <ul style="list-style-type: none"> 사용자의 고의 또는 실수, 외부해킹, 멀웨어 등을 네트워크를 이용한 정보유출을 단말 수준에서 막는 기술 |
| | | 보안스마트카드 | <ul style="list-style-type: none"> 일반카드와 달리 반도체 칩을 내장한 스마트카드 |
| | | 하드웨어토垦 (HSM) | <ul style="list-style-type: none"> 전자 서명 생성기 등 비밀정보를 안전하게 저장·보관할 수 있고, 기기 내부에 프로세스 및 암호 연산장치가 있어 전자 서명키 생성, 전자 서명 생성 및 검증 등이 가능한 장치 |
| | | 일회용 비밀번호 (OTP) | <ul style="list-style-type: none"> 로그인할 때마다 새로운 패스워드를 생성하는 보안 시스템 |
| | | 공개키 기반 구조(PKI) | <ul style="list-style-type: none"> 실체의 식별자와 공개키를 포함하는 정보로, 공개키 정보는 한 실체에 대한 데이터와 이 실체를 위한 공개키로 제한되며, 인증 기관, 실체, 공개키 또는 관련 알고리즘에 관한 다른 정적인 정보 |
| | | 통합접근관리 (EAM) /싱글사인온 (SSO) | <ul style="list-style-type: none"> 통합접근관리: 인트라넷, 액스트라넷 및 일반 클라이언트·서버 환경에서 자원의 접근인증과 이를 기반으로 자원에 대한 접근 권한을 부여 관리하는 통합인증관리 솔루션 싱글사인온: 이기종의 시스템을 사용할 때마다 다른 사용자번호와 비밀번호를 입력하지 않고도 1회 인증만으로 전 시스템을 하나의 시스템처럼 사용할 수 있도록 하는 시스템 |
| | | 통합계정관리 (IM/IAM) | <ul style="list-style-type: none"> ID와 패스워드를 종합적으로 관리해 주는 역할 기반의 사용자 계정 관리 솔루션 |
| | 보안 관리 | 통합보안관리 (ESM) | <ul style="list-style-type: none"> 방화벽, 침입탐지시스템, 가상사설망 등 각종 보안시스템 및 주요 시스템 장비를 연동하여 효율적으로 운영할 수 있도록 하는 시스템 |
| | | 위협관리 시스템(TMS) | <ul style="list-style-type: none"> 국내외 최신 취약성 정보와 보안 트렌드, 정밀 분석된 네트워크 트래픽 및 공격 형태를 상관 분석하여 사이버 공격을 예측하고 판단하여 능동적으로 대응할 수 있는 체계적인 위협관제 및 대응 시스템 |
| | | 패치관리 시스템(PMS) | <ul style="list-style-type: none"> 시스템의 보안 취약점을 보완하기 위하여 배포되는 보안 패치 파일을 원격에서 자동으로 설치·관리해 주는 시스템 |
| | | 위협관리 시스템(RMS) | <ul style="list-style-type: none"> 관리 대상 시스템의 잠재적인 위험도를 관리하며 위협 분석 기능뿐 아니라 정보시스템의 취약성을 인식하고, 이로 인하여 예상되는 손실을 분석하고 주요 자산 평가 기능 등을 총체적으로 제공하는 시스템 |
| | | 백업/복구 관리 시스템 | <ul style="list-style-type: none"> 자료 손실을 예방하기 위하여 자료를 미리 다른 곳에 임시로 보관해 두었다가 원래 상태로 복구해 주는 관리 시스템 |
| | | 로그 관리/ 분석 시스템 | <ul style="list-style-type: none"> 로그를 실시간 수집·저장·분석하는 등의 작업을 하기 위하여 사용되는 시스템 |

| 대분류 | 중분류 | 소분류 | 설명 |
|---------|--------|----------------|--|
| | | 취약점 분석 시스템 | <ul style="list-style-type: none"> · 악성코드 민감도, 안전하지 않은 소프트웨어 설정, 열린 포트 같은 컴퓨터 시스템의 알려진 취약점을 분석하기 위하여 사용되는 시스템 |
| | | 디지털 포렌식 시스템 | <ul style="list-style-type: none"> · 정보기기 내에 내장된 디지털 자료가 법적 증거가 되도록 자료를 수집·보관·분석·보고용으로 사용하는 시스템 |
| | | 기타 정보보안제품 | <ul style="list-style-type: none"> · 위의 분류에서 제외된 제품 |
| 물리보안 제품 | 바이오 인식 | CCTV 시스템 | <ul style="list-style-type: none"> · 특정한 수신자에게만 서비스하는 것을 목적으로 하는 텔레비전 전송시스템, 카메라, 모니터, 디지털비디오녹화기(DVR), 네트워크로 구성된 시스템(만약 본사에서 통제·관리하는 CCTV 시스템에 한하여 정보보호부문 자산 인정. 그 밖의 것은 정보기술 부문 자산으로만 인정) (예) 저장장치, 카메라, 주변 장비 영상감시관제 소프트웨어 및 장비, 지능형 솔루션, 액세서리 |
| | | 얼굴인식 시스템 | <ul style="list-style-type: none"> · 사람 얼굴의 대칭적 구도, 생김새, 머리카락, 눈의 색상, 얼굴 근육의 움직임 등을 분석하여 얼굴의 특징을 알아내는 생체인식 기술 |
| | | 지문인식 시스템 | <ul style="list-style-type: none"> · 지문인식 전용 센서를 이용하여 지문의 디지털 영상을 획득하여 지문에 있는 다양한 패턴을 이용하여 신원을 확인하는 기술 |
| | | 흉채인식 시스템 | <ul style="list-style-type: none"> · 흉채의 모양과 색, 망막 모세혈관의 형태소 등을 분석하여 사람을 인식하는 생체인식 기술 |
| | | 정맥인식 시스템 | <ul style="list-style-type: none"> · 손바닥이나 손가락에 흐르는 정맥을 이용하여 본인 여부를 인식하는 생체인식 기술 |
| | | 기타 (음성인식 및 기타) | <ul style="list-style-type: none"> · 위의 분류에서 제외된 시스템 |
| | | 접근제어 | <ul style="list-style-type: none"> · 주요 관공서, 군 주요 시설, 금융기관, 회사, 연구실 등의 보안 유지가 요구되는 곳 또는 이용자의 출입관리가 요구되는 곳에서 ID 카드 등의 인식 장비를 활용하여 관리하는 시스템 (예) 카드&리더(번호/마그네틱), 시큐리티게이트 및 소프트웨어 등 |
| | | 알람모니터링 | <ul style="list-style-type: none"> · 온도, 압력, 방사선 세기 등의 물리량이나 화학량을 검지하여 신호 처리가 가능하도록 변화시키는 장치 (예) 적외선·레이저·진동·장력센서, 모션디텍터·침입 탐지 장비 등 |
| | | 기타 물리보안제품 | <ul style="list-style-type: none"> · 위의 분류에서 제외된 제품 |

첨부 2

정보보호 서비스 분류표

| 대분류 | 중분류 | 소분류 | 세부 항목 |
|-------------|-------------|---------------|--|
| 정보보호 서비스 | 정보보안 서비스 | 유지관리 | · 제품 업데이트, 기술지원 등 |
| | | 보안성 지속 서비스 | · 보안 업데이트, 보안정책관리, 위협/사고분석, 보안기술 자문, 보안성 인증(KCMVP 등) 협력 유지 |
| | | 보안관제 | · 원격관제 서비스 · 파견관제 서비스 |
| | | 보안 컨설팅 | · 인증(ISO, ISMS 등) · 기반보호 · 진단 및 모의해킹 · 개인정보보호 컨설팅 · 종합보안 컨설팅 · 정보감사(내부 정보 유출방지 컨설팅 등) |
| | | 교육·훈련 | · 교육·훈련 서비스 |
| | | 인증 서비스 | · 공인·사설 인증 서비스 |
| | 물리보안 서비스 | · 출동보안 서비스 | |
| | | · 영상보안 서비스 | |
| | | · 기타 보안 서비스 | |

첨부 3

영업보고서를 작성하는 기간통신사업자 대상 정보기술부문/ 정보보호부문 투자 산출 방법

■ 개요

- 영업보고서는 자산별 대장과 계정별 원장에 기능 및 서비스 구분이 추가되어 있는 자료로, 일반적인 검토 자료와 다르지 않음.
 - 다만 계정 특성을 보다 쉽게 구분할 수 있는 상세 자료이므로 영업보고서를 추가로 검토하는 것이지, 일반적인 검토원칙을 배제하거나 영업보고서 검토만 수행하는 것을 의미하지 않음을 주의하여야 함.
- 검증받은 기간통신사업자는 영업보고서 작성을 위한 배부 전 자산대장과 비용원장을 기반으로 상세 검토를 수행하여 보다 신뢰성 있게 정보기술·정보보호 대상을 선정하는 것이며, 선정 이후 투자 현황 산출 방법은 일반적인 자료 산출 방법과 동일함.
- 영업보고서 자료를 사용하더라도 비용원장 금액이 차이가 발생하지는 않으며, 자산의 경우 영업보고서 자료를 이용하여 기능 및 서비스를 통하여 정보기술·정보보호 대상을 선정한 후에는 감사보고서상 감가상각비를 사용하여 투자금액을 산정하는 것임.
 - 일반적으로 영업보고서 작성을 위한 조정 사항과 감사보고서와의 차이내역은 마일리지 멤버십, 제조사 장려금, 계약획득원가, 공시지원금 등 정보기술부문/정보보호부문과 관련 없는 항목임.

■ 자산 투자 현황 작성 방법

- 영업보고서 배부 전 자산대장상 모든 자산의 기초분류는 형태·기능·서비스 항목으로 분류되어 있으며, 형태코드와 형태명을 통하여 자산별로 정보기술부문 자산인지 아닌지를 판단하여 자산 투자 현황을 산출함.
 - 다만 기간통신 역무 중 화선설비 임대 서비스의 직접 자산과 부가통신 역무 중 단순설비 임대 중인 직접 자산은 제외함.

참고**영업보고서상 자산의 형태코드와 형태명에 따른 분류**

| 코드 | 형태명 | 정보기술부문 투자 현황 (포함/제외/자산별 판단) |
|--------|-----------|--------------------------------|
| FC0100 | 교환설비 | 포함 |
| FC0200 | 전송설비 | 자산별 판단(기지국 장비는 제외) |
| FC0300 | 선로설비 | 제외 |
| FC0400 | 단말설비 | 자산별 판단 |
| FC0500 | 정보처리설비 | 포함 |
| FC0600 | 전원설비 | 자산별 판단 |
| FC0700 | 방송제공설비 | 자산별 판단 |
| FC1010 | 토지 | 제외 |
| FC1020 | 건물 | 제외 |
| FC1030 | 구축물 | 제외 |
| FC1110 | 선박 | 제외 |
| FC1120 | 차량운반구 | 제외 |
| FC1130 | 기타 일반지원자산 | 자산별 판단 |
| FC1210 | 영업권 | 제외 |
| FC1220 | 주파수 이용권 | 제외 |
| FC1230 | 산업재산권 | 제외 |
| FC1240 | 차지권 | 제외 |
| FC1241 | 임차권리금 | 제외 |
| FC1250 | 개발비 | 자산별 판단 |
| FC1260 | 기타 무형자산 | 자산별 판단 |
| FC1270 | 방송콘텐츠 | 제외 |
| FC1300 | 미착자산 | 제외 |
| FC1400 | 건설 중인 자산 | 제외 |
| FC1500 | 미사용자산 | 제외 |
| FC1600 | 임차보증금 | 제외 |
| FC1710 | 상품 | 제외 |
| FC1720 | 저장품 | 제외 |
| FC1730 | 미작품 | 제외 |
| FC1740 | 기타 재고자산 | 제외 |
| FC1810 | 사용권자산 | 자산별 판단 |

유의 사항

- ▶ 주요 통신 네트워크 인프라를 구성하지 않고, 가입자 쪽에 설치되는 단순 임대 장비는 회계상 장치비 수익으로, 이는 공유기(AP), 모뎀, CCTV, VPN 장비 등 네트워크를 구성하지 않는 가입자 쪽의 장비로 보아 정보기술부문 투자에 포함하지 않음.

| 구분 | 가입자 쪽 단순임대 장비 | 네트워크 구성 장비 |
|------------------|---|---|
| 통신설비의 성격 | 가입자 수의 증가와 비례하여 증가하는 통신 장비 | 단기적으로 가입자 수와 무관한 통신 장비 |
| 통신설비의 위치 | 가입자의 건물 내에 주로 위치 | 통신국사내, 가입자–국사 간, 국사–국사 간에 위치하여 주요 통신 네트워크를 구성 |
| 통신설비의 예시 | 무선공유기(AP), 모뎀, 가입자 쪽 CCTV, 가입자 쪽 VPN 설비 | COT-RT 전송 장비, DWDM, 다중화 전송 장비, 교환 장비 등, 네트워크를 구성하는 VPN 설비 |
| 정보보호 공시 투자 포함 여부 | 제외 | 대상에 포함 |

- ▶ 다양한 자산대장의 정보를 참고하여 회사의 유·무형자산 중 단순 임대관련 자산인지 여부를 판단하고, 분류할 수 있음.
 - 사용목적: 자사의 사용목적이 자산대장에 기재되어 있는지 검토
 - 위치: 자산의 사용위치가 관리되어 있는지 검토
 - 손익관리코드 검토: 수익중심점 등의 비용을 집계하기 위하여 부문별 관리코드 검토
 - 부서관리: 임대자산이 별도 부서에서 관리되고 있는지 확인
 - 프로젝트명: 프로젝트별로 임대 여부에 대한 정보의 유무 검토
 - 자산의 상태: 자산이 임대 중인지 사용 중인지 상태 정보 확인
- ▶ 기간통신사업자의 네트워크보안 또는 정보보호에 직접 관여하지 않고, 가입자 쪽의 정보보호에 활용되는 자산으로, 가입자 쪽에 설치된 단말 장비도 같은 맥락으로 정보보호부문 투자로 인정하지 않음.

| 장비 | 사용목적 | 분류 |
|--------|------------------------|-------------------|
| CCTV | 가입자 쪽에 설치된 CCTV 장치 | 정보기술부문 ×/정보보호부문 × |
| | 통신설비를 감시하기 위한 목적 | 정보기술부문 ○/정보보호부문 ○ |
| VPN 장비 | 가입자 쪽에 설치된 VPN 장치 | 정보기술부문 ×/정보보호부문 × |
| | 통신네트워크 인프라를 구성하기 위한 목적 | 정보기술부문 ○/정보보호부문 ○ |

- 형태코드와 서비스 유형을 통하여 자산을 분류한 후에도 분류되지 않은 자산은 추가로 기능코드와 기능명을 통하여 자산별로 분류 구분함.

참고

영업보고서상 기능코드와 기능명에 따른 분류

| 코드 | 기능명 | 투자 현황 포함/제외/자산별 판단 |
|-------|-----------|--------------------|
| F0101 | 교환 | 포함 |
| F0201 | 중계전송 | 포함 |
| F0212 | 기-교전송 | 포함 |
| F0213 | 교-교전송 | 포함 |
| F0220 | 기지국 설비 | 제외 |
| F022X | 이외의 전송기능 | 포함 |
| F0301 | 중계선로 | 제외 |
| F0410 | 단말 | 자산별 판단 |
| F0501 | 정보처리 | 포함 |
| F0600 | 전원 | 자산별 판단 |
| F0901 | 전기통신 공통설비 | 포함 |
| F1010 | 토건구기능 | 제외 |
| F1110 | 기타일반자산기능 | 자산별 판단 |
| F1210 | 무형자산기능 | 자산별 판단 |
| F1310 | 건설 중인 자산 | 제외 |

예시

기간통신 서비스별 정보기술부문 투자 분류

▶ 서비스별 정보기술 판단 기준 요약

| 역무 | 정보기술부문 판단 |
|-------------------|----------------------------------|
| 전송 역무 | 자산별 분류 기준에 따라 판단 |
| 주파수를 할당받아 제공하는 역무 | 자산별 분류 기준에 따라 판단 |
| 전기통신회선설비 임대 역무 | 제외 |
| 부가통신 역무 | 자산별 분류 기준에 따라 판단, 다만 설비제공 자산은 제외 |
| 전기통신사업 외의 사업 | 자산별 분류 기준에 따라 판단 |

▶ 이동통신 서비스 관련 자산의 정보기술부문 분류

| 코드 | 형태명 | 정보기술부문 포함 | 정보기술부문 제외 |
|--------|------|---|-----------|
| FC0100 | 교환설비 | 이동통신교환기(2G,3G,LTE,5G)로 MME, MSC, IGS, AuC, PGW, SGW, IMS망, SMSC, AAA, 과금, HLR/HSS, MGW , TAS, EIR 등 | |

| 코드 | 형태명 | 정보기술부문 포함 | 정보기술부문 제외 |
|--------|--------|--|---|
| FC0200 | 전송설비 | 기지국-기지국 간 전송(백홀, 프렌트홀 전송), 기지국-교환국간 전송, 국간 전송 장비, 다중화 장비, IPS, 방화벽, VPN 장비 등 | 기지국 장비 및 기지국 관리 장비 (BTS, BSC, RNC, RU, DU, e-NB, 기지국 안테나 등) |
| FC0300 | 선로설비 | | 모든 선로설비(광케이블, 동케이블, 동축케이블, 관로 등) |
| FC0400 | 단말설비 | 국사내 터미널로 이용되는 단말 | 이동통신단말, 키폰 등 |
| FC0500 | 정보처리설비 | 전기통신망을 구성하는 서버, 스토리지 등 데이터 처리장치 | |
| FC0600 | 전원설비 | 통신설비에 직접 전원을 지원하는 전원 설비 | 일반건물 또는 일반건물과 통신설비에 전원을 공동으로 공급하는 전원설비 |

▶ 유선통신 서비스 관련 자산의 정보기술부문 분류

| 코드 | 형태명 | 정보기술부문 | 제외 |
|--------|--------|--|---|
| FC0100 | 교환설비 | 인터넷전화교환기, 시내교환기, 시외 교환기, 국제교환기, 지능망교환기, 구내 교환기, CMTS 등 | |
| FC0200 | 전송설비 | 가입자 중계전송(COT-RT, L3, L2, 스위치 등), 국간 중계전송(WDM, 라우터, 스위치 등), 국제전송, 광동축혼합망 전송장치 등 | |
| FC0300 | 선로설비 | | 모든 선로설비(광케이블, 동케이블, 동축케이블, 관로 등) |
| FC0400 | 단말설비 | 국사내 터미널로 이용되는 단말 | 가입자 쪽에서 사용되는 모뎀, 셋탑 박스, 무선공유기, 전화기, CCTV 단말 등 |
| FC0500 | 정보처리설비 | 전기통신망을 구성하는 서버, 스토리지 등 데이터 처리장치 | |
| FC0600 | 전원설비 | 통신설비의 전원을 직접 지원하는 전원 설비 | 일반건물과 통신설비의 전원을 공동으로 지원하는 전원설비 |

■ 비용 투자 현황 작성 방법

- 영업보고서 배부 전 비용원장상 모든 비용의 기초분류는 형태·기능·서비스 항목으로 분류되어 있으며, 형태코드와 형태명을 통하여 비용별로 정보기술부문 비용인지 아닌지를 판단하여 비용 투자 현황을 산출함.
 - 다만 자산 투자 현황 작성 때와 마찬가지로 기간통신 역무 중 회선설비 임대 서비스의 직접 비용과 부가통신 역무 중 단순설비임대 중인 직접 비용은 제외함.

참고

영업보고서상 비용의 형태코드와 형태명에 따른 분류

| 형태코드 | 형태명 | 투자 현황 포함/제외/비용별 판단 |
|--------|---------------|--------------------|
| FO1010 | 급여 | 별도 인원 검토 |
| FO1020 | 잡급 | 별도 인원 검토 |
| FO1030 | 퇴직급여 | 별도 인원 검토 |
| FO2010 | 복리후생비 | 별도 인원 검토 |
| FO2020 | 여비교통비 | 제외 |
| FO2030 | 통신비 | 비용별 판단 |
| FO2040 | 전력수도료 등 | 제외 |
| FO2050 | 전파사용료 | 제외 |
| FO2060 | 제세공과금 등 | 비용별 판단 |
| FO2070 | 소모품비 | 비용별 판단 |
| FO2080 | 지급임차료 | 비용별 판단 |
| FO2090 | 수선유지비 | 비용별 판단 |
| FO2100 | 차량비 | 제외 |
| FO2110 | 보험료 | 제외 |
| FO2120 | 지급수수료 | 비용별 판단 |
| FO2130 | 교육·훈련비 | 비용별 판단 |
| FO2140 | 접대비 | 제외 |
| FO2150 | 광고선전비 | 제외 |
| FO2160 | 판매비 | 비용별 판단 |
| FO2170 | 잡비 | 비용별 판단 |
| FO3010 | 전용회선료 | 50% 적용 |
| FO3020 | 선로설비사용료 | 제외 |
| FO3030 | 도매제공대가 | 제외 |
| FO3040 | 기타 설비사용료 | 비용별 판단 |
| FO5010 | 대손상각비 | 제외 |
| FO5020 | 경상개발비 및 연구비 | 비용별 판단 |
| FO5030 | 국제정산부담금 | 제외 |
| FO6010 | 접속설비비 | 제외 |
| FO6020 | 접속통화료 | 제외 |
| FO6030 | 접속통신료 | 제외 |
| FO6040 | 접속부대 서비스비 | 제외 |
| FO7030 | 콘텐츠 비용 | 제외 |
| FO8010 | 출연금 | 제외 |
| FO9010 | 콘텐츠 제작비 | 제외 |
| FO9020 | 콘텐츠 구입비 | 제외 |
| FO9031 | 기본채널 콘텐츠 사용료 | 제외 |
| FO9032 | 유료채널 콘텐츠 사용료 | 제외 |
| FO9033 | 유료VOD 콘텐츠 사용료 | 제외 |
| FO9040 | 재송신 비용 | 제외 |

유의 사항

- ▶ 접속료 및 도매제공대가와 같이 다른 기간통신사업자의 네트워크를 전체적으로 사용하는 경우에 해당하는 망이용대가는 정보기술 부문으로 간주되지 않음. 이는 통신설비의 운영권한 및 책임이 다른 기간통신 사업자에게 귀속되므로 정보기술부문으로 분류되지 않는 것임.
- ▶ 다만 통신 서비스를 제공하기 위하여 통신망의 일부를 임차하는 성격인 설비사용료는 자산의 통제권이 해당 기간통신사업자에 있는 것으로 보아, 자산별 성격에 따라 정보기술부문으로 인정함. 예를 들어, 전용회선 이용료(50% 정보기술부문), 기타 설비사용료 등이 이에 속함.
- ▶ 기간통신사업자의 전용회선이용료를 50%만 인정하고 있는 이유는 기간통신사업자의 경우 전송설비와 선로설비를 직접 구축하거나 다른 회사의 전용회선(전송+선로)을 임차하여 사용하게 되는데, 다른 회사의 전송설비와 선로설비의 구성을 파악하기 어려워 동일 비율로 배분하는 방식을 채택함.

- 형태코드와 서비스 유형을 통하여 비용을 분류한 후에도 분류되지 않은 비용은 추가로 기능코드와 기능명을 통하여 분류 구분함.

〈비용의 기능코드로 투자 현황 작성하기〉

| 기능코드 | 기능명 | 정보기술부문 판단 |
|-------|--------------|-----------|
| F0101 | 교환 운영 | 포함 |
| F0201 | 전송 운영 | 포함 |
| F0212 | 기-교전송 운영 | 포함 |
| F0213 | 교-교전송 운영 | 포함 |
| F0220 | 기지국설비 운영 | 제외 |
| F022X | 이외의 전송기능 운영 | 포함 |
| F0301 | 종계선로 운영 | 제외 |
| F0410 | 단말 운영 | 비용별 판단 |
| F0501 | 정보처리 운영 | 포함 |
| F0600 | 전원 운영 | 비용별 판단 |
| F0901 | 전기통신 공통설비 운영 | 포함 |
| F10XX | 토지·건물·구축물 운영 | 제외 |
| F11XX | 기타 일반자산 운영 | 비용별 판단 |
| F2010 | 광고선전 | 제외 |
| F202X | 판매촉진 | 제외 |
| F2030 | 통신단말장치 | 제외 |
| F211X | 가입자 관리 | 비용별 판단 |
| F212X | 마일리지 멤버십 | 제외 |
| F213X | 청구수납 | 비용별 판단 |
| F2210 | 일반관리 | 비용별 판단 |
| F2310 | 기업 이미지 | 제외 |

첨부 4

정보보호 최고책임자(CISO) 신고 접수 문의처

| 기관명 | 전화번호 | FAX | 주소 | 관할 지역* |
|---------|--------------|------------------------------|---------------------------|--------------------|
| 중앙전파관리소 | 02-3400-2344 | 02-3400-2329 | 서울특별시 송파구 송파대로 234 | 국외 등 |
| 서울전파관리소 | 02-2680-1749 | 02-2680-1758 02-2680-1754 | 서울특별시 구로구 오리로 22다길 13-43 | 서울특별시 인천광역시 경기도 |
| 부산전파관리소 | 051-974-5120 | 051-974-5129 | 부산광역시 강서구 체육공원로 6번길 67-17 | 부산광역시 경상남도 |
| 광주전파관리소 | 061-330-6820 | 061-330-6829 | 전라남도 나주시 산포면 매성길 178-24 | 광주광역시 전라남도 |
| 강릉전파관리소 | 033-660-2815 | 033-660-2819 | 강원도 강릉시 연곡면 성안길 40-31 | 강원도 |
| 대전전파관리소 | 042-520-4136 | 042-520-4190 | 대전광역시 서구 신갈마로 86번길 64 | 대전광역시 세종특별자치시 충청남도 |
| 대구전파관리소 | 053-749-2818 | 053-749-2929 | 대구광역시 수성구 동원로 90 | 대구광역시 경상북도 |
| 전주전파관리소 | 063-260-0102 | 063-260-0111 | 전라북도 완주군 봉동읍 둔산3로 114 | 전라북도 |
| 제주전파관리소 | 064-740-2816 | 064-740-2820 | 제주특별자치도 제주시 애월읍 도치돌길 385 | 제주특별자치도 |
| 청주전파관리소 | 043-261-5854 | 043-261-5858 | 충청북도 청주시 서원구 사직대로157번길 30 | 충청북도 |
| 울산전파관리소 | 052-231-8884 | 052-231-8887 | 울산광역시 울주군 서생면 위곡2길 157-6 | 울산광역시 |

* 법인의 경우 등기사항증명서상 주된 사무소 소재지 기준, 개인의 경우 사업자등록증상 사업장 소재지 기준

정보보호 공시 가이드라인

2024. 3.



과학기술정보통신부
Ministry of Science and ICT

KISA **한국인터넷진흥원**
KOREA INTERNET & SECURITY AGENCY