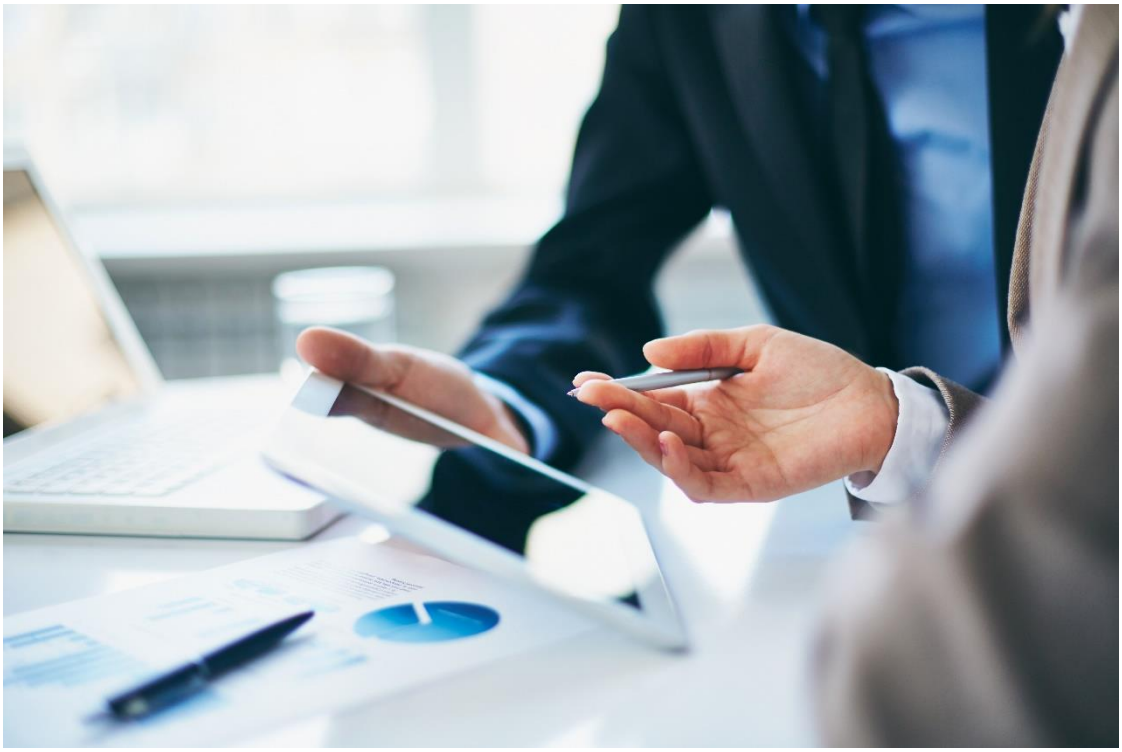
EQST insight

IT 보안 Compliance 대응의 중요성 및 기업의 활용 방안

Overview

IT 보안 시장에는 공급과 수요 즉, 보안회사와 고객사가 존재한다. 고객사는 이미 각종 업무 시스템에 많은 비용을 들여 운영을 하고 있기 때문에, 보안을 고려해야 한다는 보안회사의 제안에는 추가 비용에 대한 부담으로 보안 시스템 도입을 망설이게 된다. 이때, 보안회사는 해킹사고 등 보안 사고의 위험성보다는 관련 법령(Compliance)을 근거로 보안을 고려하지 않을 시 발생하는 회사의 안정적 경영에 대한 우려를 고객에게 전달함으로써 보안 시스템 구축에 대한 고객의 동의를 얻을 수 있다.

따라서, IT 정보통신업에 종사하는 수많은 고객과 IT 인프라 및 보안 서비스 제공 업체는 정보통신망법, 개인정보보호법 등에 의거해 많은 비용이 들더라도, 이를 준수하기 위하여 서비스 제공 업체와 면밀히 협력하고 있다. 그리고 한번 협력하고 나서 끝나는 것이 아닌, 계속해서 변화하는 법에 맞게 지속적으로 Compliance 대응을 하고 있다.



이번 헤드라인에서는 아래의 주요 법령(Compliance) 중에서 **"정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)"**을 대표로 법령을 찾는 방법을 기술하고자 한다. 이를 통해 필요시 언제든지 법을 찾아 관련 업무에 참조 가능하게 함으로써, 여타의 관련 법률도 모두 참조할 수 있는 역량을 가지게 하는 것을 목표로 한다.

정보보호 관련 주요 법령들

infosec

법(법률)	시행령 / 시행 규칙[1] / 고시
정보통신망 이용촉진 및 정보보호 등에 관한 법률 (정보통신망법)	**정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령** **정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙** 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 정보보호 관리등급 부여에 관한 고시 정보보호조치에 관한 지침 집적정보 통신시설 보호지침 정보보호 사전점검에 관한 고시 인터넷 프로토콜 주소를 할당받아 독자적으로 정보통신망을 운영하는 민간사업자 중 침해사고 관련정보 제공자의 범위 정보통신망연결기기등 정보보호인증에 관한 고시 본인확인기관 지정 등에 관한 기준 영리목적의 광고성 정보 전송 기준 위반행위자 등에 대한 과태료 부과 업무처리 지침
개인정보 보호법	개인정보 보호법 시행령 개인정보 보호 자율규제단체 지정 등에 관한 규정 개인정보 영향평가에 관한 고시 개인정보보호 법규 위반에 대한 과징금 부과기준 개인정보의 기술적·관리적 보호조치 기준 개인정보의 안전성 확보조치 기준 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 표준 개인정보 보호지침 가명정보의 결합 및 반출 등에 관한 고시 개인정보 보호위원회의 조사 및 처분에 관한 규정 개인정보 처리 방법에 관한 고시 공공기관의 가명정보 결합 및 반출 등에 관한 고시
소프트웨어 진흥법	소프트웨어 진흥법 시행령 / 시행 규칙
정보통신기반 보호법	정보통신기반 보호법 시행령 / 시행 규칙
정보보호산업의 진흥에 관한 법률	정보보호산업의 진흥에 관한 법률 시행령 / 시행 규칙
전기통신사업법	전기통신사업법 시행령
전자문서 및 전자거래 기본법	전자문서 및 전자거래 기본법 시행령 / 시행규칙
전자서명법	전자서명법 시행령 / 시행규칙
전자정부법	전자정부법 시행령
위치정보의 보호 및 이용 등에 관한 법률	위치정보의 보호 및 이용 등에 관한 법률 시행령
인터넷주소자원에 관한 법률	인터넷주소자원에 관한 법률 시행령
지능정보화 기본법	지능정보화 기본법 시행령 / 시행규칙
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 클라우드컴퓨팅서비스 정보보호에 관한 기준

* 출처 : KISA (한국인터넷진흥원)

1) 시행령 / 시행 규칙 : 어떤 법률을 실제로 시행하는 데 필요한 상세한 세부 규정을 담은 것.
법령에는 모든 상황을 모두 규정할 수 없으므로 큰 원칙만 정해 놓고 시행령/시행규칙을 통해 케이스별 자세한 실천방식을 규정한다.

1. 한국의 법(령)은 어디서 찾아볼 수 있나?

상기 법률 외에도 많은 법이 존재하지만 **"정보통신망법"**은 업무적으로 전혀 상관이 없는 사람들도 한 번쯤 들어봤을 법한 법률이다. 우선, 해당 법률은 어디서 그 상세한 내용을 찾아볼 수 있을까? 인터넷이 본격적으로 국내에 도입된 지 25 년이 넘었지만 아래 사이트를 한 번도 방문한 적이 없는 사람들은 의외로 많을 것으로 생각된다.

(국가법령정보센터 : www.law.go.kr)

사실 해당 국가법령정보센터는 우리나라의 모든 법을 전자 문서 데이터베이스화 한 것이고, 정보통신망법 등은 수많은 법률 중 일부에 해당하는 법률일 뿐이다.

IT 보안 업무를 수행하면서, 법률을 살펴야 하는 경우가 생기는데 통상 고객사에서 가장 많이 하는 질문은 "우리 회사가 왜 이 법률을 지켜야 하나요? 지켜야 한다면 어떻게 해야 하나요?"이다.

이와 같은 질문에 답하기 위해서 관련 법률을 살펴보며 그 해답을 찾는 과정을 살펴보기로 하자.

2. 관련 주요 법규 살펴보기 (예, 정보통신망법)

국가법령정보센터의 최 상단에 “정보통신망법”이라고 검색어를 입력하면 아래와 같이 해당 법률의 명확한 “목적” 과 “정의”를 알 수 있다.

모든 법률은 검색 시 동일한 구조로 목적과 정의를 확인할 수 있다. 따라서, 법률에 대한 상세한 시행령과 시행규칙을 통해 우리 회사가 해당 법률을 준수해야 하는지, 준수한다면 어떻게 해야 하는지에 대한 답변을 찾을 수 있다.

2-1. 우리회사가 왜 정보통신망법을 지켜야 하나요?

"제 3 조(정보통신서비스 제공자 및 이용자의 책무) ① 정보통신서비스 제공자는 이용자를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 이용자의 권익보호와 정보이용능력의 향상에 이바지하여야 한다." ***안전한 정보통신서비스를 제공하기 위한 정보보호는 필수이며, 하기 예와 같이 준수하지 못할 경우 책임자는 벌과금이 부과된다. (사업 지속을 위해서는 반드시 이행해야 한다.)***

과태료 대상 예

> "제 76 조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제 7 호부터 제 11 호까지의 경우에 해당하는 행위를 하도록 한 자에게는 **3 천만원 이하의 과태료를 부과**한다."
> 6 의 2. 제 45 조의 3 제 1 항을 위반하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하지 아니하거나 **정보보호 최고책임자의 지정을 신고**하지 아니한 자
> 6 의 3. 제 45 조의 3 제 3 항을 위반하여 정보보호 최고책임자로 하여금 같은 조 제 4 항의 업무 외의 다른 업무를 겸직하게 한 자
> 6 의 4. 제 47 조제 2 항을 위반하여 **정보보호 관리체계 인증**을 받지 아니한 자

"그렇다면 과태료 대상이 되지 않기 위해 ***정보보호 최고책임자를 지정***하고, ***정보보호 관리체계 인증을 우리 회사가 꼭 받아야 하는지는 어떻게 확인하고 대처***해야 하는가?"라는 추가 질문이 생길 수 있다.

이에 대한 답변은 다시 법률에서 **"정보보호 최고책임자의 지정"으로 검색**, 아래의 조항을 통해 확인할 수 있다.

2-2. 정보보호 최고책임자(CISO) 지정 및 신고 대상 기업인가요?

"제 45 조의 3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 **대통령령으로 정하는 기준에 해당하는 임직원**을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다. 〈개정 2014. 5. 28., 2017. 7. 26., 2018. 6. 12., 2021. 6. 8.〉"

그런데 상기 조항에는 자산총액, 매출액 기준에 대한 상세 내용이 없는데 어떻게 해야 할까?

법률 -〉 **시행령** -〉 시행규칙 중 아래의 "시행령"에서 상세히 대상을 설명하고 있다.

정보통신망법 시행령 45 조 3 의제 1 항 : 세부 기준 확인 가능

제 36 조의 7(정보보호 최고책임자의 지정 및 겸직금지 등) ① 법 **제 45 조의 3 제 1 항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"**이란 다음 각 호의 구분에 따른 사람을 말한다. 〈신설 2021. 12. 7.〉

1. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 사업주 또는 대표자

가. 자본금이 1 억원 이하인 자
나. 「중소기업기본법」 제 2 조제 2 항에 따른 소기업
다. 「중소기업기본법」 제 2 조제 2 항에 따른 중기업으로서 다음의 어느 하나에 해당하지 않는 자
1) 「전기통신사업법」에 따른 전기통신사업자
2) 법 제 47 조제 2 항에 따라 정보보호 관리체계 인증을 받아야 하는 자
3) 「개인정보 보호법」 제 30 조제 2 항에 따라 개인정보 처리방침을 공개해야 하는 개인정보처리자
4) 「전자상거래 등에서의 소비자보호에 관한 법률」 제 12 조에 따라 신고를 해야 하는 통신판매업자
2. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 이사(「상법」 제 401 조의 2 제 1 항제 3 호에 따른 자와 같은 법 제 408 조의 2 에 따른 집행임원을 포함한다)
가. 직전 사업연도 말 기준 자산총액이 5 조원 이상인 자
나. 법 제 47 조제 2 항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5 천억원 이상인 자

2-3. 정보보호 관리체계(ISMS) 인증 대상 기업에 해당하나요?

“제 47 조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 제 4 항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. 〈개정 2012. 2. 17., 2013. 3. 23., 2015. 12. 1., 2017. 7. 26.〉”

동일하게 정보보호 관리체계(ISMS) 인증을 우리 회사가 꼭 받아야 하는지는 시행령 49 조를 통해 확인 가능하다.

정보통신망법 시행령 49 조 : 인증 대상 기업 기준 상세 확인 가능

제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 **“대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자”란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자**를 말한다.
② 법 제47조제2항제3호에서 **“대통령령으로 정하는 기준에 해당하는 자”**란 다음 각 호의 어느 하나에 해당하는 자를 말한다. 〈개정 2016. 5. 31.〉
1. **연간 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당**하는 자
가. 「의료법」 제3조의4에 따른 상급종합병원
나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

이 밖에도 정보통신망법에서 정보통신망 서비스 제공업체(고객)가 준수해야 하는 조치사항은 상당히 많고, 고시 등을 통해 자세하게 가이드라인을 제시하고 있으며 아래와 같이 구체적인 보호조치를 기술하고 있다. **“정보보호조치에 관한 지침”**

제 2 장 정보보호조치

제3조(정보보호조치의 내용) 법 제45조 제2항에 따라 정보통신서비스 제공자가 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위하여 마련하여야 하는 관리적·기술적·물리적 보호조치의 구체적인 내용은 별표1과 같다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률
[시행 2021. 12. 9.] [법률 제18201호, 2021. 6. 8., 일부개정]
제45조(정보통신망의 안정성 확보 등) ① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다. 〈개정 2020.6.9〉
1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 "정보통신망연결기기등"이라 한다)를 제조하거나 수입하는 자
② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 제1항 각 호의 어느 하나에 해당하는 자에게 이를 지키도록 권고할 수 있다. 〈개정 2012.2.17, 2013.3.23, 2017.7.26, 2020.6.9〉
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. 〈개정 2016.3.22, 2020.6.9〉
1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치
5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치
④ 과학기술정보통신부장관은 관계 중앙행정기관의 장에게 소관 분야의 정보통신망연결기기등과 관련된 시험·검사·인증 등의 기준에 정보보호지침의 내용을 반영할 것을 요청할 수 있다.

별표·서식

법제처 국가법령정보센터

정보보호조치에 관한 지침
[시행 2017. 8. 24.] [과학기술정보통신부고시 제2017-7호, 2017. 8. 24., 타법개정]

• 별표목록 [별표 1] 보호조치의 구체적인 내용(제3조 관련) 선택

• 별표연혁 정보보호조치에 관한 지침 [별표 1] [제2017-7호, 고시, 2017. 8. 24. 선택

		설치·운영	운영
		2.1.4. 정보보호를 위한 모니터링	▸ 주요시스템·네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위한 모니터링 시스템 구축 또는 위탁 운영을 통하여 침해사고 탐지·대응 체계 운영
2. 기술적 보호조치	2.2. 정보통신 설비 보안	2.2.1. 웹서버 보안	▸ 외부에 서비스를 제공하는 웹서버는 단독서버로 운영하고 DMZ에 설치
		2.2.2. DNS서버 보안	▸ 과부하에 대비한 부하분산 대책을 마련 ▸ 설정파일 백업 실시
		2.2.3. DHCP서버 보안	▸ 과부하에 대비한 부하분산 대책을 마련 ▸ 설정파일 백업 실시 ▸ IP 할당 상황 등에 대한 로그기록 유지·관리
		2.2.4. DB서버 보안	▸ 내부망에 설치 ▸ 외부망에서 직접 접속할 수 없도록 네트워크를 구성
		2.2.5. 라우터/스위치 보안	▸ ACL(Access Control List) 등의 접근제어 기능을 적용할 수 있는 설비를 사용
		2.2.6.	▸ 이상징후 탐지를 알리는 경고 기능을 설정하여 운영 ▸ 정보보호시스템 보안기능(비정상 트래픽 차단 등)의 정상 작동

3. IT 보안 기업 Compliance 준용 가이드라인 예시

고객사는 관리적 보안의 수단으로 회사 보안규정 제•개정을 통해 정보보안을 이행할 수도 있으나, 법률에서 정의하는 보안 요구사항을 만족하기 위해서는 기술적 보안 즉, 관련 Compliance 를 만족하는 보안솔루션을 검토하여 도입하게 된다.

보안솔루션 제공 업체는 공급하는 솔루션이 법률에서 정한 규정을 준수하는지에 대해 충분히 검증하게 되며, 일반적으로 아래와 같이 제품 소개 자료에 표기하고 있다.

개인정보보호위, 금융감독원, 금융위원회 등 5대 기관의 6대 규정을 준수합니다. SSL/TLS 기반으로 만들어진 도박사이트와 구글 번역사이트 우회접속을 차단합니다.

- 개인정보보호법고시 <개인정보의 안전성 확보조치 기준>

조항	내용	WebKeeper 기능
9조 악성 프로그램 등 방지	악성프로그램 등을 방지할 수 있는 보안프로그램 운영 필요	악성코드배포/유해사이트 차단

- 금융위원회 <전자금융 감독규정>

조항	내용	WebKeeper 기능
16조	② 악성코드 감염시 확산 및 피해최소화 조치	악성코드 배포 웹사이트 차단
17조	⑤ 단말기에서 음란, 도박 등 비업무사이트 접근 통제대책마련	비업무사이트 접근 차단

- 정보통신망법고시 <개인정보의 기술적 관리적 보호조치 기준>

조항	내용	WebKeeper 기능
7조 악성프로그램 방지	- 백신SW 일1회 이상 주기적으로 갱신/점검 - 악성프로그램 관련 경보 or 백신SW, OS 업데이트 공지시 최신 SW로 즉시 갱신/점검	악성코드 배포 웹사이트 차단

* 출처: ㈜소만사 홈페이지(www.somansa.com)

마치며

법에 대해 막연히 낯설고 어려울 것이라는 생각을 가진 분들이 이번 EQST insight 헤드라인을 통해 업무와 관련된 법을 언제든 찾아보고 업무에 잘 참조할 수 있게 되길 바란다.

특히, 현장에서 고객의 Compliance 관련 문의(예, 우리 회사의 정보보호최고책임자는 꼭 임원급으로 지정해야 하나요? 겸직은 가능한가요? 등)가 들어왔을 때, 관련 법령을 "국가법령정보센터"에서 찾고, 상세 사항을 "시행령, 시행규칙, 고시, 가이드라인"에서 확인해 객관적 자료로 해답을 제시함으로써 고객 신뢰도 향상에도 도움이 되었으면 한다.