CISO

CHIEF INFORMATION SECURITY OFFICER

정보보호 최고책임자 지정·신고제도 안내서

2024. 9.

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CISO

CHIEF INFORMATION SECURITY OFFICER

정보보호 최고책임자 지정·신고제도 안내서

2024. 9.

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CISO

정보보호 최고책임자
지정·신고제도 안내서

CONTENTS

Ⅰ **정보보호 최고책임자란?** 4

Ⅱ (지정·신고 제도에 따른) **대상자 구분** 6

Ⅲ (일반) **신고의무 대상자** 8

Ⅳ **CISO의 겸직** 10

Ⅴ **CISO의 겸직 예외 대상** 14

Ⅵ **CISO 자격요건** 16

Ⅶ **행정조치** 19

Ⅷ **신고요령** 21

붙임1 CISO 지정신고서 / 22

붙임2 CISO 신고접수 문의처/ /23

I 정보보호 최고책임자란?

정보보호 최고책임자(CISO)는 기업의 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리 등 정보보호 업무를 총괄하는 최고책임자(CISO, Chief Information Security Officer)를 말함

- 정보보호 최고책임자는 정보통신망법 제45조의3제4항 각 호에 따른 정보보호 관련 업무에 대한 최종 결정권 및 책임, 정보보호 업무관련 예산·인사에 대한 직접적 권한을 가짐

1. 정보보호 최고책임자의 업무

- **(정보보호 계획의 수립·시행 및 개선)** 정보통신망의 안정성·신뢰성 확보를 위하여 관리적, 기술적, 물리적 보호조치를 포함하는 종합적 관리계획의 수립·시행 및 개선
- **(정보보호 실태와 관행의 정기적인 감사 및 개선)** 정보보호 실태 등에 대하여 조사하거나 관계 대상자로부터 보고를 받을 수 있으며 정기적인 감사를 통해 사업주 또는 대표자에게 조사결과 및 개선조치를 보고
- **(정보보호 위험의 식별·평가 및 정보보호 대책 마련)** 하드웨어 또는 소프트웨어의 결함이나 체계 설계상의 허점으로 인해 사용자에게 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보의 열람·변조·유출을 가능하게 하는 약점(취약점) 및 위험의 식별평가, 위험을 처리하기 위한 보안조치 설계, 정보보호 대책 마련
- **(정보보호 교육과 모의훈련 계획의 수립 및 시행)** 정보통신서비스 제공자를 대상으로 정보보호를 위해 최소 연 1회 이상 필요한 교육 및 침해사고 모의훈련을 실시

2. 겸직가능 업무

① 정보보호산업의 진흥에 관한 법률 제13조에 따른 정보보호 공시에 관한 업무
② 정보통신기반 보호법 제5조제5항에 따른 정보보호책임자의 업무
③ 전자금융거래법 제21조의2제4항에 따른 정보보호최고책임자의 업무
④ 개인정보 보호법 제31조제2항에 따른 개인정보 보호책임자의 업무
⑤ 그 밖에 이 법 또는 관계법령에 따라 정보보호를 위하여 필요한 조치의 이행

※ ⑤는 직무·직위기술서, CISO 조직 등이 망법에서 규정하는 업무를 전담하고 있는지 여부를 종합적으로 확인

정보보호 최고책임자 직무 질의답변

Q1 인프라 운영·관리(IT 정보시스템) 업무가 정보보호 업무에 포함되는지?

- 일반적인 인프라 운영·관리 업무는 정보보호 업무에 미포함
  - 백신, 보안관리 서버 등 정보보호 차원에서 인프라를 운영·관리하는 업무는 정보보호 업무에 해당

Q2 보안 서비스 사업이 정보보호 업무에 포함되는지?

- 기업 내부의 정보보호 서비스는 정보보호 업무에 해당되나, 타 기업에 대한 보안 서비스 사업은 정보보호 업무에 미해당

Q3 홈페이지 등에 게시하는 개인정보 처리방침에 정보보호 최고책임자를 표시해야하는지?

- 정보통신망법에는 개인정보 처리방침에 정보보호 최고책임자를 표시해야한다는 의무 규정은 없음

Q4 중소기업에서 자체적인 교육 및 침해사고 모의훈련 계획의 수립·시행이 어려운 경우, 참고할 수 있는 정보가 있는지?

- 한국인터넷진흥원 홈페이지(www.kisa.or.kr) 또는 보호나라(www.boho.or.kr) 등에 중소기업 대상 침해사고 교육 및 모의훈련 지원 사업 등을 참고

Ⅱ (지정·신고 제도에 따른) 대상자 구분

- **정보보호 최고책임자(CISO) 지정·신고 기준은 기업유형 및 규모 등에 따라 차이가 있음**
- **신고의무가 제외된 기업은 별도 지정·신고 행위가 없는 경우 영 제36조의7제3항에 따라 사업주나 대표자를 정보보호 최고책임자로 지정한 것으로 간주하여 정보보호 공백을 방지**

신고의무 제외대상

- 자본금 1억원 이하인 자
- 중소기업기본법 제2조제2항에 따른 소기업
- 전기통신사업자, ISMS의무대상자, 개인정보처리자, 통신판매업자 중 어느 하나에 해당하지 않은 중기업 정보통신서비스 제공자

→ **사업주** 또는 **대표자**

일반신고 의무대상

- (신고의무 제외대상에 해당하지 않은) 중기업 이상의 정보통신서비스 제공자

★ '정보통신서비스 제공자'로서 '전기통신사업자, ISMS의무대상자, 개인정보처리자, 통신판매업자'는 CISO를 지정·신고하여야 함

→ **부서의 장** 이상

겸직금지 의무대상

- '정보통신서비스 제공자'로서 ①직전 사업연도 말 기준 자산총액 5조원 이상 또는 ②정보보호 관리체계(ISMS) 인증의무대상자 중 직전 사업연도 말 기준 자산총액 5천억 원 이상

→ 상법 상 **이사**

정보보호 최고책임자 지정·신고 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란 다음 각 호의 구분에 따른 사람을 말한다.

1. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 사업주 또는 대표자
   가. 자본금이 1억원 이하인 자
   나. 「중소기업기본법」 제2조제2항에 따른 소기업
   다. 「중소기업기본법」 제2조제2항에 따른 중기업으로서 다음의 어느 하나에 해당하지 않는 자
      1) 「전기통신사업법」에 따른 전기통신사업자
      2) 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자
      3) 「개인정보 보호법」 제30조제2항에 따라 개인정보 처리방침을 공개해야 하는 개인정보처리자
      4) 「전자상거래 등에서의 소비자보호에 관한 법률」 제12조에 따라 신고를 해야 하는 통신판매업자
2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   가. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자
   나. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 자
3. 제1호 및 제2호에 해당하지 않는 정보통신서비스 제공자: 다음 각 목의 어느 하나에 해당하는 사람
   가. 사업주 또는 대표자
   나. 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   다. 정보보호 관련 업무를 총괄하는 부서의 장

② 법 제45조의3제1항 단서에서 "자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자"란 정보통신서비스 제공자로서 제1항제1호 각 목의 어느 하나에 해당하는 자를 말한다.

③ 법 제45조의3제1항 단서에 해당하는 자가 정보보호 최고책임자를 신고하지 않은 경우에는 사업주나 대표자를 정보보호 최고책임자로 지정한 것으로 본다.

Ⅲ (일반) 신고의무 대상자 (정보통신망법 제45조의3제3항)

원칙적으로 아래 ① 신고의무 제외대상자를 제외하고, 정보보호 필요성이 큰 '중기업' 이상의 ② 정보통신서비스 제공자는 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 (중앙전파관리소장에게 위임) **신고하여야 함**

※ (신고기한) 신고의무*가 발생한 날로부터 180일 이내에 신고 *전임자 퇴사 및 인사이동, (현황점검)개선조치 등

① 신고의무 제외대상자 (신고하지 않더라도 사업주나 대표자를 CISO로 간주)

- 자본금 1억원 이하인 정보통신서비스 제공자
- 중소기업기본법 제2조제2항에 따른 소기업
- 중기업으로서 ①전기통신사업자, ②정보보호 관리체계(ISMS) 인증의무대상자, ③개인정보처리자, ④통신판매업자 중 어느 하나에 해당하지 않은 정보통신서비스 제공자

※ ①~④ 중 어느 하나에 해당하는 정보통신서비스 제공자는 정보보호최고책임자(CISO)를 지정·신고하여야 함

② 정보통신서비스 제공자

- 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자
  - 따라서, 모든 전기통신사업자(기간통신사업자, 부가통신사업자)는 정보통신서비스 제공자에 해당
  - 요건인 ①영리 목적, ②전기통신사업자의 전기통신역무 이용, ③정보의 제공 또는 매개 등과 관련하여서는 법인의 특성·서비스 성격, 목적 등을 종합적으로 고려하여 판단

정보통신서비스 제공자 해당 여부

정보통신서비스 제공자			해당 여부	
영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자	**상법상의 상인 및 회사**		• **영리를 목적으로 사업을 영위하므로 구체적인 영리행위가 없어도 정보통신서비스 제공자에 해당** ※ 단순 제품홍보, 기관 안내 등을 위해 홈페이지를 운영하는 자 등	Y
	비영리 법인		• 학술·종교·자선·기예·사교 등 영리가 아닌 사업을 목적으로 설립된 비영리법인이 설립목적을 실현하기 위해 정보통신서비스를 제공하는 경우	N
			• 다만, **비영리법인이 수익사업을 위해 정보통신서비스를 제공하는 경우**	Y
	특수 법인		• 특수법인 법률 상 목적 중 비영리사업을 위해 정보통신서비스를 제공하는 경우	N
			• 다만, **목적사업 중 영리사업을 위해 정보통신서비스를 제공하는 경우**	Y
	공공 기관	**공기업**	• **기본적으로 영리를 목적으로 사업을 영위** ex) ~공사, ~발전사	Y
		준정부기관	• 정부업무의 수탁수행, 기금관리 업무를 수행 ex) ~진흥원, ~공단	N
		기타공공기관	• 개별적으로 사업목적·설립근거 등으로 영리 목적 여부 판단	Y/N
	의료 기관		• **의료업을 위해 정보통신서비스를 제공하는 경우** ex) 공공의료원, 대학병원도 개인의 민감정보 등을 수집하며 영리활동을 하므로 포함	Y
	학교		• **교육은 비영리 목적에 해당하므로 정보통신서비스 제공자에 해당하지 않음**	N
			• 다만, **학교가 수익사업을 위해 정보통신서비스를 제공하는 경우**	Y
	금융 회사		• **영리목적의 금융업을 영위하는 금융회사**	Y

Ⅳ CISO의 겸직 (정보통신망법 제45조의3제3항)

직전 사업연도 말 기준 자산총액이 5조원 이상이거나, 정보보호 관리체계(ISMS) 인증의무 대상자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 정보통신서비스 제공자

* 자산총액은 개별 법인별로 산정

지위기준

① 정보보호 최고책임자의 직위 (정보통신망법 시행령 제36조의7제1항)

- 겸직제한에 해당하는 대상기업은 이사(상법 제401조의2제1항제3호에 따른 자 또는 같은 법 제408조의2에 따른 집행임원 포함)로 정보보호 최고책임자를 지정해야 함

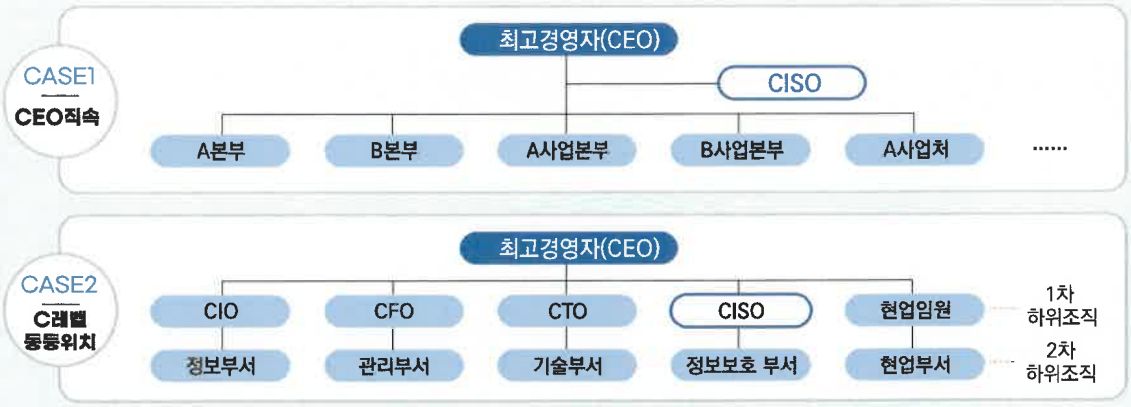
② 정보보호 최고책임자의 지위

- 관련 근거에 따라 지위기준은 '대내외적으로 인정 될 만한 이사급 호칭을 사용' 하고 '실질적 의사 결정'을 종합적으로 확인

모범사례

- **(이사급 호칭)** 전무·상무(보)·이사·본부장·처장·임원 등 **대내외적으로 인정될 만한 이사급 호칭**을 사용
  ※ 호칭은 단순 부여된 명칭 이외에 **인사명령서 및 인사카드, 호칭에 따른 대내외 역할 등을 종합적으로 확인**
- **(실질적 의사결정)** 다른 임원과 직무상 독립하여 권한과 책임을 가진 자를 지정하여야 한다는 점을 고려하여 **CEO 직속 또는 다른 C-레벨과 동등한 위치를 가지는 정보보호 조직도, 위임전결규정 등을 종합적으로 확인**

• (조직체계 예시)



위반사례

• **팀장·파트장·부장·차장·책임 등** 임원이 아닌 일반 직원에게 부여되는 호칭을 사용하고 있음

• 조직구성에 따른 직급체계와는 달리 **특수한 호칭**(센터장·실장·국장 등)을 부여하고 있으나, **실질적 정보보호 집행권한이 있다고 판단하기 어려운 경우**

ex) CEO 직속이 아닌 2차 하위조직으로 운영 or CEO 직속이지만 팀 단위(전체 조직도와 비교)로 판단되는 경우

겸직금지 운영기준

- 망법 상 겸직 제한은 직위에 대한 겸직 제한이 아니라, 업무에 대한 겸직 제한에 해당
- 관련근거(정보통신망법 제45조의3제4항제1호, 정보통신망법 45조의3제4항제2호)에 따라 '정보보호관련 업무'로 규정된 업무 외의 다른 업무는 겸직금지

겸직가능 업무

• **①정보보호 공시**에 관한 업무, **②정보통신기반 보호법**에 따른 정보보호책임자 업무, **③전자금융거래법**에 따른 정보보호최고책임자 업무, **④개인정보 보호법**에 따른 개인정보 보호책임자 업무, ⑤ 그 밖에 이 법 또는 관계 법령상 업무로써 정보보호 최고책임자의 업무와 유사한 업무

※ ⑤는 직무·직위기술서, 조직도 등 CISO 조직이 망법에서 규정하는 업무를 전담하고 있는지 여부를 종합적으로 확인

위반사례

• **'대표이사', '경영기획·운영', '디지털(데이터) 전략기획', 'ICT기획·운영', '비상계획', '진료업무'** 등을 겸직

정보보호 최고책임자 겸직금지 질의답변

Q1 정보보호 최고책임자가 대통령령으로 정하는 임직원에 해당함을 소명하는 방법

- 등기 이사의 경우 법인 등기사항증명서 등을 통해 소명가능
- 비등기이사의 경우 직무·직위기술서, 조직도, 인사명령서, 인사카드 등의 직함명칭, 실질적 업무집행 권한·책임 범위가 포함되어 있는 증빙 서류를 통해 소명가능

Q2 부장(팀장) 직급자로 지정한 정보보호 최고책임자를 이사(상법에 따른 이사로) 볼 수 있는지?

- 부장(팀장) 직급은 임원급으로 보기 어려움
- 상법에 따른 이사에 대한 해석은 전무·상무(보)·이사·본부장· 처장·임원 등 대내외적으로 인정될 만한 이사급 호칭을 사용하고, 다른 임원과의 대등성 및 지휘 관계, 직급 체계, 대우 등을 종합적으로 고려함

Q3 최고위 임원이 아니라 그 이하의 임원을 정보보호 최고책임자로 지정할 수 있는지?

- 정보보호 최고책임자로 지정된 임원(예: 상무이사) 상위에 다른 임원(예: 전무이사)이 있다 하더라도, 정보보호 최고책임자가 정보보호에 관한 회사의 업무를 집행할 수 있는 독자적인 권한과 책임을 갖는 경우 지정요건을 충족하고 있다고 판단

Q4 공공의 경우 이사에 대한 해석은?

- 공공의 경우 처·실장급 이상인 경우 이사급으로 판단

Q5 금융회사의 경우 겸직금지에 해당하나요?

- 전자금융거래법 제2조 제3호 가~마목에 해당하는 자는 정보통신망법 제45조의3제4항 따라 CISO 겸직금지 대상에서 제외함

정보보호 최고책임자 자격요건 관련법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

④ 정보보호 최고책임자의 업무는 다음 각 호와 같다.

1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
   가. 정보보호 계획의 수립·시행 및 개선
   나. 정보보호 실태와 관행의 정기적인 감사 및 개선
   다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
   라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.
   가. 정보보호산업의 진흥에 관한 법률 제13조에 따른 정보보호 공시에 관한 업무
   나. 정보통신기반 보호법 제5조제5항에 따른 정보보호책임자의 업무
   다. 전자금융거래법 제21조의제4항에 따른 정보보호최고책임자의 업무
   라. 개인정보 보호법 제31조제2항에 따른 개인정보 보호책임자의 업무
   마. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란 다음 각 호의 구분에 따른 사람을 말한다.

2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제401조의2제1항 제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)
   가. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자
   나. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 자

V CISO의 겸직 예외 대상

정보보호 최고책임자(CISO) 겸직금지 대상기업 중 자회사의 지배·관리 업무만 수행하는 '순수지주회사'의 경우 겸직운영 예외로 규정하여 겸직금지 의무를 완화

- 자산총액을 기준으로 일률적으로 CISO 겸직금지 의무를 부과함에 따라 자산총액만 클 뿐 소규모 운영·영리사업을 추진하지 않는 순주지주회사의 특수성을 고려
- 다만, 사이버 침해사고 발생시 CISO의 책임과 의무이행, 지주회사의 상징적인 역할을 고려하여 이사급 지위 지정은 유지

〈 정보통신망법 시행령 개정 전후 비교 〉

[기존] 겸직금지 의무대상		[개선] 시행령 개정 후 변화내용			비교
		대상 구분	**순수지주**	**이사급 CISO 지정**	**겸직금지 완화**
이사급 CISO지정 + 겸직금지 이사급	① 자산총액 5조원 이상		순수지주 외	이사급 CISO 지정 + 겸직금지	(기존동일)
	② ISMS 의무대상 + 자산총액 5천억원 이상	-	이사급 CISO 지정 + 겸직금지		(기존동일)

기 존	개 정('23.12.26)
제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란 다음 각 호의 구분에 따른 사람을 말한다. 생략 2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다) 가. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자 나. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인 자 3. 생략 ② 생략 ③ 생략 ④ 생략 ⑤ 법 제45조의3제3항에서 "자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스제공자"란 정보통신서비스 제공자로서 제1항제2호 각 목의 어느 하나에 해당하는 자를 말한다.	⑤ 법 제45조의3제3항에서 "자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스제공자"란 정보통신서비스 제공자로서 제1항제2호 각 목의 어느 하나에 해당하는 자를 말한다. **다만 제1항제2호가목에 해당하는 자 중 독점규제 및 공정거래에 관한 법률 제2조제7호에 따른 지주회사로서 자회사의 경영관리 업무와 그에 부수하는 업무 외에 영리를 목적으로 하는 다른 업무를 영위하지 않는 자**는 제외한다.

한편, '순수지주회사'의 경우 명확한 법적기준이 아닌 사회적 정의만 존재하여, 특정기업이 예외대상에 해당되는지 여부는 현황 점검 요청 시 기업이 직접 입증*필요

* 예외대상 입증을 위해 필요한 서류(예시): 사업자등록증, 재무제표, 영업보고서 및 사업소개 설명자료 등

▸ 지주회사 : 자산총액이 5천억원 이상이면서 **자회사의 주식가액 합계액이 자산총액의 50% 이상**인 회사
- (순수지주회사) 자회사 **지배·관리 업무**만 수행/ (사업지주회사) 자회사 **지배·관리 외 영리사업도 영위**

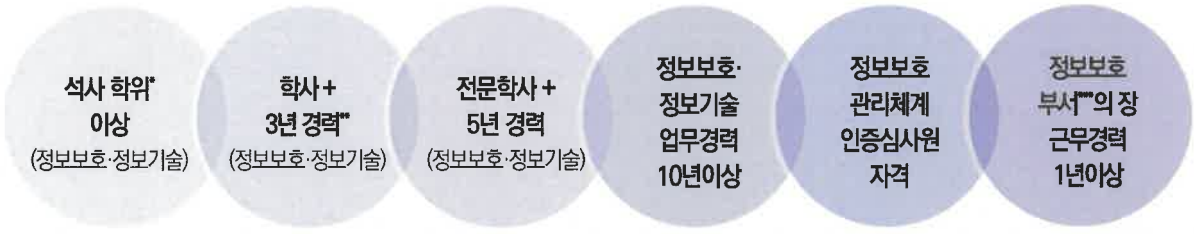
Ⅵ CISO 자격요건

- **정보보호의 전문성을 갖춘 정보보호 최고책임자를 임명할 수 있도록 자격요건 규정**
- **지정·신고 의무대상의 정보보호 최고책임자는 일반 자격요건을 갖추어야 하고, 겸직금지 대상 정보보호 최고책임자는 일반 자격요건과 특별 자격요건을 함께 갖추어야 함**

일반 자격요건 (정보통신망법 시행령 제36조의7제4항)

- 정보보호 최고책임자는 임직원급으로서 다음 중 어느 하나의 자격요건을 갖추어야 함

[일반자격 요건항목]



* 정보보호 또는 정보기술 분야 학위란 전자 관련 학과, 정보통신 관련 학과, 정보보호 또는 정보처리기술 관련 학과의 과정을 이수·졸업한 학력을 의미함

** 정보보호 관련 업무는 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호 업무 등을, 정보기술 관련 업무는 정보통신서비스, 정보통신기기, SW 및 컴퓨터 관련 서비스 업무 등을 말함

*** 부서란 부, 팀 등 명칭과 관계없이 정보보호 업무를 담당하는 책임자와 담당자 등으로 구성된 조직을 말하며 장이란, 해당 조직의 책임자를 말함 (경력은 합산하여 산정)

특별 자격요건 (정보통신망법 시행령 제36조의7제6항)

- 겸직금지 대상의 정보보호 최고책임자는 일반 자격요건을 충족하고 상근하는 자로서, 다음 중 어느 하나에 해당하는 특별 자격요건을 추가로 갖추어야 함
  - 상근이란 날마다 일정한 시간에 출근하여 정해진 시간동안 근무하는 것을 말함
  - 출근이란 사회상규 상 해당 임직원의 근무장소 및 사무공간, 사무용 자산 등에 지배력이 있는 상황에서 근로서비스를 제공하기 위한 근로 준비가 완료된 상태를 의미

[특별자격 요건항목]

정보보호 분야 업무경력이 4년이상	**정보보호 분야 업무경력과 정보기술 업무경력을 합산한 기간이 5년이상** (2년 이상은 정보보호 분야 업무경력 필요*)

* 정보보호 분야 업무와 정보기술 분야 업무를 동시에 수행한 경우에는 정보보호 경력으로 산정

정보보호 최고책임자 자격요건 질의답변

Q1 정보보호 관련 학력·경력의 증명방법

- 졸업증명서, 경력증명서 등으로 증명함

Q2 정보보호 최고책임자가 퇴사 등의 이유로 일시적으로 공석이 된 경우, 자격요건을 만족하지 않은 대직자를 정보보호 최고책임자로 지정·신고하는 것이 가능한지 여부

- 자격요건을 만족하지 않은 대상은 지정·신고 불가
- 정보통신망법에서 규정하는 자격요건을 만족하는 자를 정보보호 최고책임자로 신고해야함

정보보호 최고책임자의 자격요건 관련 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제45조의3(정보보호 최고책임자의 지정 등) ⑦ 정보보호 최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

제36조의7(정보보호 최고책임자의 지정 및 겸직금지 등) ④ 법 제45조의3제1항 및 제7항에 따라 정보통신서비스 제공자가 지정·신고해야 하는 정보보호 최고책임자는 다음 각 호의 어느 하나에 해당하는 자격을 갖추어야 한다. 이 경우 정보보호 또는 정보기술 분야의 학위는 「고등교육법」 제2조 각 호의 학교에서 「전자금융거래법 시행령」 별표 1 비고 제1호 각 목에 따른 학과의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 이와 같은 수준 이상으로 인정되는 학위로 하고, 정보보호 또는 정보기술 분야의 업무는 같은 비고 제3호 및 제4호에 따른 업무를 말한다.

1. 정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위 이상 학위를 취득한 사람
2. 정보보호 또는 정보기술 분야의 국내 또는 외국의 학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 3년 이상 수행한 경력이 있는 사람
3. 정보보호 또는 정보기술 분야의 국내 또는 외국의 전문학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행한 경력이 있는 사람
4. 정보보호 또는 정보기술 분야의 업무를 10년 이상 수행한 경력이 있는 사람
5. 법 제47조제6항제5호에 따른 정보보호 관리체계 인증심사원의 자격을 취득한 사람
6. 해당 정보통신서비스 제공자의 소속인 정보보호 관련 업무를 담당하는 부서의 장으로 1년 이상 근무한 경력이 있는 사람

⑥ 제5항에 따른 정보통신서비스 제공자가 지정신고해야 하는 정보보호 최고책임자는 제4항에 따른 자격과 다음 각 호의 어느 하나에 해당하는 자격을 추가로 갖춰야 하며, 상근(常勤)해야 한다. 이 경우 정보보호 또는 정보기술 분야의 업무는 「전자금융거래법 시행령」 별표1 비고 제3호 및 제4호에 따른 업무로 한다.

1. 정보보호 분야의 업무를 4년 이상 수행한 경력(제4항제1호부터 제3호까지에서 정한 학위 또는 같은 항 제5호의 자격 취득 전의 경력을 포함한다)이 있는 사람
2. 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행(그중 2년 이상은 정보보호 분야의 업무를 수행해야 한다)한 경력(제4항제1호부터 제3호까지에서 정한 학위 또는 같은 항 제5호의 자격 취득 전의 경력을 포함한다)이 있는 사람

Ⅶ 행정조치

정보보호 최고책임자 지정·신고 위반 관련하여 아래와 같은 과태료 부과항목 있음

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〉

[별표 9] 과태료의 부과기준

2. 개별기준

(단위 : 만 원)

위반행위	근거 법조문	위반횟수별 과태료 금액		
		1회	2회	3회
카. 법 제45조의3제1항을 위반하여 제36조의7제1항에 따른 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하지 않거나 정보보호 최고책임자의 지정을 신고하지 않은 경우	법 제76조제1항 제6호의2	750	1,500	3,000
타. 법 제45조의3제3항을 위반하여 정보보호 최고책임자로 하여금 같은 조 제4항의 업무 외의 다른 업무를 겸직하게 한 경우	법 제76조제1항 제6호의3	1,000	2,000	3,000
부. 이 법을 위반하여 법 제 64조제4항에 따라 과학기술정보통신부장관 또는 방송통신위원회로부터 받은 시정조치 명령을 이행하지 않은 경우	법 제76조제1항 제12호			
4) 법 제76조제1항제1호, 제2호, 제6호의2 및 제6호의3의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		1,000	1,000	1,000
두. 법 제 64조제1항에 따른 관계 물품·서류 등을 제출하지 않거나 거짓으로 제출한 경우	법 제76조제3항 제22호	300	600	1,000

또한, 정보통신망법을 위반한 자에 대해서는 해당 위반행위의 중지 또는 시정을 위하여 필요한 시정조치 명령, 시정조치 명령을 받은자에게 시정조치 명령을 받은 사실을 공표할 수 있음

(정보통신망법 제64조 제4항)

정보통신망법 위반에 대해서는 관계 물품·서류 등에 대해 과학기술정보통신부장관 또는 방송통신위원회에 제출할 수 있고, 사업자에 출입하여 업무상황, 장부 또는 서류 등을 검사할 수 있음

(정보통신망법 제64조제1항 및 같은 조 제3항)

행정조치 관련 법령 법령

〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

제64조(자료의 제출 등) ① 과학기술정보통신부장관 또는 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 정보통신서비스 제공자(국내대리인을 포함한다. 이하 이 조에서 같다)에게 관계 물품·서류 등을 제출하게 할 수 있다.

1. 이 법에 위반되는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우

2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우

3. 그 밖에 이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

③ 과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자가 제1항 및 제2항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 정보통신서비스 제공자, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다.

④ 과학기술정보통신부장관 또는 방송통신위원회는 이 법을 위반한 정보통신서비스 제공자에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있고, 시정조치의 명령을 받은 정보통신서비스 제공자에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다. 이 경우 공표의 방법·기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.

6의2. 제45조의3제1항을 위반하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하지 아니하거나 정보보호 최고책임자의 지정을 신고하지 아니한 자

6의3. 제45조의3제3항을 위반하여 정보보호 최고책임자로 하여금 같은 조 제4항의 업무 외의 다른 업무를 겸직하게 한 자

12. 이 법을 위반하여 제64조제4항에 따라 과학기술정보통신부장관 또는 방송통신위원회로부터 받은 시정조치 명령을 이행하지 아니한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다

22. 제64조제1항에 따른 관계 물품·서류 등을 제출하지 아니하거나 거짓으로 제출한 자

Ⅷ 신고요령

신고인

- 회사 대표자
- 정보보호 최고책임자

접수처

① 과학기술정보통신부 전자민원센터(https://www.emsit.go.kr) 온라인 민원신청

회원가입 또는 비회원로그인 > 전자민원신청 > 민원신청 > 신청인 정보입력 > 완료

② 지역별 관할 전파관리소 방문·우편 또는 팩스 접수

제출서류

- 정보보호 최고책임자 지정신고서
- 법인등기사항 증명서(또는 사업자등록증 사본)

붙임1 CISO 지정신고서

정보보호 최고책임자 지정신고서

접수번호	접수일자	처리기간 30일

신고인	상호명(법인명)		사업자등록번호(법인등록번호)
	사무소 소재지		
	대표자		전화번호
정보보호 최고 책임자	성명		전화번호
	휴대전화번호		전자우편주소
	직책/직급		겸직 여부 ☐ 전담 ☐ 겸직 (겸직업무:)
	관련 업무경력	정보보호: 년 개월, 정보기술: 년 개월 총 년 개월	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3, 같은 법 시행령 제36조의7 및 같은 법 시행규칙 제2조제1항에 따라 위와 같이 정보보호 최고책임자의 지정을 신고합니다.

년 월 일

신고인(대표자) (서명 또는 인)

과학기술정보통신부장관 귀하

담당 공무원 확인사항	1. 법인 등기사항증명서(법인인 경우만 해당합니다) 2. 사업자등록증(개인인 경우만 해당합니다)	수수료 없음

행정정보 공동이용 동의서

본인은 이 건 업무처리와 관련하여 담당 공무원이 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 위의 담당 공무원 확인사항 제2호를 확인하는 것에 동의합니다.

※ 담당 공무원의 행정정보 공동이용에 동의하지 않는 경우에는 신고인이 해당 서류를 직접 제출해야 합니다.

신고인 (서명 또는 인)

처리절차

신고서 작성	➡	접수	➡	검토	➡	신고완료
신고인		과학기술정보통신부				

[붙임2]

정보보호최고책임자(CISO) 신고 · 접수 기관

기 관 명	전화번호	모사전송 (FAX)	주 소	관할지역
서울전파관리소	02-2680-1749	02-2680-1758	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	061-330-6823	061-330-6829	전라남도 나주시 산포면 매성길 178-24	광주광역시, 전라남도
강릉전파관리소	033-660-2816	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	053-749-2817	053-749-2929	대구광역시 수성구 동원로 90	대구광역시, 경상북도
전주전파관리소	063-260-0102	063-260-0111	전라북도 완주군 봉동읍 둔산3로 114	전라북도
제주전파관리소	064-740-2812	064-740-2820	제주특별자치도 제주시 애월읍 도치돌길 385	제주특별자치도
청주전파관리소	043-261-5856	043-261-5839	충청북도 청주시 서원구 사직대로157번길 30	충청북도
울산전파관리소	052-231-8883	052-231-8887	울산시 울주군 서생면 위곡2길 157-6	울산광역시

정보보호 최고책임자
지정·신고제도 안내서

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY