

실무 꿀 tip! 총무 업무 지침서	
16차시	정보보안 관리

<1> 인적 보안 관리하기

[1] 인적 보안 관리 계획 수립

- 인적 보안 관리를 수행하기 위해서는 정보 통신망 이용 촉진 및 정보 보호에 관한 법률, 부정 경쟁 및 비밀 보호 관련 법률, 영업 비밀 보호 법률, 저작권 보호법, 개인 정보에 관한 법률, 공공 기관의 개인 정보 보호에 관한 법률을 숙지해야 한다.
- (1) 정보통신망 이용 관련 법률 : 정보 통신망 이용 촉진 및 정보 보호에 관한 법률은 개인 정보를 보호하고 안전한 정보 통신 환경을 조성하기 위한 법률
- (2) 부정 경쟁 및 비밀 보호 관련 법률 : 부정 경쟁 행위는 유사한 표지를 사용하여 타인의 상품과 혼동하게 하는 행위, 원산지를 허위 표시하는 행위, 타 상품과 유사한 이름을 사용하는 행위이며, 영업 비밀 침해행위는 수많은 노력과 시간이 투입되어 만들어진 기업의 비밀 정보를 부정한 수단으로 취득하여 사용하거나, 비밀 유지의 의무를 가진 자가 그 비밀을 사용하거나 공개하는 행위를 가리킨다. 이러한 행위는 모두 법에 의해 처벌을 받게 되며, 특히 영업 비밀 보호의 필요성이 강조되고 있는 사회의 변화에 따라 영업 보호를 위한 법률이 강화되고 있다.
- (3) 저작권보호법 : 2005년부터 저작권 보호법이 발효되어 시행되고 있다. 저작권 보호법은 저작자의 권리를 보호하고 저작물의 공정한 이용을 도모하여 문화 발전에 기여 한다.
- (4) 개인정보보호에관한 법률 : 공공 기관의 컴퓨터에 의해 처리되는 개인 정보를 보호하기 위해 필요한 사항을 정한 법률

[2] 인적 보안 관리 운영

(1) 내부 인원 보안 관리 항목

- 내부 인원에 대한 보안 관리 항목은 신상 검증, 정보 보호 서약서 작성, 업무 시스템 계정관리, 사원증 관리, 장비 지급, 사원증(출입 카드 관리), 자산 회수 등이 있다. 또한 채용, 재직, 퇴직 시 등 단계별로 구분하여 적절한 보안 대책에 대해 이해한다.
- 직원을 채용할 때에는 재직 중 취득한 회사 비밀을 누설하는 경우 손해 배상은 물론 민형사상 책임을 지겠다는 내용의 보안 서약서에 대한 세부 내용을 숙지하고 실무 반영에 대해 이해한다.
- 재직 중인 핵심 인력에 대해서는 정기적으로 면담을 실시하고 금전적 문제와 근무 여건 제반 애로 사항을 수시로 파악하여 불만이 없도록 사전에 조치하도록 운영하여야 한다.
- 정기적으로 보안 교육을 실시하는 한편, 정기 또는 불시 보안 점검을 실시하여 경각심을 제고할 수 있도록 보안 교육 내용을 이해해야 한다.
- 퇴직 시에는 재직 중에 관리하였던 연구·개발 및 영업 비밀과 관련된 서류 등 일체를 반납할 수 있도록 관련 부분 보안 관리 내용을 이해하고 반영할 수 있어야 한다.

(2) 외부 인원 보안 관리 항목

- 외부 인원에 대한 통제, 보안 준수, 계약 등에 대한 필수 항목에 대하여 이해해야 한다. 업무상 정기적으로 출입하는 협력업체 직원은 최소한으로 제한하고 출입 지역도 일정한 한계를 두어 핵심 시설에는 일체 접근하지 못하도록 엄격하게 통제할 수 있도록 관련 내용을 숙지해야 한다.

- 하청 및 부품업체와 제품 판매업체 직원에 대해서도 중요 정보에 접근하지 못하도록 사안별로 적절한 보안 대책을 수립해야 함을 숙지한다. 특히 R&D 연구 인력에 대해서는 언행과 동향 등을 파악하고 이상 행동이 포착 되었을 때에는 지체 없이 보안 담당자에게 통보하여 조치를 취할 수 있도록 한다.

(3) 중요 자료 보안 관리 항목

- 제품의 설계도, 소스 코드 등 핵심 기술 자료는 영업 비밀로 분류하고 비인가자는 접근하지 못하도록 물리적, 기술적 보안 대책을 강구 하도록 하며, 중요 자료를 외부에 제공하거나 열람시키는 것은 엄격히 제한하되, 부득이하게 제공해야 할 경우에는 관련 인원을 최소한으로 제한하고 보안 서약서를 받는 등 적절한 보안 대책을 실행할 수 있도록 한다. 기술 이전이나 하청 계약 체결 시 자료를 제공할 때에는 반드시 비밀 유지 의무 조항을 포함 시키고 이를 위반하였을 경우 책임 소재를 명시하여 회사 자산을 보호할 수 있도록 운영해야 한다.

<2> 시설물 보안 관리하기

[1] 시설물 보안 관리 계획 수립

(1) 시설 보호 관리

- 회사는 주요 정보 자산 및 관련 시설을 포함하고 있는 물리적 보호 구역을 설정하는데. 그 이유는 권한 없는 물리적 접근이나 각종 물리적, 환경적 재난으로부터 정보 및 정보 시스템을 보호하기 위하여 물리적 보호 구역의 지정이 필요하다.
- 보안 구역은 통제 구역, 제한 구역을 설정한 후 운영하여야 하며, 보안 구역 통제는 출입 통제 관리, 통제 구역 통제, 제한 구역 통제 등을 실시해야 한다. 또 물리적 보호 구역은 환경 재난에 대비한 설비를 규정하여 화재, 수재, 전력 이상 등의 환경 재난을 감지하고 경보 및 대응하는 설비를 설치하여 관리하며, 화재, 홍수, 지진 등 자연 재난 및 인재에 대비한 설비를 충분히 갖추고 있어야 한다. 환경 설비는 화재 방지 및 소화 설비, 그리고 장비 설비를 관리하여야 하며, 전원 설비는 무정전 전원 공급 장치(UPS)와 백업 발전기를 구축하여야 한다.

(2) 출입 보안 관리

- 출입 제한을 요구하는 업무 및 장소는 출입 통제 시스템을 구축하여 비인가자에 대한 접근을 사전에 차단하고 주요 시설물, 인원, 문서 등을 외부 침입이나 파괴 행위로부터 보호한다.
- 출입 통제 대상을 명확하게 하고 해당 장소에 적절한 출입 통제 시스템을 설치, 운영해야 한다.
- 외부인이 내부로 무단출입할 수 없도록 물리적 접근 통제 시설과 감시 장치 또는 무단 침입 경보 시스템 등을 구축해야 하며, 회사의 각 출입문은 출입이 허가되지 않은 비인가자가 출입할 수 없도록 통제하고 관리 운영해야 한다.
- 타 업체와 함께 건물을 사용할 경우 외부로부터의 투시, 도청에 대한 보안 대책을 수립하여야 한다.
- 보안 관리자는 정보 자산 관리를 위해 회사에 출입하는 임직원 및 협력 회사 임직원, 모든 외부 인력(차량 등 포함)에 대하여 물품 검색 및 반출입 내용을 점검할 수 있으며, 임직원 및 외부 인력은 이러한 검색 및 점검에 협조해야 한다.

[2] 시설물 보안 관리 운영

(1) 중요 시설 보호 관리 항목

- 중요 시설 보호 관리 항목은 생산 공장, 사무실, 연구실 등 중요 시설의 위치, 특성 등을 면밀히 검토하여 시설 자체보다는 그 시설이 가지고 있는 기능을 보호할 수 있는 대책을 수립할 수 있도록 중요 시설을 숙지한다. 시설은 중요도에 따라 제한 지역, 제한 구역, 통제 구역으로 구분하여 지정하고 비인가자가 임의로 출입하지 못하도록 보안 대책을 수립하여 시행할 수 있도록 한다. 중요 시설에는 CCTV, 적외선 감지기, 카드 키, 지문 인식 시스템 등 과학 장비를 이용한 24시간 출입 통제 시스템을 설치, 운영한다.

(2) 출입 통제 항목

- 핵심 시설에 대해서는 출입 인가자를 지정하고, 인가된 인원 이외에는 출입하지 못하도록 통제해야 한다. 협력업체 직원이나 시설 또는 장비 보수 등을 목적으로 정기적으로 출입하는 인원은 사전에 신원 확인에 필요한 서류를 확보하여 비치하고 보안 서약서를 받아야 하며, 보안 서약서 내용을 숙지해야 한다. 임시 출입자는 먼저 신분을 확인한 후 출입 대장에 인적 사항, 방문 목적, 방문 대상 직원 등을 기재하고 임시 출입증을 패용하게 한 후 반드시 직원의 안내를 받아 출입하도록 조치를 취한다.

(3) 보안 구역 선정 기준

- 제한 지역은 본사 건물 전체, 공장 및 연구소 건물 전체, 지사 및 계열 회사 전체로 적용한다. 제한 구역은 사내한 이상의 정보 자산을 취급 및 보관하는 장소, 주요 인프라 시설구역, 주요 시설 운영 및 감시를 위한 관제 센터, 주요 경영진이나 VIP 등의 업무 구역, 업무 및 조직의 특성상 조직장 및 정보 보안 책임자가 제한 구역으로 지정이 필요하다고 판단되는 장소로 한다.
- 통제 구역은 통신실, 전산실, 방재실, 무기고, 기밀에 해당하는 정보 자산을 대량으로 취급하거나 보관하는 장소, 업무 및 조직의 특성을 고려하여 정보보호위원회에서 통제 구역으로 지정이 필요하다고 판단되는 장소로 한다.

(4) 보안 구역 승인 및 책임

- 제한 구역과 통제 구역의 설정은 최소한의 범위로 제한하고, 비인가자 또는 외부 인원의 업무상 출입이 빈번한 구역의 설정을 지양한다. 선정된 대상을 통제 구역으로 설정 시 정보보호위원회의 승인을 득한다. 단, 제한 구역은 조직장 및 정보 보안 책임자의 전결로 승인할 수 있다. 보호 구역의 관리로 관리 책임자'정'은 보호 구역 담당 조직의 장이 되며, 관리 책임자 '부'는 관리 책임자 '정'이 소속 직원 중에서 지정하여 보호 구역을 관리한다.

<3> 정보 보안 관리하기

[1] 정보 유출 방지 계획 수립

(1) 정보 보안의 주요 목표로는 기밀성, 무결성, 가용성이 있다.

1) 기밀성

- 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다. 비밀 보장이라고 할 수도 있으며, 원치 않는 정보의 공개를 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있다.

2) 무결성

- 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다. 다시 말하면,

수신자가 정보를 수신했을 때 또는 보관되어 있던 정보를 꺼내 보았을 때 그 정보가 중간에 수정 또는 침삭되지 않았음을 확인할 수 있도록 하는 것이다.

3) 가용성

- 허락된 사용자 또는 객체가 정보에 접근하려고 할 때 이것에 방해받지 않도록 하는 것이다. 최근 네트워크의 고도화로 대중에게 많이 알려진 서비스 거부 공격(DoS: Denial of Service Attack)이 이러한 가용성을 해치는 공격이다. 정보 보안 관리 내용(항목) 정보 보안 관리는 문서 보안 등급 관리, 보안 등급 분류 기준, 폐기, 쇄절기 운용, 조직 내 인사 정보 보안, 전산 및 통신 보안 관리, 도청 방지, 이동식 저장 매체, 모사 전송 기기 관리, 전자 우편 관리, 인터넷 보안 관리, 암호 관리 등이 있다.

(2) 정보 보안 정책은 최고 경영자의 승인을 받아야 하며, 정보보호위원회가 설치되어 있는 경우 보안 정책이 정보보호위원회에 의해서 검토되고 결정되어야 한다. 보안 정책 문서는 모든 관련자 및 임직원에게 이해하기 쉬운 형태로 공유한다. 정보 보안 정책서가 모든 관련자 및 임직원에게 배포되고, 모든 관련자 및 임직원은 정보 보안 정책을 숙지한다. 정보 보안 문서 하위 관련 문서도 필요시 모든 관련자 및 임직원에게 배포하고 관련자 및 임직원이 숙지한다.

(3) 정보 보안 정책은 회사의 사업 목표와 연구 개발 및 기술 정책과 일관성을 유지해야 한다. 정보 보안 정책을 구체적으로 시행하기 위한 정보 보호 지침, 절차, 표준을 수립한다. 정보 보안 정책은 정기적으로 타당성을 검토하여야 하며, 중대한 보안 사고 발생, 취약성 발생에 의한 새로운 위협, 정보 보안 환경에 중요한 변화 등이 발생하였을 경우에는 관련 사항의 타당성을 추가로 검토한다.

[2] 정보 보안 관리 운영

- 정보 보안이란 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다. 정보를 제공하는 공급자 측면에서 보면 내외부의 위협 요인들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산 시설 등 정보 자산을 안전하게 보호·운영하기 위한 일련의 행위를 말하며, 사용자 측면에서는 개인 정보 유출, 남용을 방지하기 위한 일련의 행위를 말한다. 수립된 계획에 따라 통제 계획이 효과적으로 운영되도록 정기 점검을 한다.