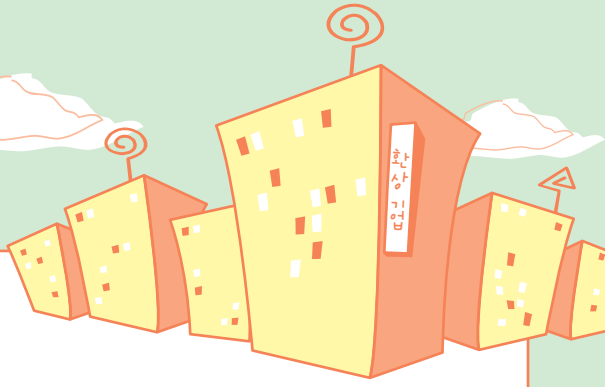


정보보호 정책 규정집

정보보호 활동 기준 제시하기

KISA의 중소기업 정보보호 수준 자가평가를 통해 얻은 환상기업의 보안 성적표는 김 대리의 예상보다 훨씬 더 심각한 수준이었다. 정보화 규모와 정보화 의존도가 중간 수준으로 평가된 환상기업의 가장 큰 문제는 정보보호 활동을 위한 정책지침과 활동방향이 없다는 점. 환상기업의 정보보호 업무가 시작된 지 불과 3개월이 채 되지 않는다는 점을 감안해 본다면 당연한 결과였다. 그래서 김 대리의 업무 목표는 자연스럽게 환상기업의 정보보호 정책수립으로 이어지게 됐다.

정보보호뉴스 취재팀

국가는 물론 모든 조직에는 규칙이라는 것이 존재한다. 해서는 안 될 것과 허용 가능한 범위를 알려주는 규칙은 모든 구성원들의 행동기준이 된다. 정보보호 분야 역시 마찬가지. 기업이나 기관의 정보보호 활동을 보다 체계적으로 정립하고 기업 차원의 정보보호 방향을 제시하기 위해 반드시 필요한 것이 정보보호 정책규정집이다. 생각이 여기에 이르자, 김 대리는 보안정책을 마련하기 위한 사전 준비단계에 들어가게 된다. 그리고 첫 단계로 보안정책의 구성을 위한 환상기업의 정보보호 범위를 규정하는 작업부터 시작했다.

기업 정보보호 정책 규정집이란

기업이 정보보호 활동을 성공적으로 수립하고 지속시키기 위한 우선적으로 해야 할 사항은 해당 기업만의 보안정책을 수립하고 이를 적용시켜 나가는 것이다. 정보보호 규정집은 기업이 보호해야 할 대상을 정의하고, 보호 대상에 위협을 가할 수 있는 위협요소를 분석해 그에 대응하는 방안을 지침형태로 수립해 놓은 일종의 법률집인 셈이다. 대개 보안규정집이 작성되면 기업의 최고 경영진의 승인을 통해 구성원들에게 알려지게 되며, 조직의 모든 구성원들이 보안정책과 절차를 따를 수 있도록 별도의 훈련 및 교육이 이뤄진다.

기업의 정보보호 정책 및 규정 내용을 일반화하기에는 어려움이 존재하게 되는데, 가장 큰 이유는 산업별로, 또 기업별로 각각 정보보호의 범위 및 대상이 다르기 때문이다. 가령, 제조업체에서는 가장 중요한 정보보호 대상이 자동화된 공장라인이 될 수 있으며, IT 서비스 기업의 경우에는 개인정보보호, 즉 회원 DB가 가장 중요한 보안 대상이 되며, '무엇을 보호할 것인지'에 따라 기업의 정보보호 정책 방향은 변경되고 또 달라지게 된다. 아래는 보안정책 구성 시 적용되는 일반적인 구성요소들이며, 정보보호 범위와 대상에 대해서는 담당부서의 주기적인 점검을 통해 지속적으로 검토 보완해 나가야 한다.

〈정보보호 정책의 일반적인 구성〉

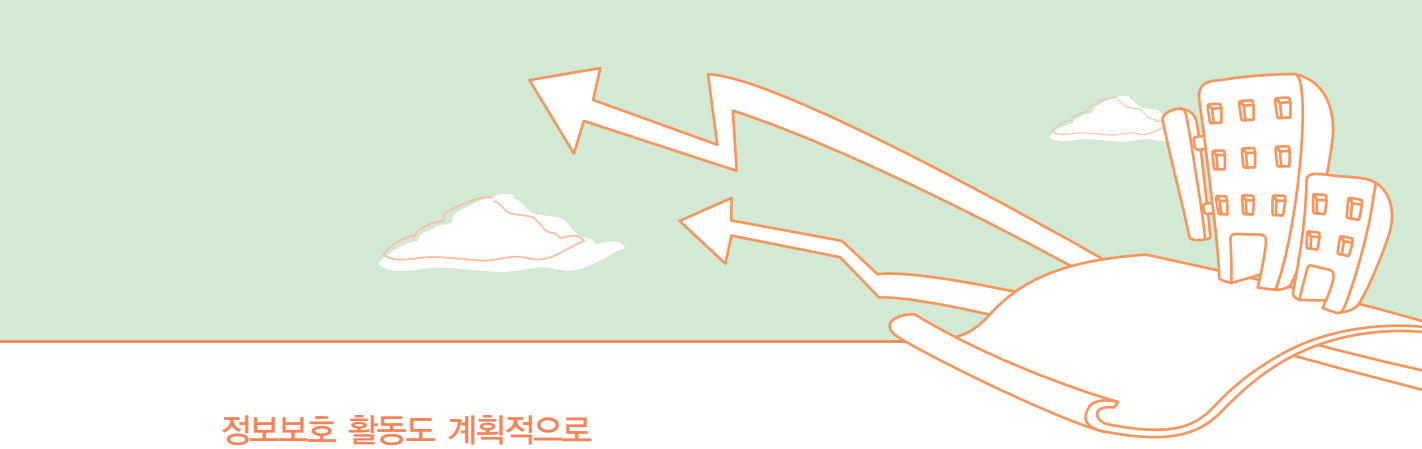
- 보안조직 구성 및 운영
- 정보자산 관리
- 출입자 및 반출입 관리
- 인원 보안(입사/퇴사자 관리)
- PC 보안
- 저장장치 보안
- 전산시스템 보안
- 통신망 보안
- 침해사고 예방 및 대응절차
- 상벌기준

보안정책 위반 시 대응 및 처벌 방법

사회법률, 가령 교통법규를 준수하지 않는다면 벌금이나 그에 상응하는 처벌을 받게 되듯, 기업의 정보보호 정책에 명시된 규정을 위반하는 구성원들에게도 분명한 징계가 필요하다. 국내에서는 정보보호 정책과 징계가 일반화돼 있지 않기 때문에 보안사항을 위반한다 해도 유야무야 끝나는 경우가 많지만, 정보보호가 기업 문화 속에서 생활화되기 위해서는 보안 위반사항에 대한 적절한 징계는 매우 중요하다. 보안정책 위반에 대해서는 징계위원회 개최를 통해 보안기준 위반자(고의, 실수, 공모, 교사, 방조자 등)와 해당 부서 관리 책임자에게 징계를 내릴 수 있다. 일반적으로 보안정책 위반자에게는 1차 보안경고장을 발부하고 위반사항에 따라, 연간 벌점 누적 합계를 계산해 인사고과에 반영하는 경우가 많다.

보안규정 위반내용 및 벌점/징계 건의 기준 예시

(출처 : 2007 CERT 구축 및 운영 가이드(KISA, CONCERT 공동발행)



정보보호 활동도 계획적으로

쉽지는 않았지만, 환상기업의 정보보호 대상과 범위를 파악하고 이를 바탕으로 목차를 구성해 정보보호 규정집을 만들게 된 김 대리. 막상 규정집 제작을 완료한 김 대리는 정보보호 규정집이 보다 현실적이고 효과적으로 활용되기 위해서는 환상기업 구성원들에게 이해시킬 수 있도록 해야 하며, 이를 위해서는 정보보호 규정에 근거한 정보보호 활동계획과 실천이 필요하다는 사실을 알게 됐다. 특히, 약 20년 전 설립된 환상기업에서는 지금까지 단 한번도 정보보호 정책이나 규정을 제작해 놓은 사례가 없었기 때문에 김 대리가 만들어낸 정보보호 정책은 오히려 구성원들에게 불쾌감을 주거나 낯선 문화로만 비춰질 수 있기 때문이다. 김 대리는 그런 의미에서 환상기업의 정보보호 규정홍보를 중심으로 한 활동계획을 수립하기로 결심했다.

보안활동 계획 수립

보안활동 계획은 조직의 성격에 따라 연간 또는 월간 계획을 수립해 진행하는 것으로, 체계적인 보안활동 수행에 효과적이다. 보안활동 계획 수립 시에는 기업의 정보보호 전략방향을 먼저 선정하고, 그 전략에 따른 세부 실행과제 설정, 수행시기 등을 명확히 표기하는 것이 필요하다. 특히, 정보보호 관련 부서 혹은 담당자의 경우에는 자신들의 업무 성과를 입증할 수 있는 명확한 근거자료가 부족하기 때문에 작성된 보안활동 계획은 정보보호 업무 성과와도 밀접한 관련을 맺고 있음을 잊지 말아야 한다.

정보보호 보안활동 계획 예시
(출처 : 2007 CERT 구축 및 운영 가이드(KISA, CONCERT 공동발행)

환상기업의 정보보호 정책 규정집과 정보보호 활동계획을 정보보호 담당자 홀로 만들어내기 쉽지 않았음에도 불구하고, 회사 내 구성원들에게 정보보호를 실천할 수 있는 기준을 마련해 놓았다는 점에서 김 대리는 보안업무에 대한 자신감을 갖게 됐다. 물론, 이런 정보보호 정책을 구성원들이 따를 수 있도록 충분한 홍보와 계도가 필요하겠지만 말이다.

이제 한 숨을 돌린 김 대리. 다음 목표로 환상기업의 직원들이 정보보호를 얼마나 잘 수행하고 있는지 살펴보는 감사활동을 수행해 보기로 했다.