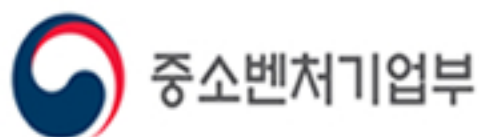


중소기업 기술보호 지침서



CONTENTS

제1장 개 요

제1절 기술보호 지침서의 목적	06
제2절 기술보호 지침서의 활용과 적용	07

제2장 중소기업 기술의 보호수준 자가진단

제1절 자가진단의 필요성	08
제2절 자가진단 항목	12
제3절 자가진단 분야별 관리사항	18

제3장 중소기업 기술의 유출방지 및 보호를 위한 관리와 운영

제1절 유출방지 및 보호 대상	24
제2절 기술유출 방지 및 보호를 위한 관리와 운영방안	26
1. 기술보호 정책	26
2. 주요 자산관리	28
3. 영업비밀 관리	30
4. 인적자원 관리	31
5. 기업의 시설관리	33
6. 정보시스템 관리	34
제3절 기술개발 및 기술거래 시 관리와 운영방안	35
1. 기술개발 형태에 따른 기술유출 방지 대책	35
2. 기술거래에 따른 기술유출 및 보호 관리방안	38

제4장 중소기업 기술의 유출 및 침해에 대한 대응과 복구

제1절 기술 유출 주체 및 유출 방법	42
1. 유출 주체	42
2. 유출 방법	43
3. 유출 경로	43
제2절 기술유출 대응 프로세스	44
1. 기술유출의 대응계획	44
2. 기술유출 대응 프로세스	45

제3절 기술 유출 및 침해의 유형별 사례와 대응방안	48
1. 인력유출을 통한 기술유출	48
2. 거래관계에서의 기술유출	51
3. 해외 기술유출	55
4. 경영정보 유출 및 전직금지 사례	56
제4절 판례를 통해 살펴 본 “기술보호 노력”의 의미와 정도	59
1. 기술보호 노력의 의미와 정도	59
2. 기술보호의 구체적 방법과 정도	60

제5장 중소기업의 기술인력에 대한 관리 및 보안 교육

제1절 내부 기술인력 관리 방안	68
1. 기술인력에 대한 관리의 필요성	68
2. 기술인력 채용 시 조치	69
3. 기술인력 실무상 조치	70
4. 퇴사 시 조치	73
5. 핵심 연구인력의 퇴사 후 관리	73
6. 기술인력 이직에 따른 분쟁 시 조치	74
제2절 프로젝트에 참여하는 기술인력 관리	77
1. 국가 R&D 사업참여 시 인력관리 및 보안조치	77
2. 공동개발 프로젝트 추진 시 인력관리 및 보안조치	78
3. 해외 진출기업 기술개발 시 인력관리 및 보안조치	78
4. IT 외주인력 보안 통제	81
제3절 기술인력 교육 운영방향	81
1. 기술보호 규정 제정 및 교육	82
2. 기술보호 우수자에 대한 조치	83
3. 기술보호 위반자에 대한 조치	84

제6장 중소기업의 기술보호 수칙 및 가이드

제1절 기술보호 핵심 수칙	85
제2절 관련 문헌 및 중소기업청 기술보호 지원제도	89
1. 기술보호 관련 법령	89
2. 중소기업기술보호 관련 지원제도	90

제1절

기술보호 지침서의 목적

중소기업에서 핵심기술은 중요한 자산이자 경쟁력과 생존의 원천이다. 국내 중소기업의 기술의존도가 점차로 높아지고 있는 반면 기술보호에 대한 인식이 부족하고 보안체계의 수립이 미흡하여 핵심기술의 유출이 계속해서 증가하고 있다.

또한 대기업 및 국내·외 다른 중소기업과의 기술계약을 적극적으로 추진하는 과정에서 불법적인 기술의 유출 및 침해행위가 끊임없이 발생하여 기업의 존립에 심각한 위협을 초래해왔다.

최근 우리 중소기업들의 해외진출이 증가하면서 내부 직원에 의한 그리고 해외 경쟁기업에 의한 불법적인 기술 유출 시도가 급증하고 있어 이에 대한 대책이 시급하다. 해외에 진출하는 경쟁력이 있는 중소기업의 경우에도 기술유출로 인한 피해가 심각한 것으로 나타났다.

불공정한 행위를 통한 중소기업의 기술유출을 차단하기 위해 관행과 법제도를 정비하는 정부의 역할도 중요하나 무엇보다도 중소기업이 스스로 기술유출을 차단하기 위한 노력을 하는 것이 중요하다. 거래상 우월적 지위에 있는 기업이 횡포를 부린다 하더라도 중소기업 스스로 기술보호에 대한 인식을 가지고 다양한 법제도를 활용하여 자구책을 갖춘다면 기술유출을 효과적으로 차단할 수 있으며 핵심기술을 기반으로 반드시 강소기업으로 성장해 갈 것이다.

중소기업청은 이에 중소기업기술보호를 지원하기 위한 기반을 확충하고, 중소기업이 보유한 기술을 보호하기 위해 2014년 5월 28일에 「중소기업기술 보호지원에 관한 법률」을 제정하였고, 동 법률 제8조에 따라 중소기업기술의 유출을 방지하고 보호하기 위하여 필요한 방법·절차 등에 관한 지침(이하 ‘기술보호지침’이라 한다)을 작성하게 되었다.

본 보호지침은 중소기업기술의 보호수준 자가진단, 중소기업 기술의 유출방지 및 보호를 위한 관리와 운영, 중소기업 기술의 유출 및 침해에 대한 대응과 복구, 기술인력에 대한 관리 및 보안교육 등에 대해 중소기업이 활용할 수 있는 방법과 절차 등을 제시함으로써 중소기업의 기술 보안에 대한 인식을 제고하고, 기술보호 역량을 강화하여 중소기업의 경쟁력을 확보하도록 하기 위해 마련되었다.

제2절

기술보호 지침서의 활용과 적용

본 중소기업 기술보호 지침서에서 다루고 있는 중소기업 기술의 유출방지 및 보호에 관한 방법과 절차 등은 매우 다양하며, 중소기업의 특성에 따라 적용할 수 있는 것과 적용할 수 없는 것이 있을 수 있다.

기술이 일단 유출되면 피해 복구가 쉽지 않은 만큼, 중요기술을 보유하고 있는 기업이라면 기술보호 수준 진단을 통해 취약점을 보완하여 기술 유출을 사전에 예방하는 것이 무엇보다 중요하다.

따라서 본 중소기업 기술보호 지침서는 중소기업 기술연구소를 포함하여 기술개발을 수행하는 중소기업을 대상으로 작성하였으나, 기술 보호지침을 활용하기 위해서는 각 중소기업의 고유한 특성을 고려하여 필요한 부분을 선택하여, 중소기업 기술 보호를 추진하여야 한다.

중소기업이 본 보호지침을 효과적으로 활용하기 위해서는 제2장 중소기업 기술의 보호수준 자가진단을 수행함과 동시에 제3장 제1절에 제시되어 있는 기술유출방지 및 보호 대상에서 규정한 자산의 분류방법에 따라 보유자산을 분류하고, 각 자산이 유출 또는 침해되었을 경우 경영에 가장 큰 피해를 주는 자산부터 우선순위를 정하여 유출방지 및 보호대책을 강구하여야 한다.

제3절 자가진단 분야별 관리사항은 자가진단을 통하여 중소기업에서 기술보호 지침을 제정할 수 있도록 연계를 하였으며, 부록에서 제공되는 각종 양식을 활용하여 기업의 특성에 맞게 가감할 수 있도록 배려하였다.

본격적인 자가진단을 수행하기 전에 약 20개의 사전설문을 통하여 중소기업의 기술보호 필요성과 중소기업 기술보호 지원제도의 빠른 이해를 돕고자 하였다.

제4장 중소기업 기술의 유출 및 침해에 대한 대응과 복구방법을 충분히 숙지하여 실행하는 것이 필요하다. 또한, 본 지침서 내에서 사용된 "정기적" 또는 "주기적"은 일정한 시기나 기간을 정해 시행함을 전제로 하나, 업체의 상황 또는 과정에 따라 달라지기에 기업의 기술보호지침에서 정리된 기간을 말한다.

제1절

자가진단의 필요성

중소기업 기술을 보호하기 위하여 각 중소기업에서 우선적으로 해야 할 일은 각 중소기업이 시행하는 중소기업 기술보호활동에 관한 상태 즉, 자신이 보유하고 있는 기술의 보호수준을 파악하는 것이다. 기술보호 자가진단을 위한 지표를 통해 중소기업이 기술보호 수준을 스스로 진단, 기술보호가 미흡한 분야를 찾아내고, 미흡한 분야들을 비교하여 우선순위에 따라 해당 조치를 할 수 있게 하는 데 그 중요성이 있다. 따라서 본 지침에서는 중소기업청에서 개발하고, 기술보호 자문 상담 시 사용하고 있는 자가진단을 중소기업의 수준에 맞게 재개정하여 자가진단 항목을 선정하고, 그에 따른 보호조치의 방법들을 제시하였다.

자가진단은 현재 중소기업청 기술보호 자문 상담 및 현장클리닉에서 사용하는 “보안수준 실태조사표”를 참조하여 중소기업의 보안에서 핵심적인 질문사항으로 조정하였으며, 이를 바탕으로 세부적인 자가진단을 실시할 수 있다.

세부적인 자가진단 서식은 6개 분야에 걸쳐 50개 문항으로 구성되어 있으며, 질문을 통해 진단이 필요한 사항이 무엇인지 알 수 있도록 설계되었다.

6개 분야 : 기술보호 정책, 주요 자산관리, 경영정보 관리, 인적자원 관리, 기업의 시설관리, 정보시스템 관리로 되어있다. 자가진단 결과는 기본적인 부분을 적절히 이행한 경우 70점 이상(우수, 양호)의 점수를 취득할 수 있도록 설계되었으며, 만일 진단결과 점수가 70점 미만(보통, 취약, 위험)이라면 미흡한 부분을 보완하여 70점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 한다.

또한 자가진단 결과 양호 이상의 기술보호 수준이라고 하더라도 기업의 보안 위험은 언제나 나타날 수 있으므로 전 영역에 걸쳐 기술보호가 이루어지도록 지속적 관리가 필요하다.

〈표 1-1〉 기술보호 수준

점 수	기술보호 수준
85점 이상	우수 수준 기술보호에 대한 결점 및 취약성이 거의 없으며, 기술의 유출 및 침해사고 발생 시 피해가 최소화되는 상태이다.
70점 이상~85점 미만	양호 수준 기술보호에 대해 심각하지 않은 결점 및 취약성을 내포하며, 회사 차원의 기술보호업무가 나름대로 이루어지고 있는 상태이다.
55점 이상~70점 미만	보통 수준 기술보호에 대해 일반적인 결점 및 취약성을 내포하며, 기술의 유출 및 침해정도에 따라 피해가 커질 수 있는 상태이다.
40점 이상~55점 미만	취약 수준 기술보호에 대해 다소 심각한 결점 및 취약성을 내포하며, 기술의 유출 및 침해정도에 따라 치명적인 피해를 가져올 수 있는 상태이다.
40점 미만	위험 수준 기술보호에 대해 심각한 결점 및 취약성이 상존하며, 기술의 유출 및 침해정도에 따라 치명적인 피해가 우려되는 상태이다.

사전 간이진단

항 목	질 문 내 용
1	귀사에는 외부로 유출되었을 때 피해가 예상되는 기술이나 경영상의 정보가 있습니까? <input type="checkbox"/> 있다 <input type="checkbox"/> 없다
2	내부 기밀정보의 외부유출에 대해 귀사가 대외적으로 느끼는 위협 정도는? <input type="checkbox"/> 매우 심함 <input type="checkbox"/> 약간 심함 <input type="checkbox"/> 보통 <input type="checkbox"/> 별로 없음 <input type="checkbox"/> 거의 없음
3	귀사의 내부 업무담당자가 기밀유출을 시도할 경우 성공가능성은 어느 정도입니까? <input type="checkbox"/> 큰 어려움 없이 유출 가능 <input type="checkbox"/> 계획수립시 성공가능성 높음 <input type="checkbox"/> 감독체계 강화로 적발가능성 높음 <input type="checkbox"/> 엄격한 보안체제로 원천적으로 불가능
4	귀사에는 내부의 중요정보를 보호하기 위한 자체 보안규정을 가지고 있습니까? <input type="checkbox"/> 있다 <input type="checkbox"/> 없다
5	귀사는 내부 기술정보 보호를 위해 직원대상교육을 실시한 적이 있습니까? <input type="checkbox"/> 있다 <input type="checkbox"/> 없다
6	귀사가 보유한 시설을 분리하고, 중요 정보자산이 위치한 시설에 대해 cctv등 출입통제시스템을 설치운영하고 있습니까? <input type="checkbox"/> 회사의 시설을 분류하고 중요자산이 위치한 시설에 대한 출입통제시스템을 운영하고 있다. <input type="checkbox"/> 회사의 시설을 분류 관리하고 있으나, 회사의 모든 시설에 임직원은 자유로이 출입할 수 있다. <input type="checkbox"/> 특별히 회사의 시설을 분류하지 않고 모든 임직원은 보유한 자산에 대한 접근이 자유롭다.
7	귀사는 직원 채용시 보안서약서를 징구하고 있습니까? <input type="checkbox"/> 입사시 징구 <input type="checkbox"/> 퇴사시 징구 <input type="checkbox"/> 입·퇴사시 모두 징구 <input type="checkbox"/> 징구하지 않음
8	기술유출 등 보안사고 발생 시 직원에 대한 공식적인 징계절차가 있습니까? <input type="checkbox"/> 징계절차가 마련되어 있으며, 필요시 징계조치가 이루어진다 <input type="checkbox"/> 징계절차는 마련되어 있으나, 징계조치는 거의 이루어지지 않는다 <input type="checkbox"/> 징계절차가 마련되어 있지 않다
9	퇴사자의 퇴사 후 진로 및 동향을 파악하고 있습니까? <input type="checkbox"/> 모든 퇴사자의 동향을 파악하고 있다 <input type="checkbox"/> 주요 임직원에 한하여 파악하고 있다 <input type="checkbox"/> 전혀 파악하고 있지 않다
10	귀사에는 협력업체, 방문객 등 외부인의 회사 내 출입절차가 존재합니까? <input type="checkbox"/> 출입절차가 존재하며, 출입관리대장을 기재한다 <input type="checkbox"/> 출입절차가 존재하지만, 출입관리대장은 기재하지 않는다 <input type="checkbox"/> 별도의 출입절차가 존재하지 않는다

항 목	질 문 내 용
11	기술유출 및 침해사고 발생시 회사 차원의 대응방안이 마련되어 있는가? <input type="checkbox"/> 마련되어 있다 <input type="checkbox"/> 마련되어 있지 않다
12	기술개발 시 법적 권리를 설정하고 있는가? <input type="checkbox"/> 특허권, 저작권, 실용신안 등의 권리를 설정하고 있다 <input type="checkbox"/> 어떻게 설정하는지 몰라 그냥 두고 있다
13	기술정보 유출사고 발생시 제일 먼저 도움을 요청해야겠다고 생각되는 기관은? <input type="checkbox"/> 정부기관(→ _____) <input type="checkbox"/> 모기업 또는 협력기업 <input type="checkbox"/> 법률회사/변호사 <input type="checkbox"/> 기타()
14	기술의 거래(기술계약)유형에 대한 위험요인을 알고 있는가? <input type="checkbox"/> 유형 및 위험요인을 잘 알고 있다. <input type="checkbox"/> 유형 및 위험요인에 대해 전혀 모르겠다.
15	국내 중소기업의 기술보호를 위해 정부차원에서 가장 우선적으로 추진해야할 사항은? (우선순위 2개 채택) <input type="checkbox"/> 중소기업 대상 기술보호 교육 <input type="checkbox"/> 법률자문 등 기업에 대한 소송지원 <input type="checkbox"/> 기술유출시 정부차원의 실사 <input type="checkbox"/> 현장방문 진단 및 보안상담 실시 <input type="checkbox"/> 보안시스템 구축 지원 <input type="checkbox"/> 기타()
16	USB, 플래시카메라 등 정보의 저장 가능한 매체에 대한 관리 및 통제를 하고 있는가? <input type="checkbox"/> 관리 및 통제를 하고 있다. <input type="checkbox"/> PC에서 정보의 저장이 가능한 매체에 자유로이 복사가 가능하다.
17	현재 운영중인 중소기업 기술보호 상담서비스의 필요성에 대하여 <input type="checkbox"/> 필요하다 <input type="checkbox"/> 필요치 않다 ※상담서비스 : 기업의 핵심 기술유출방지를 위한 애로사항을 지원하는 On/Off-Line 상담서비스로 현재 대중소기업협력재단에서 운영중
18	현재 운영 중인 중소기업 정보보안 관제서비스의 필요성에 대하여 <input type="checkbox"/> 필요하다 <input type="checkbox"/> 필요치 않다 ※관제서비스 : 기업이 운영하는 정보시스템을 대상으로 해킹, 기술유출 등에 대해 정부가 실시간 모니터링하고 침해사례 이력을 종합적으로 원격 관리하는 서비스로 현재 산업기술보호협회에서 운영 중
19	현재 운영 중인 중소기업 핵심 기술자료 임치서비스의 필요성에 대하여 <input type="checkbox"/> 필요하다 <input type="checkbox"/> 필요치 않다 ※기술자료 임치서비스 : 중소기업의 기술자료를 제3의 기관(임치센터)에 등록·보관함으로써 분쟁발생시 증빙자료로 활용하고, 임치기업의 도산/폐업시 협력기업의 기술사용을 보장하는 서비스로 현재 대중소기업협력재단에서 운영 중
20	현재 운영 중인 중소기업 기술분쟁 조정·중재제도의 필요성에 대하여 <input type="checkbox"/> 필요하다 <input type="checkbox"/> 필요치 않다 ※조정·중재제도 : 조정은 조정부의 도움을 받아 합의를 바탕으로 분쟁을 자율적으로 해결하는 제도이며, 중재는 중재절차에 대한 합의로 분쟁을 법원의 재판이 아닌 중재부의 판정으로 해결하는 구속력 있는 제도. 양 제도 모두 중소기업에 적합한 신속성, 저렴성, 전문성 등을 가지고 있으며 현재 대중소기업협력재단에서 운영 중

제2절

자가진단 항목 ¹⁾

1.기술보호 정책 (20점)

구분	진단 내용	평가
1.1	기술보호 규정을 보유하고 있는가? ① 보유하고 있다. (2점) ② 보유하고 있지 않다. (0점) ※기술보호 규정이란 기업별 특성에 맞는 기술정보 보호 및 운영에 관한 보안규정을 말하며, ‘보안정책서’ 또는 ‘보안지침서’ 등에 표현된 규칙 등을 말함	
1.2	회사의 기술보호 정책, 지침, 절차 등의 내용에 대해 임직원들에게 공지하고 있는가? ① 공지하고 있다. (2점) ② 공지하고 있지 않다. (0점)	
1.3	기술보호를 위한 전담조직이 존재하는가? ① 보안전담조직과 기술보호 담당자가 존재한다. (2점) ② 보안담당자만 존재한다. (1점) ③ 보안전담조직과 담당자 모두 존재하지 않는다. (0점)	
1.4	회사의 주요 정보(기술, 영업 등)는 어떻게 공유되는가? ① 업무담당자, 관계자 등 소수만이 볼 수 있다. (2점) ② 핵심정보를 제외하고는 직원들이 볼 수 있다. (1점) ③ 대부분의 정보에 대해서 직원들이 볼 수 있다. (0점)	
1.5	임직원의 업무에 기밀사항의 보호 등 기술보호관련 내용이 포함되어 있는가? ① 포함되어 있다. (2점) ② 포함되어 있지 않다. (0점)	
1.6	회사 내 기술보호업무 수행을 위해 팀(혹은 그룹)간 업무 공조체계가 갖추어져 있는가? ① 갖추어져 있다. (2점) ② 갖추어져 있지 않다. (0점)	
1.7	1년에 1회 기술보호를 위한 보안감사를 실시하고 있는가? ① 실시하고 있다. (2점) ② 필요할 때 실시하고 있다. (1점) ③ 실시하지 않고 있다. (0점)	
1.8	회사가 보유한 주요 정보 및 자산을 보호하기 위해 투자하는 비용수준은 어떠한가? ① 기술적, 물리적, 관리적 기술보호를 위해 매년 일정비용 이상을 꾸준히 투자하고 있다. (2점) ② 특정 기술보호분야에 대해 필요시 비용투자가 이루어지고 있다. (1점) ③ 기술보호분야에 대한 투자가 이루어지고 있지 않다. (0점)	
1.9	기술보호업무 추진을 위해 외부 전담기관의 도움을 받고 있는가? ① 도움을 받고 있다. (2점) ② 도움을 받고 있지 않다. (0점)	
1.10	기술유출 및 침해사고 발생시 회사 차원의 대응방안이 마련되어 있는가? ① 구체적으로 마련되어 있다. (2점) ② 일정부분에 한해서만 마련되어 있다. (1점) ③ 마련되어 있지 않다. (0점)	

※진단결과 점수가 10점 미만이라면 미흡한 부분을 보완하여 10점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함.

1) 자가진단 분야별 관리사항은 본 지침서 18쪽~23쪽 참고.

2. 주요 자산관리 (10점)

구분	진단 내용	평가
2.1	회사가 보유한 주요자산에 대해 자산의 분류 및 평가를 실시하고 있는가? ① 그렇다. (2점) ② 그렇지 않다. (0점)	
2.2	회사의 자산 또는 문서에 대해 등급설정 및 표시를 하고 있는가? ① 자산의 중요도에 따라 등급을 표시하고 있다. (2점) ② 등급은 설정되어 있으나 표시는 하지 않는다. (1점) ③ 등급/표시를 사용하지 않는다. (0점)	
2.3	분류된 자산은 책임자를 선정하여 관리하고 있는가? ① 자산별 책임자를 임명하여 관리하고 있다. (2점) ② 부서에만 책임을 지게하고 있다. (1점) ③ 자산 책임자는 없다. (0점)	
2.4	회사의 자산 분류는 정기적으로 이루어지는가? ① 정기적으로 이루어진다. (2점) ② 필요시 이루어진다. (1점) ③ 이루어지지 않고 있다. (0점)	
2.5	특허, 실용신안, 디자인 등 지식재산권과 기술 관련 자료(영업비밀)에 대한 권리는 어떤 형태로 설정되어 있는가? ① 모두 권리 설정이 되어 있다. (2점) ② 일부만 권리 설정이 되어 있다. (1점) ③ 출력문서로 존재하며 권리 설정이 되어 있지 않다. (0점)	

※진단결과 점수가 5점 미만이라면 미흡한 부분을 보완하여 5점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함.

3. 영업비밀 관리 (14점)

구분	진단 내용	평가
3.1	내부에서 생성된 중요 기술상/경영상 영업비밀 자료는 관리번호를 부여하여 관리하는가? ① 그렇다. (2점) ② 그렇지 않다. (0점)	
3.2	내부에서 생성된 중요 기술상/경영상 영업비밀 자료의 보관은 다른 문서와 구별하여 보관하는가? ① 중요 정보와 그 기록매체는 다른 문서와 구별하여 보관함에 보관하거나 접근제한 조치된 정보시스템에 보관한다. (2점) ② 일반문서와 구별하여 보관하지만 시간장치 없는 서랍에 보관하는 등 보관상태가 취약하다. (1점) ③ 회사 내 일반문서와 함께 보관하고 있다. (0점)	
3.3	임직원의 주요 기술상/경영상 영업비밀 관련 정보시스템 및 서비스에 대한 접근은 어떻게 하고 있는가? ① 사용자등록 절차를 통한 정당한 사용자 및 한정된 자원만 접근이 가능하다. (2점) ② 사원으로 등록된 사용자는 회사의 회계시스템만 제외하고 모든 정보시스템 접근이 가능하다. (1점) ③ 사원으로 등록된 사용자는 회사의 모든 정보시스템에 접근이 가능하다. (0점)	

3. 영업비밀 관리 (14점)

구분	진단 내용	평가
3.4	중요 기술상/경영상 영업비밀 관련 정보시스템에 보관된 자료는 어떻게 관리되고 있는가? ① 권한별, 직군별 등으로 접근이 제어되어 있다. (2점) ② 사내 시스템에 접근 가능하면 자료 대부분을 볼 수 있다. (1점) ③ 모든 자료는 언제든지 접근이 가능하다. (0점)	
3.5	기술정보를 보호하기 위하여 기술자료 임치, 관제서비스 등 보호제도를 활용하고 있는가? ① 활용하고 있다. (2점) ② 어떻게 설정하는지 몰라 그냥 두고 있다. (0점)	
3.6	기술의 거래(기술계약)유형에 대한 위험요인을 알고 있는가? ① 유형 및 위험요인을 잘 알고 있다. (2점) ② 유형 및 위험요인에 대해 어느 정도는 알고 있다. (1점) ③ 유형 및 위험요인에 대해 전혀 모르겠다. (0점)	
3.7	회사의 정보자산에 대한 사용자(임직원, 계약자, 제3의 사용자 등)들의 접근 권한은 퇴사, 계약종료, 역할 조정 등의 사유발생시 조정되고 있는가? ① 사유발생 즉시 조정되어진다. (2점) ② 사유발생 1주일 이내에 조정되어진다. (1점) ③ 조정이 지연되거나 이루어지지 않는다. (0점)	

※진단결과 점수가 7점 미만이라면 미흡한 부분을 보완하여 7점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함.

4. 인적자원 관리 (22점)

구분	진단 내용	평가
4.1	임직원 및 신규 입사자를 대상으로 기술보호교육을 실시하고 있는가? ① 1년에 1회 실시하고 있다. (2점) ② 필요시에만 실시하고 있다. (1점) ③ 실시하고 있지 않다. (0점)	
4.2	'직무발명보상제도'를 운영하고 있는가? ① 실시하고 있다. (2점) ② 실시하고 있지 않다. (0점)	
4.3	신규 입사자에 대해 비밀유지서약서를 받고 있는가? ① 보안서약서를 근로계약서와 별도로 받고 있다. (2점) ② 별도로 비밀유지서약서를 받고 있지는 않지만, 고용계약서에 보안책임을 명시하고 있다. (1점) ③ 받고 있지 않다. (0점)	

구분	진단 내용	평가
4.4	<p>임직원 기술보호의식을 제고하기 위해 '개인보안 지침'을 제정하고, PC 화면보호기 설정하고 있는가?</p> <p>① 개인보안 지침을 제정하고 있으며 PC화면보호기를 설정하고 있다. (2점) ② 개인보안 지침은 없으나, PC화면보호기를 설정하도록 한다. (1점) ③ 개인보안에 대한 교육 및 PC화면보호기 설정에 대한 내용이 없다. (0점)</p>	
4.5	<p>주요 R&D 프로젝트 참가 인력에 대해 비밀유지서약서를 받고 있는가?</p> <p>① 받고 있다. (2점) ② 받지 않고 있다. (0점)</p>	
4.6	<p>임직원이 기업의 기술보호 규정 등을 위반하는 경우 임직원에 대한 공식적인 징계 절차가 마련되어 있는가?</p> <p>① 징계절차가 마련되어 있으며, 필요시 징계조치가 이루어진다. (2점) ② 징계절차는 마련되어 있으나, 징계조치는 거의 이루어지지 않는다. (1점) ③ 징계절차가 마련되어 있지 않다. (0점)</p>	
4.7	<p>퇴직자에 대해 회사 정보자산의 유출방지를 위한 비밀유지서약서를 징구하고 있는가?</p> <p>① 징구하고 있다. (2점) ② 징구하고 있지 않다. (0점)</p>	
4.8	<p>퇴직자의 향후 진로 및 동향을 파악하고 있는가?</p> <p>① 모든 퇴직자의 동향을 파악하고 있다. (2점) ② 주요 임직원에 한하여 파악하고 있다. (1점) ③ 전혀 파악하고 있지 않다. (0점)</p>	
4.9	<p>제3자(외주업체, 협력업체, 외국인 등)에 대한 관리를 하고 있는가?</p> <p>① 별도의 관리방안이 마련되어 있으며, 대상자에 대한 비밀유지서약을 하고 있다. (2점) ② 별도의 관리방안은 마련되어 있지 않으나, 대상자에 대한 비밀유지서약은 하고 있다. (1점) ③ 별도의 관리방안이 마련되어 있지 않으며, 대상자에 대한 비밀유지서약도 하고 있지 않다. (0점)</p>	
4.10	<p>외부인 식별을 위하여 임직원의 사원 증 패용을 의무화하고 있는가?</p> <p>① 의무화 하고 있다. (2점) ② 의무화 하고 있지 않다. (0점)</p>	
4.11	<p>업무를 위한 아웃소싱 규정이 수립되어 있는가?</p> <p>① 규정이 수립되어 있고 준수하고 있다. (2점) ② 규정이 없다. (0점)</p>	

※진단결과 점수가 총점수 22점의 50% = 11점 미만이라면 미흡한 부분을 보완하여 11점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함.

5. 기업의 시설관리 (14점)

구분	진단 내용	평가
5.1	회사 내 중요시설에 대한 관리기준이 있는가? ① 관리기준이 존재한다. (2점) ② 관리기준이 존재하지 않는다. (0점)	
5.2	협력업체, 방문객 등 외부인의 회사 내 출입절차가 존재하는가? ① 출입절차가 존재하며, 출입관리대장을 기재한다. (2점) ② 출입절차가 존재하지만, 출입관리대장은 기재하지 않는다. (1점) ③ 별도의 출입절차가 존재하지 않는다. (0점)	
5.3	회사 내 중요시설에 대해 출입통제시스템을 설치하여 운영하고 있는가? ① 출입통제시스템을 운영하고 있으며, 내부의 한정된 인원만 출입이 가능하다. (2점) ② 출입통제시스템을 운영하고 있으며, 내부 인원은 자유로이 출입이 가능하다. (1점) ③ 출입통제시스템을 운영하고 있지 않으며, 내·외부 인원의 자유로운 출입이 가능하다. (0점)	
5.4	건물 출입구나 중요시설에 대해 CCTV 등의 감시 장치가 설치되어 있는가? ① 설치되어 있다. (2점) ② 설치되어 있지 않다. (0점)	
5.5	중요시설 및 통제구역에 대해 화재, 전원, 수해 등으로부터의 보호방안이 강구되어 있는가? ① 보호방안이 강구되어 있다. (2점) ② 보호방안이 강구되어 있지 않다. (0점)	
5.6	장비, 정보 또는 소프트웨어 등의 회사 자산의 반출은 어떤 식으로 이루어지는가? ① 사전 인가가 있어야만 반출이 가능하다. (2점) ② 사전 인가 없이도 반출이 가능하다. (0점)	
5.7	회사 내 중요시설에 카메라, 비디오카메라 등의 장비반입이 규정에 의해 통제되고 있는가? ① 규정에 의해 통제되고 있다. (2점) ② 규정에 의해 통제되고 있지 않다. (0점)	

※진단결과 점수가 7점 미만이라면 미흡한 부분을 보완하여 7점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함.

6. 정보시스템 관리 (20점)

구분	진단 내용	평가
6.1	<p>서버 및 DB 현황에 대한 보안점검을 실시하고 있는가?</p> <p>① 6개월에 1회 주기로 보안 상태에 대해 점검하고 있다. (2점) ② 필요가 있을 때만 실시하고 있다. (1점) ③ 보안점검을 실시하고 있지 않다. (0점)</p>	
6.2	<p>바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위한 대책을 강구하고 있는가?</p> <p>① 각종 보안솔루션을 도입하여 사용하고 있다. (2점) ② 일부 보안솔루션을 도입하여 사용하고 있다. (1점) ③ 보안솔루션 도입은 아직 이루어지고 있지 않다. (0점)</p>	
6.3	<p>내부에서 생성된 주요 정보 및 소프트웨어는 백업되어 관리되고 있는가?</p> <p>① 3개월 1회 주기로 백업하여 관리하고 있다. (2점) ② 필요시에만 백업하여 관리하고 있다. (1점) ③ 백업하여 관리하고 있지 않다. (0점)</p>	
6.4	<p>USB, 플래시카메라 등 정보의 저장에 가능한 매체에 대한 관리절차가 마련되어 있는가?</p> <p>① 관리절차가 마련되어 있다. (2점) ② 관리절차가 마련되어 있지 않다. (0점)</p>	
6.5	<p>이메일의 첨부문서에 대한 통제를 실시하고 있는가?</p> <p>① 이메일의 첨부문서는 문서 통제규정을 활용하여 발송하도록 하고 있다. (2점) ② 외부로 발송은 통제하고 있으나 회사 내부로 발송은 전혀 통제하고 있지 않다. (1점) ③ 전자문서 발송에 대한 통제가 존재하지 않는다. (0점)</p>	
6.6	<p>PC 및 주요 시스템 사용자에게 대한 패스워드 관리를 하고 있는가?</p> <p>① 3개월 주기로 패스워드를 변경하고 있으며, 이를 1개월마다 점검한다. (2점) ② 필요시에만 패스워드를 변경하고 관리하고 있다. (1점) ③ 패스워드 관리를 하지 않고 있다. (0점)</p>	
6.7	<p>서버 및 데이터베이스 로그인 계정관리 기준을 정의하고, 접근통제를 실시하고 있는가?</p> <p>① 시스템별 로그인 계정관리 기준을 정의하고, 접근통제를 실시한다. (2점) ② 계정관리 없이 임직원은 서버 및 데이터베이스 접근 가능하다. (0점)</p>	
6.8	<p>기업 내부에서 사용하는 인터넷망은 외부의 침입으로부터 안전한가?</p> <p>① 내부 및 외부 인터넷으로 구분되어 있고 내부인터넷 접근 시 별도의 인증이 필요하다. (2점) ② 내부 인터넷 망 접근 시 별도의 인증 없이 사용할 수 있다. (0점)</p>	
6.9	<p>주요 장애 발생 시 장애내용이 보고되어 신속하게 시정조치가 이루어지는가?</p> <p>① 장애내용이 보고되어 신속한 시정조치가 이루어진다. (2점) ② 장애내용의 보고 누락 또는 시정조치가 다소 지연되는 경향이 있다. (1점) ③ 장애내용이 누락되며, 시정조치가 지연되는 경향이 있다. (0점)</p>	
6.10	<p>정보자산의 침해발생 등 비상시 따라야 할 절차와 관련자의 책임이 규정되어 있는가?</p> <p>① 침해사고 대응팀과 비상연락체계가 마련되어 있다. (2점) ② 침해사고 대응팀은 없으나 비상연락체계가 마련되어 있다. (1점) ③ 침해사고 대응팀 및 비상연락체계가 없다. (0점)</p>	

※진단결과 점수가 10점 미만이라면 미흡한 부분을 보완하여 10점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함.

제3절

자가진단 분야별 관리사항

1. 기술보호 정책

- 1.1. 중소기업은 ‘기술보호정책서’를 참조하여 기업별 특성에 맞는 기술보호에 관한 규정을 제정하여야 한다.
- 1.2. 제정된 기술보호규정을 정리한 ‘기술보호정책서’, ‘기술보호지침서’ 등은 임직원들에게 공지하고, 주기적으로 제·개정하며, 정당한 절차에 의해 모든 임직원에게 공지하여 그 효력이 발휘될 수 있도록 하여야 한다.
- 1.3. 기업의 기술보호 담당자(보안 책임자)를 지정하여야 하며, 중소기업의 규모 및 특성에 따라 ‘기술보호 조직 지침’에 따른 전담조직을 둘 수 있다.
- 1.4. 회사의 주요 정보(기술, 경영 등)는 ‘접근통제지침’에 따라 업무담당자, 관계자 등 소수만이 볼 수 있도록 해야 한다.
- 1.5. 임직원 업무에 기밀사항의 보호 등 보안관련 내용이 포함될 경우 ‘자산분류지침’에 따라 분류하고 정보 자산의 접근 권한을 제한해야 한다.
- 1.6. 중소기업 내 기술보호업무 수행을 위해 팀(혹은 그룹)간 업무 공조체계가 내부에서 제정된 기술보호 규정에 근거한 ‘기술보호조직지침’에 따라 구성되어야 한다.
- 1.7. 중소기업은 내부적으로 제정된 기술보호규정에 근거한 ‘기술보호감사지침’을 고려하여 정기적으로 내부 보안감사를 실시하여야 한다.
- 1.8. 중소기업이 보유한 주요 정보 및 자산을 보호하기 위해 기술적, 물리적, 관리적인 기술보호에 대한 확보 노력과 일정 비용의 지속적인 투자가 필요하다.

- 1.9. 기술보호업무 추진을 위해 별도로 지정된 조연자가 없을 경우 기술보호 담당자는 보안에 관한 조언을 제공해야하며, 기술보호의 특정분야에 대한 조언이나 도움이 필요한 경우 외부 전문가의 도움을 받도록 한다.
- 1.10. 기술유출 및 침해사고 발생시 기업에 제정된 기술보호규정에 근거한 ‘침해사고 대응 지침’의 침해사고 대응방안에 따라 회사 차원의 대응방안이 마련되어야 한다.

2. 주요 자산관리

- 2.1. 기업이 보유한 자산에 대해 제시된 ‘자산분류 및 평가’와 자산관리지침에 따라 기업의 자산분류 및 관리기준을 수립하여야 한다.
- 2.2. 기업의 자산 또는 문서에 대해 ‘자산관리 지침’의 자산 평가 기준을 고려하여 등급설정 및 표시를 하여야 한다.
- 2.3. 분류된 자산은 소유자(책임자)를 선정하여 ‘자산분류지침’에 따라 관리하여야 하며, 담당자(정보보호 담당자)와 사용자를 지정할 수 있다.
- 2.4. 기업의 자산 분류는 ‘자산관리 지침’에 따라 정기적으로 재분류하여야 한다.
- 2.5. 특허, 실용신안, 디자인 등 지식재산권과 기술 관련 자료는 ‘자산관리 지침’에 따라 모두 권한을 설정하여 관리하여야 한다.

3. 영업비밀 관리

- 3.1. 내부에서 생성된 중요 정보 및 자료 등은 ‘자산 분류 지침’의 정보자산 관리에 따라 관리번호를 부여하여 관리하여야 한다.
- 3.2. 내부에서 생성된 중요 정보 및 자료의 보관은 ‘자산 분류 지침’의 자산의 등록에 따라 다른 문서와 구별하여 보관하여야 한다.

- 3.3. 임직원의 주요 정보시스템 및 서비스에 대한 접근은 접근 권한은 ‘접근통제 지침’의 사용자 접근 관리에 따라 사용자등록 절차를 통한 정당한 사용자 및 한정된 자원만 접근할 수 있어야 한다.
- 3.4. 정보시스템에 보관된 자료는 ‘정보자산 보안관리 지침’상의 서버관리, 전산자료 및 데이터베이스 관리에 따라 권한별, 직군별 등으로 접근이 제한되어야 한다.
- 3.5. 내부 및 외부에 의한 핵심기술 유출을 방지하기 위하여 기술자료 임치제도, 보안관제서비스 등을 활용한다.
- 3.6. 기술의 거래(기술계약)유형을 이해하고 기업에서 수행하는 기술거래에 따른 기술유출 방지 대책을 마련하여야 한다.
- 3.7. 중소기업의 정보자산에 대한 임직원, 계약자, 제3의 사용자 등의 접근 권한은 ‘접근 통제 지침’에 따라 퇴사, 계약종료, 역할 조정 등의 사유발생시 즉시 조정되어야 한다.

4. 인적자원 관리

- 4.1. 중소기업은 ‘기술보호 교육 수행 지침’에 따라 임직원 및 신규 입사자에 대해 기술보호교육을 실시하여야 한다.
- 4.2. 중소기업은 내부직원에 의한 기술유출을 방지하고 기술개발을 증진시키기 위하여 ‘직무발명보상제도’를 실시하여야 한다.
- 4.3. 임직원의 기술보호의식을 제고하기 위해 ‘개인보안 지침’을 제정하고, 장시간 자리가탈시 화면보호기 설정 및 퇴근 시 사용된 노트북 반납, 출입문, 캐비닛, 개인서랍의 시건 확인, 문서 및 도면의 정돈 등을 확인해야 한다.
- 4.4. 중소기업은 ‘인적 관리 지침’에 따라 신규 입사자에 대해 비밀유지서약서를 받아야 한다.
- 4.5. 중소기업은 ‘인적 관리 지침’에 따라 주요 R&D 프로젝트 참가자에 대해 비밀유지서약서를 받아야 한다.

- 4.6. 중소기업의 임직원이 보안정책, 지침, 절차 등을 위반하는 경우 중소기업의 보안규정에 근거한 ‘보안 위반자처리 지침’에 따라 직원에 대한 공식적인 징계 절차를 마련하여 징계조치가 이루어져야 한다.
- 4.7. 중소기업은 ‘인적자원 관리 지침’에 따라 퇴직자에 대해 회사 정보자산의 유출방지를 위한 비밀유지서약서 징구 및 일정기간 동종업계에서 일하는 것을 제한하도록 하여야 한다.
- 4.8. 중소기업은 ‘인적 관리 지침’에 따라 퇴직자의 향후 진로 및 동향을 파악하고 있어야 한다.
- 4.9. 제3자(협력업체, 외국인 등)의 업무참여시 별도의 권한관리 방안을 ‘접근통제 지침’에서 마련하고 관련사항을 대상자로부터 비밀유지서약서를 받아야 한다.
- 4.10. 외부인 식별을 위하여 ‘인적 자원 관리 지침’에 따라 임직원의 사원증 패용을 의무화해야 한다.
- 4.11. 업무를 위한 아웃소싱을 제3자와 체결할 경우 관련 규정이 ‘정보자산 보안관리 지침’의 운영아웃소싱 관리에 따라 수립해야하고 준수되어야 한다.

5. 기업의 시설관리

- 5.1. 중소기업 내 중요시설에 대해 ‘자산분류 지침’의 주요시설 관리기준에 따라 분류해야 한다.
- 5.2. 협력업체, 방문객 등 외부인의 회사 내 출입 시 ‘자산분류 지침’의 구역별 보호대책에 따라 출입관리대장에 기재 후 출입절차에 따라 안내해야 한다.
- 5.3. 중소기업 내 중요시설에 대해 ‘자산분류 지침’의 시설물 보안대책에 따라 출입통제시스템을 운영하고 허용된 인원만 출입하여야 한다.
- 5.4. 중소기업 내 중요시설에 대해 ‘자산분류 지침’의 구역별 보호대책에 따라 건물 출입구나 중요시설에 대해 CCTV 등의 감시 장치가 설치되어야 한다.

- 5.5. 중소기업 내 중요시설 및 통제구역에 대해 ‘자산분류 지침’의 전산시설 보안대책에 따라 화재, 전원, 수해 등으로부터의 보호방안이 강구되어야 한다.
- 5.6. 장비, 정보 또는 소프트웨어 등의 회사 자산의 반출은 ‘개인보안 지침’의 임직원의 임무에 따라 장비반출신청서를 작성하여 부서장의 승인을 얻어야 한다.
- 5.7. 중소기업 내 중요시설에 휴대폰, 카메라, 비디오카메라 등의 장비를 반입할 경우 ‘자산분류 지침’의 구역별 보호대책에 따라 반입이 통제되어야 한다.

6. 정보시스템 관리

- 6.1. 서버 및 DB 현황에 대하여 ‘정보자산 보안관리 지침’의 서버관리, 전산자료 및 데이터베이스 관리에 따라 6개월에 1회 주기로 보안점검을 실시하여야 한다.
- 6.2. 바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위해 ‘정보자산 보안관리 지침’의 PC관리에 따라 각종 보안솔루션을 도입하여 사용하여야 한다.
- 6.3. 내부에서 생성된 주요 정보 및 소프트웨어는 ‘정보자산 보안관리 지침’의 백업관리에 의해 정기적으로 백업하여 관리하여야 한다.
- 6.4. CD, USB, 플래쉬 카메라 등 정보의 저장이 가능한 매체에 대해서는 중소기업에서 제정된 보안규정에 근거한 ‘정보자산 보안관리 지침’의 보조기억매체의 관리에 따라 관리절차가 마련되어야 한다.
- 6.5. 이메일에 대한 통제는 중소기업 내부에서 제정된 ‘개인보안 지침’의 전자메일(이메일) 사용에 따라 모든 메일은 문서 통제방안을 활용하여 발송하도록 통제되어야 한다.
- 6.6. PC 및 주요 시스템 사용자에 대한 패스워드 관리는 중소기업 내부에서 제정된 보안규정에 근거한 ‘개인보안 지침’의 패스워드관리 및 업무용 PC의 사용에 따라 3개월 주기로 패스워드를 변경하고, 이를 1개월단위로 점검해야 한다.

- 6.7. 서버 및 데이터베이스 로그인 계정관리를 ‘정보자산 보안관리 지침’의 서버관리, 전산자료 및 데이터베이스 관리와 ‘인적관리 지침’의 사용자 계정관리에 따라 시스템별 로그인 계정관리 기준을 정의하고, 접근통제를 실시해야한다.
- 6.8. 내부 인터넷망과 외부 인터넷망은 ‘정보자산 보안관리 지침’의 인터넷 망 분리기준에 의거해 운영하여야 한다.
- 6.9. 주요 장애 발생 시 ‘정보자산 보안관리 지침’의 장애관리에 따라 장애내용이 보고되고 신속하게 시정조치가 이루어져야 한다.
- 6.10. 정보자산의 침해발생 등 비상시 따라야 할 절차와 관련자의 책임이 ‘침해사고 대응 지침’의 침해사고 대응 및 복구에 따라 침해사고 대응팀과 비상연락체계가 마련되어야 한다.

제1절

유출방지 및 보호 대상

중소기업이 보유하고 있는 기술의 유출을 방지하고 보호하려는 경우 구체적으로 무엇을 보호해야 하는지 판단하는 것은 어려운 일이다. 기술은 추상적인 개념이며, 그 기술을 담고 있는 형태가 대상기관별로 다양하기 때문에 하나로 규정짓기 어렵다고 할 수 있다. 따라서 구체적으로 무엇을 보호해야 하는지 그 대상을 규정하는 것이 매우 중요하다.

1. 기술보호 관련 법령에 따른 보호대상

기술보호와 관련한 법률은 <표 3-1>에서처럼 현재 총 5가지 종류로 나누어지며, 각 법률에서 규정하고 있는 보호대상을 명확히 이해할 필요가 있다.

<표 3-1> 법률별 보호대상

법률명	보호대상
중소기업기술보호 지원에 관한 법률	중소기업기술 : 중소기업 및 『중소기업 기술혁신 촉진법』 제2조제2호에 따른 중소기업자가 직접 생산하거나 생산할 예정인 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 독립된 경제적 가치를 가지는 기술 또는 경영상의 정보(법 제2조제2호)
부정경쟁방지 및 영업비밀 보호에 관한 법률	영업비밀 : 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 합리적인 노력에 의하여 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보(법 제2조 제2호)
산업기술의 유출방지 및 보호에 관한 법률	산업기술 : 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계중앙행정기관의 장이 지정, 고시, 공고하는 기술로서 제2조제1호 각 목에 해당하는 기술(법 제2조 제1호) 가. 제9조에 따라 고시된 국가핵심기술 나. 「산업발전법」 제5조에 따라 고시된 첨단기술의 범위에 속하는 기술 다. 「산업기술혁신 촉진법」 제15조의2에 따라 인증된 신기술 라. 「전력기술관리법」 제6조의2에 따라 지정·고시된 새로운 전력기술 마. 「환경기술 및 환경산업 지원법」 제7조에 따라 인증된 신기술 바. 「건설기술 진흥법」 제14조에 따라 지정·고시된 새로운 건설기술 사. 「보건의료기술 진흥법」 제8조에 따라 인증된 보건신기술 아. 「뿌리산업 진흥과 첨단화에 관한 법률」 제14조에 따라 지정된 핵심 뿌리기술 자. 그 밖의 법률 또는 해당 법률에서 위임한 명령에 따라 지정·고시·공고·인증하는 기술 중 산업통상자원부장관이 관보에 고시하는 기술

2) 중소기업 기술보호 매뉴얼, 중소기업청, 2013

3) 보안컨설팅트용 실무 가이드북, 중소기업청, 2007

법률명	보호대상
대·중소기업 상생협력 촉진에 관한 법률	기술자료 : 물품 등의 제조 방법, 생산 방법, 그 밖에 영업활동에 유용하고 독립된 경제적 가치가 있는 것으로, 다음에 해당하는 자료(법 제2조 제9호) ① 특허권, 실용신안권, 디자인권, 저작권 등의 지식재산권과 관련된 정보 ② 제조·생산방법과 판매방법 등 그 밖의 영업활동에 유용한 기술상 또는 경영상의 정보(시행령 제1조의2)
하도급거래 공정화에 관한 법률	기술자료 : 상당한 노력에 의하여 비밀로 유지된 제조·수리 시공 또는 용역수행 방법에 관한 자료, 그 밖에 영업활동에 유용하고 독립된 경제적 가치를 가지는 것 (법 제2조 제15항) ① 특허권, 실용신안권, 디자인권, 저작권 등의 지식재산권과 관련된 정보 ② 그 밖에 영업활동에 유용하고, 독립된 경제적 가치가 있는 기술상 또는 경영상의 정보(시행령 제2조제8항)

2. 기술보호 대상의 유형

중소기업이 경쟁사가 알지 못하는 유용한 기술을 개발한 경우 특허(실용신안) 또는 영업비밀로 보호할 수 있다. 영업비밀의 경우 기술상의 정보뿐만 아니라 경영상의 정보도 보호한다.

(1) 특허

기업은 기술개발을 했을 때 특허(실용신안)로 보호받을지 아니면 영업비밀로 보호받을지를 결정하여야 한다. 먼저 특허가 되기 위해서는 개발한 기술이 새롭고 진보한 기술이어야 하며, 자신의 기술을 설명한 출원서를 특허청에 제출하여 일정한 심사를 거친 후 등록을 받아야 보호받을 수 있다. 특허등록이 되면 독점배타적 권리인 특허권을 받는 대신 기술이 공개되며 20년간 보호받게 된다. 특허는 외부로 공개가 되므로 기업평가를 향상시키고 홍보에 기여할 수 있다.

(2) 영업비밀

경제적 가치를 가지는 유용한 기술은 영업비밀로 보호받을 수 있다. 특허와 달리 출원절차가 없으며 기업 스스로 합리적인 노력으로 기술정보를 비밀로 유지해야 한다. 이러한 측면에서 영업비밀에 대한 권리는 특허와 달리 독점배타적 권리가 아니며, 다만 부정한 방법으로 영업비밀을 유출하는 행위를 규제하고 있다. 따라서 경쟁사가 스스로 연구개발을 통하여 자사와 동일한 기술을 개발하였다면 사실상 두 개의 동일한 기술이 합법적으로 비밀상태로 존재하게 된다.

영업비밀은 특허와 달리 보호기간에 제한이 없다. 앞서 설명한 기술보호정책 및 자산관리와, 이하에서 상술하는 인력관리, 시설관리, 정보시스템 관리 등은 모두 합리적 노력과 관련된 일들이다.

한편, 영업비밀은 특허와 달리 기술정보 외에도 경영상의 정보를 보호한다. 경영상 정보는 고객 명부, 시장조사정보, M&A 계획, 기타 기업 관리 정보 등을 포함된다.

제2절

기술유출 방지 및 보호를 위한 관리와 운영방안

1. 기술보호 정책

기술보호 구성단계 중 하나로서 회사의 기술보호 및 운영에 대해 기본정책을 수립해 임직원(협력사 포함한다.) 및 기업이 대내외적 경영활동을 할 때 회사의 핵심자산을 관리하고 기업정보를 체계적으로 보호하는 활동이다.

(1) 필요성

- 기술보호 담당자가 기술보호와 관련된 모든 것들에 대해 어떻게 관리할 것인가를 결정하고 사용자에게 준수하여야 할 사항을 알리기 위함이다.

(2) 분류

① 기술보호조직 정책

- 조직 안에 기술보호를 추진하고 통제하는 경영관리 틀

② 정보자산관리 정책

- 정보시스템 관련 자산들에 대한 책임자를 명시하고, 비밀의 정도에 따라 적절한 등급으로 분류하여 취급

③ 인력관리 정책

- 임직원, 연구·개발부서의 직원, 외부 업체 관련자 등에 의한 기술보호 및 유출 방지 정책 수립

④ 물리 및 환경적 보안 정책

- 정보와 정보처리 시설에 대한 불법적인 물리적 접근과 시설의 파손을 막기 위한 환경적 통제 제시

⑤ 기술적 보안 정책

- 중요 기술 데이터는 삭제나 변조를 대비하여 주기적 백업, 불필요한 서비스 중단, 백신, 방화벽 등 기본적인 보안프로그램 설치 및 운용

⑥ 기술보호 운영관리 및 사고대응 정책

- 운영 절차와 책임, 시스템 운영, 네트워크 운영 및 문서관리, 악성 소프트웨어 통제, 원격 작업, 대응계획 및 체계, 복구, 사후관리

⑦ 기술보호 교육 수행 정책

- 임직원에 대한 기술보호교육, 인사 고과, 감사 등 정책

(3) 세부규정 제정 및 수립

- ① 중소기업이 보유하고 있는 기술을 보호하기 위해 필요한 것 가운데 가장 기본이 되는 것이 바로 ‘중소기업 기술보호 세부규정’(이하 규정이라 한다.)이다. 동 규정은 중소기업기술의 유출방지 및 보호를 위해 중소기업이 지켜야 할 기술보호의 원칙이라 할 수 있다.
- ② 따라서 세부규정의 수립은 무엇보다 정확해야하고, 이해하기 쉬워야 하며, 실천이 가능해야하고, 세밀한 부분까지 언급되어야 한다.
- ③ <표 3-2> 및 각 영역별 기술보호지침을 참조하여 중소기업별 특성에 맞게 조문화하는 것이 바람직하다.

<표 3-2> 중소기업 기술 보호 세부 규정안

영역	세부항목	비고
기술보호조직 정책	- 기관 총괄조직(전담부서) - 부서별 담당자 지정 및 업무분장 - 외부기관과의 공조체제 명시	기능과 업무분장
정보자산관리 정책	- 보유하고 있는 자산에 대한 분류기준을 정하고, 등급 분류 및 표시	비밀성, 무결성, 가용성
인력관리 정책	- 임직원, 퇴직자, 사내근무 외주업체직원, 외부업체 관련자, 외국인 등 관리 대책 - 직무발명 보상 정책 수립 등 명시	직책구분 대책 서약서, 보상책
물리 및 환경적 보안 정책	- 중요시설과 설비 구분하여 보호조치 명시 - 예방적 차원의 접근방식에 해당하는 대책명시	중요시설의 보호 및 접근통제

영역	세 부 항 목	비 고
기술적 보안 정책	- 정보통신, 서버, DB, 이메일 보안, 개인 PC, 노트북, 외부 침입방지 (Firewall/Anti-Virus), CD 및 USB, 화면보호, P/W보호대책 명시	H/W, S/W발달에 따라 수시로 보완
기술보호 운영관리 및 사고대응 정책	- 기술의 유출 또는 침해사고 발생 시 대응책 - 피해최소화 복구방안의 절차 및 법적 대응 방법 - 유관기관 통보, 원인 및 취약점 분석, 개선 절차	사고 시 관계기관에 보고
기술보호 교육 수행 정책	- 기술보호교육, 지도점검, 감사, 상벌 등 규정	상벌기준 명시

2. 주요 자산관리

중소기업이 대내외의 부정행위로부터 주요 기술을 보호하기 위해서는 기업이 보유하고 있는 주요 정보 자산을 적절히 파악해서 관리해야 한다. 기업의 모든 정보를 영업비밀로 관리하기에는 비용과 인력이 요구되므로 기업에 부담이 될 수 있다. 따라서 주요 자산을 파악하여 분류하고 가치를 평가하여 관리체계를 수립하는 것이 요구된다. 실제 영업비밀 유출사례에서 주요 자산관리가 되어 있지 않은 경우 법적 구제를 받을 수 없는 경우가 많다.

(1) 필요성

- 핵심자산을 분류, 평가, 통제하여 유출방지 및 보호하기 위함이다.

(2) 자산의 분류

- 중소기업이 보유하고 있는 자산은 국제 기술보호 표준규격(ISO/IEC 27001)에 따라 다음과 같이 분류할 수 있다.

〈표 3-3〉 국제 기술보호 표준규격(ISO/IEC 27001)

구 분	대 상	세부내용	
정보자산	중소기업이 보유 관리하는 모든 종류의 정보	- 기술정보 - 업무관련정보 - 세일즈, 마케팅 정보	- 개인정보 - 조직정보 - DB정보
문서자산	중소기업이 보유 관리하고 있는 모든 문서	- 정책, 지침 인사기록	- 업무관련 문서 - 송장 등
소프트웨어 자산	정보시스템에 사용하는 프로그램	- 운영프로그램 통신 프로그램	- 어플리케이션
물리적 자산	업무에 활용되는 하드웨어	- 설비, 서버, 책상, 의자 등	
인적자산	중소기업에 속해 있는 모든 인원	- 내부직원 - 제3자 (외주업체, 컨설턴트 등)	- 아웃소싱 직원 - 퇴직자 - 고객 등
대외기관 제공서비스	대외기관에서 제공되는 서비스	- 정보서비스 - 전기, 수도, 사무실 등	- 통신서비스

(3) 주요 자산의 파악

다른 경쟁기업보다 우월한 지위를 획득할 수 있는 제품 및 서비스로부터 자산을 분석하는 것이 바람직하다. 특히 자사만이 생산하는 독창적인 제품이나 기업에게 이윤을 주는 제품 또는 서비스로부터 자산을 파악한다.

기업 경쟁력의 원천이 되는 제품이나 서비스를 특정하고, 이와 관련된 업무프로세스인 ①연구개발, ②제조, ③판매, ④기타 영업활동에 있어서 주요한 정보를 파악하고 분석한다. 제품에 포함된 핵심 기술이나 서비스의 노하우 등은 그 자체가 주요한 자산이 되며, 이러한 정보를 만들고 관리하는 각 프로세스를 문서로 정리해 두는 것이 매우 중요하다.

- ① 연구개발 단계 : 연구노트, 실험데이터, 설계정보, 금형정보, 디자인 정보, 신제품의 사양, 미래 연구개발 계획 등
- ② 제조 단계 : 설비(배치도, 투자계획), 원료(배합비율, 원가구성), 구입처목록, 원가 등
- ③ 판매 단계 : 판매전략, 고객명부, 소비동향분석, 클레임관리, 시장분석정보 등
- ④ 기타 경영활동 단계 : 경영계획, 인사정보, 회계정보, 임금체계, M&A 계획, 직원교육프로그램, 정보관리시스템 등

(4) 주요 자산 목록 작성

앞서 파악된 기업의 주요한 자산을 제품 및 서비스의 프로세스별로 그리고 자산의 종류별로 분류하여 목록을 작성해 두어야 한다. 특히 기밀로 유지해야 하는 기술 및 경영상의 정보는 별도의 목록으로 작성하는 것이 바람직하다.

기밀정보는 명칭, 관리번호, 비밀등급, 등록일, 보존기간, 기록매체, 비치장소, 관리책임자를 표시하여 목록을 작성한다. 비밀등급은 회사 임원 및 특정 인력만이 볼 수 있는 정보(1급), 모든 직원이 볼 수 있는 대외비(2급)로 분류하여 표시한다.

한편 기술의 가치를 평가해 두는 것이 좋다. 제품이나 서비스에서 중요한 기술이나 노하우가 차지하는 비중을 평가하여 가치를 산정해 놓으면 기술이전, M&A, 손해배상 산정 등에 활용할 수 있다.

3. 영업비밀 관리

중소기업 기술은 특허 및 실용신안으로 보호할 수 있지만 또한 영업비밀의 형태로 존재하는 경우가 많다. 특허는 특허청에 출원을 통해 심사를 받아 등록되어야 보호받는 반면, 영업비밀은 공공연히 알려져 있지 않고 합리적인 노력을 통해 비밀로 관리되어야 한다. 따라서 중소기업은 스스로 생산방법, 판매방법, 그밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 규정하고 관리하여야 한다.

(1) 필요성

막대한 시간과 비용을 투자하여 개발한 기술과 관련 정보는 그 재산적 가치가 높아 기업의 가장 중요한 자산이라고 할 수 있다. 기업은 이러한 기술정보를 많은 경우 비밀로 유지하는 경우가 많은데, 이를 제대로 지키지 못하면 기업은 어려움에 처하게 되거나 파산으로 이어지는 경우도 있다. 기술유출이 만연해 지면 시장질서가 교란되고 장기적으로 국가 경쟁력도 떨어지게 된다. ‘부정경쟁방지 및 영업비밀보호에 관한 법률(이하, ‘영업비밀보호법’이라 한다)’은 기술정보를 합리적인 노력으로 비밀로 유지한 기업을 보호해 주고 있다.

영업비밀 보호를 위한 법과 제도적 장치가 마련되어 있다 하더라도 영업 비밀을 보유한 기업 스스로의 보호노력과 관리가 선행되지 않는 한, 항시 영업비밀 유출의 위험에 노출될 수밖에 없다. 따라서 기업이 연구·개발한 영업비밀 보호를 위한 체계적인 관리방안을 수립하는 것이 매우 중요하다.

(2) 영업비밀 보호 요건

영업비밀이란, “공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 합리적인 노력에 의하여 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보”를 말한다.(부정경쟁방지법 제2조 제2호)

따라서 중소기업기술을 영업비밀로 보호하기 위해서는 비공지성(비밀성), 경제적 유용성, 비밀관리성을 갖추어야 한다. 요건으로 정의된다. 각 요건에 대한 세부사항을 잘 이해하여 기술보호를 위한 노력을 적극적으로 추진하여야 한다.

① 비공지성(비밀성)

‘공연히 알려져 있지 아니하다’고 하는 것은 그 정보가 간행물 등의 매체에 실리는 등 불특정 다수인에게 알려져 있지 않기 때문에 보유자를 통하지 아니하고는 그 정보를 통상 입수할 수 없는 것을 말하고, 보유자가 비밀로서 관리하고 있다고 하더라도 당해 정보의 내용이 이미 일반적으로 알려져 있을 때에는 영업비밀이라고 할 수 없다.(대법원 2004.9.23. 선고 2002다60610 판결)

② 경제적 유용성

‘독립된 경제적 가치를 가진다’는 의미는 정보의 보유자가 그 정보의 사용을 통해 경쟁자에 대하여 경쟁상의 이익을 얻을 수 있거나, 또는 그 정보의 취득이나 개발을 위해 상당한 비용이나 노력이 필요하다는 것을 말한다.
(대법원 2008.2.15. 선고 2005도 6223 판결)

③ 비밀관리성

영업비밀로 보호받기 위해선 객관적이고 실질적으로 합리적인 노력(직원교육, 기술보호규정, 비밀유지서약, 출입통제, 비밀번호관리, 네트워크 및 저장매체에 대한 보안 등)에 의하여 기업정보를 비밀로 관리해야 하며, 중소기업은 회사의 매출, 인력 등 사정에 맞춰 합리적인 수준에서 기술보호 노력을 할 것이 요구된다. (2015.1.28 시행 부정경쟁방지법 이전에는 비밀관리성의 정도를 엄격한 수준인 “상당한 노력”을 요구하였다.)

(3) 영업비밀의 대상

- ① 기술 정보 : 설계도면, 기계 운용 매뉴얼, 화장품 식품 의약품 등의 원재료 성분 표, 혼합 또는 배합 요령 및 비율, 실험 데이터, 소스코드, 회로도, 제조 공정도 등
- ② 경영 정보 : 제품원가 분석자료, 대리점 마진율, 할인율, 신제품 개발 생산 판매 계획, 원자재의 구입 선, 주문서, 거래선 루트, 고객리스트, 타사와의 합병·지원·투자계획, 자금 조달 계획 등

4. 인적자원 관리

중소기업의 가장 취약한 기술 유출 위협 요인은 조직의 내부 인력이다. 따라서 기업의 핵심인력 유출에 대한 여러 요인을 고려하여 핵심인력 유출을 방지하기 위한 대책을 마련하여야 한다.

(1) 인적 자원 관리의 필요성

- 2014년에 국가정보원 산업기밀보호센터에서 발표한 2009 ~ 2013년까지 5년간 산업기술 해외유출 적발 현황을 보면, 전·현직 임직원이 전체 유출자의 80%를 상회하고 있다.
- 경영자의 보안마인드와 보안담당자의 의식변화가 중요하며, 기술보호를 위한 제도를 활용하고 내부 규정을 제대로 갖추고 통합보안시스템을 구축하는 것이 바람직하다.

(2) 비밀유지서약서(보안서약서)

- 내부 직원이 서명한 비밀유지서약은 내부직원과 회사 간 계약으로서 내부 직원에게 비밀유지의무를 부과하고 인지시켰다는 사실에 대한 법적 증거
- 입사 시, 퇴사 시, 교육 시 또는 부서배치 및 프로젝트 투입 시 등에 있어서 비밀서약서에 서명 또는 날인하도록 한다.

- 교육 시에는 보안정책 및 보안세부규정을 인지시키고, 해당내용 숙지하였다는 문구 포함한다.
- 프로젝트 투입 시에는 구체적인 업무, 신분, 기밀 업무 범위 등을 서약서에 명시(각종 서약서 양식 참조)

(3) 전직/경업 금지약정

- 근로자가 재직 중 얻게 된 회사의 기술, 고객, 거래처 등의 정보를 이용해 다른 경쟁업체에 취업하거나, 회사를 설립함으로써 손해가 발생하는 것을 막기 위해 일정기간 제직회사와 경쟁관계에 놓일 수 있는 업무를 하지 못하도록 금지하는 약정
- 비밀유지서약서는 모든 임직원들에게 부과되어야 하는 반면, 전직금지약정 또는 경업금지약정은 핵심기술인력 또는 임원 등과 체결
- 주의할 점은 전직금지 기간이 비밀의 정도, 시장성 등을 고려해 볼 때 과도하게 장기간일 경우에 약정이 무효가 될 수 있다.(통상 6개월 - 1년/ 경업금지의 경우 2년-3년)
- 또한 전직금지 기간 동안에는 적절한 보상(예, 급여에 해당하는 금액)을 지급하여야 한다. 전직금지 기간을 초과하여 부과되는 경업금지 기간 동안에는 전직금지 보상금 보다 적은 금액으로 책정할 수 있다.

(판례) 법원은 경업금지약정의 유효성을 ① 보호할 가치가 있는 사용자의 이익, ② 근로자의 퇴직 전 지위 및 퇴직 경위, ③ 경업 제한의 기간·지역 및 대상 직종, ④ 근로자에 대한 대가의 제공 유무 등을 고려해 판단하고 있으며, 경업제한 기간이나 지역 등을 약정한 내용보다 감축하여 인정하는 경우도 있다. (대법원 2010.3.11. 선고 2009다92244 판결)

(4) 직무발명보상제도의 운영

- 직무발명은 종업원이 종업원의 현재 또는 과거의 직무에 관하여 발명한 것이 사용자의 업무범위에 속하는 것으로 발명진흥법은 종업원의 직무발명에 대한 권리를 사용자(회사)가 승계한 경우 상당한 보상을 하도록 규정
- 연구개발 업무를 담당하는 직원이 회사 업무와 관련된 발명을 한 경우 해당 발명에 대한 권리는 원시적으로 그 직원에게 귀속되며, 회사는 계약 또는 근무규정에 의하여 직무발명에 대한 권리를 승계할 수 있다. 종업원이 직무발명에 대하여 특허를 받을 수 있는 권리를 사용자 등에게 승계하거나 전용실시권을 설정한 경우에는 상당한 보상을 받을 권리를 가진다.
- 보상의 종류 : 발명제안보상, 출원보상, 등록보상, 실시보상, 출원유보보상 등
- 보상형태와 보상액에 관한 규정은 종업원과 협의하여 정한다.
- 직무발명은 중소기업의 기술개발을 장려할 뿐만 아니라 숙련된 핵심인력 및 기술의 유출을 방지하는 효과가 있다.

(5) 입·퇴사자 관리

가) 입사자

- ① 도덕성, 범죄 및 개인파산 등 법률적 문제, 입사 동기, 이전 회사의 퇴직 동기 등을 면밀히 검토하고 비밀유지서약서를 제출토록 한다.
- ② 특히 경력 입사자는 이전 회사에서 영업비밀을 취급하였던 내용을 서면으로 작성하여 제출토록 함으로써 회사 간 분쟁 발생을 예방할 수 있다.

나) 퇴사자

- ① 업무 인수인계 리스트를 충실히 작성하도록 하여 서명하도록 하며, 경업금지 및 비밀유지 특약이 포함된 퇴직서를 제출하게 한다.
- ② 퇴사자가 재직 시 작성한 각종 서약서나 프로젝트 투입 기록, 전자파일 입출력 또는 암호화 해제 로그 등을 해당 부서 팀장 또는 중역, 보안 담당 부서에서 확인하고 반드시 보존하여 사후 분쟁에 대비

(6) 사원증 관리

- 재직자와 외부 방문객을 구분하고 출입지역에 대한 차등적 제한
- BAR CODE, RFID CARD, SMART CARD를 적용한 사원증이 많이 보급되며, 복사, 위변조가 용이한 BAR CODE 방식은 사용을 지양한다.
- 재직자도 출입할 수 있는 지역과 출입을 제한하는 지역을 구분할 수 있도록 사원증을 칼라로 구별하거나 전자식별 시스템을 구현

5. 기업의 시설관리

물리적인 위협으로부터 주요 정보자산을 보호하기 위해 주요 사무실, 연구소, 중요 설비 및 장치 설치장소, 지역 등을 일정한 기준에 따라 구역을 지정한 후 구역별 보호대책을 마련하여 외부인 및 관련 없는 내부인의 출입 통제 구역으로 지정하여 구역별 보호대책을 마련해야한다.

(1) 공동구역

- ① 외부인의 출입시 이름, 주소, 주민등록번호, 연락처, 소속 등 출입자의 정보를 관리한다.
- ② 주요 정보를 출입관리대장에 기재하고, 내부인력을 통해 안내한다.
- ③ 과도한 불편을 주어 거부감을 주지 않도록 적절한 수준을 유지한다.

(2) 일반구역

- ① 주요 정보에 대한 보호의식이 약해지기 쉬워 기술 유출 가능성이 높다.
- ② 외부인과 내부인을 구별하기 위해 사원증을 패용하도록 한다.
- ③ 자리가탈 시 화면보호기 설정, 책상 정리, 주요문서는 캐비닛에 보관한다.
- ④ 복사기, 팩스기 등은 사무실 안쪽에 비치한다.

(3) 제한구역

- ① 승인받은 내부인만이 출입하도록 하며, 외부인의 출입은 반드시 통제한다.
- ② 설비의 훼손, 파괴, 오작동 등의 문제에 대한 주의가 필요하다.

(4) 통제구역

- ① 통제구역은 주요 기술에 대한 개발 및 연구가 이루어지고 주요 정보를 보관하고 있으므로, 최상위의 보안대책을 적용한다.
- ② 해당 근무자 이외 모든 출입을 금지한다.
- ③ 일반직원도 승인을 받은 후에 출입하고 외부인은 절대 출입을 금지한다.

〈표 3-4〉 제한구역 보호 시스템

구 분	내 용	사용 가능한 장비
출입통제시스템	시설 출입 인원 및 차량 통제	- RFID 태그 및 ID카드 - Interlocking Portal Door
반·출입관리시스템	장비, 특히 전산장비 반·출입 통제	- X-ray 검색장비 - 문형 금속탐지기
화상감시시스템	인원 및 차량 등의 출입여부 확인	- CCTV 등
차량출입통제 시스템	차량 출입 통제	- 차량번호판 인식장비 - 역방향 진입금지 장비
방범시스템	불법적 침입 및 시설 피해 경고, 방지	- 방탄유리 - 유리파손 알람 장비

6. 정보시스템 관리

기술보호가 관리되지 않는 정보시스템은 절대 신뢰하지 않아야 하고, 네트워크 보안은 암호화를 하지 않은 패킷(packet : 네트워크를 통해 전송하기 좋도록 자른 데이터의 단위)의 송수신은 엄격하게 금지하고 모든 네트워크를 최적화해야 한다.

기술적 보안을 담당하는 담당자가 다음과 같은 보안조치를 취할 수 있도록 보안정책을 수립해야 한다.

(1) 주기적인 백업

중요 데이터는 삭제나 변조를 대비해 주기적으로 백업이 되어야 한다. 고의적인 사고로 데이터 손실이 발생할 수도 있지만, 관리자의 실수, 시스템의 하드웨어, 소프트웨어의 장애로 인해서도 발생할 수 있으므로 백업은 매우 중요하다.

(2) 불필요한 서비스 중단

시스템설치 시 디폴트(default)로 열려 있는 서비스 포트(port)를 막아야 한다. 방화벽을 활용해 사용하지 않는 포트는 막고, 사용하는 포트도 웹 서비스(web service)를 제외하고는 잘 관리해야 한다. 물론 포트스캔(port scan) 프로그램을 활용하면 열려 있는 포트를 확인해 침입을 할 수 있지만 그래도 최소한의 보안조치는 취해 두는 것이 좋다.

(3) 보안프로그램 설치 운용

백신, 방화벽 등 기본적인 보안프로그램은 반드시 설치하여 운용하고, 새롭게 생성되는 변종 바이러스 및 해킹을 방지하기 위하여 반드시 업그레이드를 한다. 시스템의 운영체제도 개발사가 보안취약점이 발견될 때마다 패치(patch)를 제공하므로 이에 관한 정보를 취합해 즉각적으로 반영해야 한다.

제3절

기술개발 및 기술거래 시 관리와 운영방안⁴⁾

1. 기술개발 형태에 따른 기술유출 방지 대책

기술의 개발은 여러 형태로 이루어질 수 있는데 크게 구분하면 국가연구개발 사업에 의해 개발되는 경우, 대상기관 자체로 개발되는 경우, 공동/위탁연구에 의해 개발되는 경우로 구분할 수 있다. 이러한 개발 형태는 고유의 특성 때문에 기술이 유출되는 것도 형태별로 다르게 나타나며, 기술 개발 시에 유출 및 침해가 발생하는 주요원인 중 공통적인 원인은 인력관리 및 권리설정의 소홀이다. 특히 80% 이상의 기술 유출 및 침해사고는 임·직원(연구원 포함)에 의해서 일어나고 있다. 또한 법적 권리를 설정하지 않음으로 인해 기술의 유출 및 침해 이후 법적으로 보호받을 수 없게 되는 경우도 빈번하게 발생하고 있다.

4) 국가연구개발사업 기술보호 표준 매뉴얼, 미래창조과학부, 2015-08.

(1) 국가연구개발 사업을 통한 기술 개발

국가연구개발 사업을 수행하는 중소기업은 미래창조과학부에서 제정한 ‘국가연구개발 사업 공통기술보호 지침’을 준수해야 한다. 따라서 위 지침에 의해 중소기업이 어떤 일을 해야 하는지 파악하는 것이 중요하다.

국가연구개발 사업을 통해 개발할 경우 중소기업이 보안관련 이행해야하는 사항은 다음과 같다.

〈표 3-5〉 중소기업 준수사항

조 항	기술보호 관리/이행사항
제3조 활용	<ul style="list-style-type: none"> • 관련 기술보호 담당자 지정 및 규정을 마련하는 등의 보안대책을 수립, 시행
제6조 중소기업(연구기관)기술 보호심의회	<ul style="list-style-type: none"> • 중소기업(연구기관)기술보호심의회 구성, 운영 <ul style="list-style-type: none"> - 국가연구개발사업의 수행과 관련된 기술 보호에 관한 사항을 심의하기 위해 “연구기관기술보호심의회” 구성, 운영
제7조 분류기준	<ul style="list-style-type: none"> • 분류기준에 따른 보안등급 분류 <ul style="list-style-type: none"> - 보안등급 분류 및 과제수행에 따른 모든 문서에 보안등급 표기
제8조 분류절차	<ul style="list-style-type: none"> • 과제신청서 및 연구개발계획서에 보안등급 표기 <ul style="list-style-type: none"> - 연구책임자는 과제신청서에 등급을 분류하여 연구보안심의회에 제출 - 연구기관장은 연구개발계획서에 등급을 표기하여 제출
제11조 보안등급에 따른 조치	<ul style="list-style-type: none"> • 보안등급에 따른 조치 <ul style="list-style-type: none"> - 보안등급(보안과제/일반과제)에 따라 보안조치수행
제12조 기술보호현황보고	<ul style="list-style-type: none"> • 연구개발과제 기술보호 현황 보고
제13조 보안사고 발생 시 처리	<ul style="list-style-type: none"> • 보안사고 발생 시 조치 <ul style="list-style-type: none"> - 사고보고, 수습 및 재발방지 대책 마련
제14조 기술보호 위반 시 조치	<ul style="list-style-type: none"> • 기술보호 위반 시 조치(협약서에 반영) <ul style="list-style-type: none"> - 기술보호에 최선의 노력의무 및 정당한 사유 없이 보안조치를 이행하지 않을 경우 참여제한

(2) 중소기업 자체적인 기술 개발

인력관리 및 권리설정의 소홀로 인해 기술 유출 및 침해되는 빈도가 가장 많은 것이 중소기업에서 자체 개발하는 경우이다. 특히 연구개발에 직접 참여한 임직원에 대한 관리 소홀로 인해 유출 및 침해되는 경우가 가장 많다. 임직원은 자신이 참여한 연구 결과를 자신의 것이라고 생각하게 되고 외부의 유혹이 있을 때 거리낌 없이 제공하는 경우가 발생하기에, 중소기업이 개발한 기술 자료에 대한 권리설정을 소홀히 하면 부정경쟁방지법에서 정하는 영업비밀 보호는 물론 특허, 실용신안, 디자인 등의 보호를 받을 수 없게 된다.

1) 인력관리

연구과정에서 핵심 연구원, 행정관리 인력 등에 대한 관리는 앞서 인적자원 관리 부분에서 설명한 바와 같이 기술보호의 가장 중요한 요소이다. 교육을 통하여 기술보호에 대한 이들의 인식을 변화시키고, 비밀유지 서약이나 보안시스템 등 제도적 장치를 통하여 인력을 관리해야 한다.

2) 권리의 설정

① 특허권

특허는 발명자에게 독점배타적 권리를 부여하며, 출원이라는 절차를 통하여 발명의 내용을 일정한 기재방식에 따라 작성한 특허명세서와 도면 등을 특허청에 제출하여야 한다. 특허청은 출원된 발명이 특허의 요건을 만족하는지를 심사하여 특허등록 여부를 결정한다. 특허는 출원 후 18개월이 지나면 공개가 되며 등록된 특허에 대해서 20년간 특허권을 부여한다. 특허권자는 유사제품 등 침해 기술에 대하여 민·형사적 제재를 가할 수 있다.

② 실용신안권

실용신안은 물건의 형상·구조 또는 조합에 관한 실용적 고안에 대하여 주어지는 독점배타적 권리이며, 특허와 같이 신규성, 진보성 등을 만족하여야 등록이 가능하다. 실용신안은 특허와 유사하지만 개인발명가나 중소기업의 작은 발명을 보호하는데 목적이 있어 진보성 요건이 특허에 비하여 다소 완화되어 있다. 실용신안의 보호기간은 출원일로부터 10년이다.

③ 디자인권

디자인이란 물품(물품의 부분 및 글자체 포함)의 형상, 모양이나 색채 또는 이들을 결합한 것으로서 시각을 통하여 미감을 일으키게 하는 것을 말한다. 독립거래의 대상이 되는 유체 동산인 물품(또는 동 물품의 부분)의 외관에 관한 창작을 보호하며, 출원을 통해 디자인등록이 되면 20년간 권리를 향유할 수 있다.

④ 저작권

저작권은 인간의 사상이나 감정을 표현한 창작물에 대해서 주어지는 배타적 권리를 말한다. 따라서 저작권의 대상에는 음악, 영화, 소설, 건축물, 사진, 지도, 미술, 소프트웨어 등이 있다. 저작권은 창작을 하면 권리가 발생되어 특허와 달리 반드시 등록을 요하지 않는다. 그러나 등록을 하게 되면 일정한 법적 추정력을 부여받아 두터운 보호를 받을 수 있다. 저작물의 등록은 한국저작권위원회에서 담당하며, 오/오프라인에서 등록할 수 있다. (<http://www.copyright.or.kr>) 저작권의 보호기간은 창작자의 생존동안과 사후 70년이며, 기업의 저작권(업무상저작물)은 공표한 때부터 70년간 보호된다.

(3) 공동/위탁연구 기술 개발

공동/위탁연구 개발은 사전조사, 의향서 교환, 비밀유지 계약 체결, 옵션계약 체결, 공동/위탁연구과제 계획서 검토, 예비적 합의 조인, 중요 계약조건의 교섭 및 확인, 공동연구계약의 체결, 공동연구결과물 보호를 위한 사후관리의 단계를 거치게 된다. 이 중 기술유출의 가능성이 높은 단계는 공동/위탁연구과제 계획서 검토 단계이다. 계획서 검토과정에서 개발기술 및 제품 관련 연구 인력, 연구 성과, 연구절차 등에 대한 의견교환 및 협의를 진행하면서 노하우와 중요정보에 대한 유출 및 침해가 발생할 가능성이 높다.

공동/위탁연구 개발시 각 단계 중 기술의 유출 및 침해가 발생할 가능성이 높은 순서는 ① 연구과제 계획서 검토단계, ② 계약단계, ③ 연구결과물 사후관리 단계 등이다. 각 단계별 유출 및 침해 예방 방법은 다음과 같다.

〈표 3-6〉 공동/위탁 단계별 유출 및 침해 예방

구분	내용
공동 / 위탁연구과제 계획서 검토단계	<ul style="list-style-type: none"> 공동 / 위탁연구하는 주체가 기술유출 방지전략을 이행하는지 여부 확인 실무 협의 과정에서 참석 대상자에 대한기술유출 방지 사전교육 실시 연구과제를 세분화하여 계획서만으로는전체의 기술이 확인되지 않도록 조치
공동 / 위탁연구 계약단계	<ul style="list-style-type: none"> 공동 / 위탁연구 범위 및 연구개발 시발명성과 개시의무 협의 지식재산권이나 노하우의 귀속 여부 확인 상용화에 대비한 제조 / 판매주체 결정 공동 / 위탁연구와 연관된 연구개발 제한
공동 / 위탁연구 결과물 사후관리 단계	<ul style="list-style-type: none"> 공동 / 위탁연구 결과물에 대한 활용이 합의범위 내에 존재하는 지 여부 확인 사용된 기자재 / 설비에 대한 소유권 협의

2. 기술거래에 따른 기술유출 및 보호 관리방안

두개 이상의 기업이 합병을 추진하거나, 공동출자를 통해 신규 사업을 진행하는 등의 과정에서 상호간의 이해관계에 따라 기술이 거래될 수 있다. 그러나 이와 같이 기술이 거래되는 경우 일방의 기업이 기술계약의 특성을 악용하여 상대방 중소기업의 기술을 악의적으로 유출하려는 시도가 종종 발생하고 있다. 합병을 추진하면서 실사를 핑계로 상대 중소기업의 중요 정보만을 빼내어 간다거나, 공동출자를 통해 진행되는 신규사업을 독자적으로 이용하거나, 기술만 제공받고 계약 없이 무단 사용하는 등 그 형태도 다양하다. 기술의 부당한 유출 시도는 기술계약의 유형에 따라 각각 다른 양상을 보이고 있으며, 기술계약별로는 빈번하게 발생하는 특정 단계가 있다.

(1) 기술거래(기술계약)의 유형

〈표 3-7〉 기술거래 유형

구분	설명	
기술양도형 계약	합병계약(M&A)	• 당사자 일방이 기술의 소유권을 이전하는 계약과 둘 이상의 회사를 하나의 회사로 합병하는 것을 목적으로 하는 계약
	조인트벤처	• 2인 이상의 업자 간에 단일의 특정일을 행하게 하는 출자계약 또는 공동계약
기술대여형 계약	라이선스 계약	• 기술제공자가 상대방인 기술 도입자에게 특정기술에 대하여 실시권을 허락하는 계약
	위·수탁 계약	• 위탁자가 하청기업에게 특정기술을 제공하고 상대방에게 자기의 기관으로서 해당 기술을 실시하게 하는 계약 ('하청 라이선스 계약')

(2) 유형별 기술 유출 및 보호 관리방안

1) 합병계약

합병계약은 두 개의 중소기업이 각 중소기업에 속해있는 모든 기술을 포함하여 하나의 중소기업으로 합쳐지는 계약을 말한다. 따라서 상대 기업에 어떠한 기술이 있는지 확인하는 과정을 거치는데, 그 과정에서 기술이 빈번하게 유출되고 있다.

〈표 3-8〉 합병계약의 기술유출 방지 대책

계약 단계	기술 유출 및 보호 관리방안
경영전략 수립 및 M&A 전략팀 구성	<ul style="list-style-type: none"> • 공동 / 위탁연구하는 주체가 기술유출 방지전략을 이행하는지 여부 확인 • 실무 협의 과정에서 참석 대상자에 대한기술유출 방지 사전교육 실시 • 연구과제를 세분화하여 계획서만으로는전체의 기술이 확인되지 않도록 조치
인수의향서 및 비밀유지 계약 체결	<ul style="list-style-type: none"> • 실제 계약서가 작성되어 법적으로 보호받을 수 있기 전까지 기술에 대한 세부자료가 제공되지 않도록 유의
정밀실사, 기업가치 평가 및 가격 결정	<ul style="list-style-type: none"> • M&A 중개기관을 통하여 업무를 추진하는 경우 중개기관에 의해 기술이 무단 사용되지 않도록 비밀유지 계약을 체결 • 중개기관을 통하지 않을 경우 비밀유지 계약을 체결하고 재확인 후 실사 진행
협상 및 계약서 작성	<ul style="list-style-type: none"> • 합병계약서에는 자료보존 방법과 유출의 금지, 제한에 관한 조항 삽입 • 계약단계에서 근로자와의 기술보호 서약서 징구 • 개인이 비밀을 유출한 경우 합병상대기업의 연대책임 명시

2) 조인트벤처

조인트벤처는 각기 다른 중소기업의 기술을 이용하여 공동 투자하는 방식으로 투자 후 운영을 위해 기술을 공유해야 한다. 이 때 기술의 유출이 발생 가능하다. 다음은 조인트벤처의 단계에 따른 기술 유출 및 침해 대응방안이다.

〈표 3-9〉 조인트 벤처의 기술유출 방지 대책

계약 단계	기술 유출 및 보호 관리방안
대상기업 발굴	<ul style="list-style-type: none"> 대상기업이 비밀유지의무의 이행 능력이 있는지 여부 확인
의향서(MOU) 체결	<ul style="list-style-type: none"> 합작투자할 상대방을 발굴하는 단계에서 상대방 기업에 핵심적인 기술정보에 대한 자세한 정보를 제공하지 않도록 주의 세부 계약 조건에 대해 신의성실의 원칙에 따른 의무를 부과하고 기술에 대하여 제3자에게 공개하거나 이를 임의로 이용하지 않을 의무를 부담
조인트 벤처설립절차 진행	<ul style="list-style-type: none"> 합작투자회사를 설립하는 팀의 담당자로부터 비밀유지 서약서 징구
최종계약체결	
조인트 벤처 설립 완료	

3) 라이선스 계약

라이선스 계약은 제품이나 기술을 독자적으로 개발하는데 필요한 시간과 자원을 별도로 투입하지 않고 그 제품이나 기술을 획득하는 방법이다. 기술을 보유하고 있는 기업이 라이선스 계약 체결시 단계별로 발생될 수 있는 기술유출의 문제는 아래 도표와 같다.

특히, 해외에 기업과 기술거래를 하는 경우 해외로 이전하기 전에 이전 국에 특허 및 기술에 대한 권리화를 완료하여 등록이 유효한지 여부를 항상 확인할 수 있는 시스템을 구축한다. 특히 계약서에는 다음사항을 명시한다.

- 개량기술에 대한 소유권의 귀속문제
- 서브 라이선스(재실시 허락) 금지
- 기술 및 노하우의 범위, 대상지역 특정, 계약 종료 후 비밀유지, 관련 물품 및 설비의 반환, 계약 위반에 대한 벌칙 등이 문제된다.

〈표 3-10〉 라이선스 계약의 기술유출 방지 대책

계약 단계	기술 유출 및 보호 관리방안	
기술계약 점검	<ul style="list-style-type: none"> 대상기술의 가치 및 기술이전의 유형 	
계약상대방과 협의	<ul style="list-style-type: none"> 권리능력, 행위능력의 유무 기업규모(계약기술의 사업화 역량) 대가 지급을 위한 재정능력 	<ul style="list-style-type: none"> 계약상대방 중 조건협상의 주요 담당자 추가 기술개발의 능력
계약조건 검토	<ul style="list-style-type: none"> 기술이전의 대가 지급방법 / 지급처 성과의 귀속(개량 발명의 범위, 보고 등), 권리의 지분분할 기술이전의 대가(선급기술료, 경상기술료 등) 계약 유효기간, 계약의 변경 / 해지 / 종료 	<ul style="list-style-type: none"> 기술이전을 위한 지도방법 출원, 등록의 절차 및 비용의 부담 방법 손해배상 청구 / 범위
기타	<ul style="list-style-type: none"> 계약의 목적, 배경, 경위 확인 비밀의 유지, 정보의 반환 내용 협의 	<ul style="list-style-type: none"> 다른 법률과의 저촉여부 확인 정보의 상호 교환

4) 위·수탁 계약

위·수탁 계약은 위탁기업이 수탁기업에게 해당 물품을 생산하는 데 필요한 원재료를 공급하는 것이 보통이다. 또한 수탁기업은 위탁기업에 비하여 기술수준이 낮은 경우가 대부분이기 때문에 위탁기업의 기술지도가 필수적이다. 따라서 위·수탁 계약과 관련하여 생산공정, 제조설비, 기술지도 등 전 범위에 걸쳐 기술유출이 일어날 소지가 많다. 그래서 위·수탁 계약은 계약 단계별 대응이 아닌 다음과 같은 전략적 대응이 필요하다.

〈표 3-11〉 위·수탁 계약의 기술유출 방지 대책

계약 고려사항	기술 유출 및 보호 관리방안
제조설비에 대한 기술보호 유지	<ul style="list-style-type: none"> 핵심 제조공정이 포함된 도면이나 서류의 블랙박스를 추진 해외에 도면을 제공하는 경우에는 제조도면에 기재된 시험방법, 소재정보 등 개발 노하우를 삭제하고 제공 CAD/CAM 데이터는 현지 컴퓨터로 읽을 수 없도록 암호화
설비의 유지, 보수 관련	<ul style="list-style-type: none"> 유지보수를 직접 수행하고 부득이하게 현지인을 고용할 경우 출입지역은 한정 설비의 판매계약에 제조설비의 정기적인 유지보수 조항을 삽입

〈표 3-12〉 위·수탁 계약의 전략적 대응

계약 단계	기술 유출 및 보호 관리방안
계약전략 수립	<ul style="list-style-type: none"> 노동집약적 공정은 해외에서, 기술집약적 공정은 국내 혹은 지식재산권 보호가 가능한 국가에 두는 것을 원칙으로 하고 생산에 필요한 것만 현지에 이전
기술지도 범위	<ul style="list-style-type: none"> 제품 생산에 필요한 범위 만큼에 대하여만 지도
생산공정 관련 유의사항	<ul style="list-style-type: none"> 중요한 제조공정 등은 특정 본사로부터 파견된 직원만 관여 외부판매제한 조항, 자사의 중요한 노하우의 보호 의무조항, 위반행위에 대한 처벌조항 등을 계약서에 삽입 본사에서 핵심부품을 모듈화 하여 수출하고 해외에서 조립 순정품에 대한 위조방지 대책을 강구

제1절

기술 유출 주체 및 유출 방법

중소기업의 기술유출은 국내 대기업이나 경쟁사뿐만 아니라, 현재 첨단산업기술을 다수 확보한 우리나라와 경쟁관계에 있는 국외 기업들도 불법적인 방법뿐만 아니라 합법적인 방법으로 점차 고도화 되는 IT기술을 이용해 다양한 경로를 이루어지고 있다.

1. 유출 주체

유출의 주체는 크게 내부인(전·현직 임직원)과 외부인(외부협력업체, 경쟁업체, 대기업)으로 나눌 수 있다.

내부인에 의한 유출에 대해 살펴보면, <그림 4-1>과 같이 개인 PC 또는 업무시스템의 중요 정보나 전자문서를 Web/Mail/메신저의 첨부형태로 유출하거나, 오프라인문서의 경우 프린트/복사물을 불법 유출하거나 FAX를 통하여 유출한다.

외부협력업체의 경우, 업무상 필요에 의해 제공받은 영업비밀이나 자신들이 개발한 영업 비밀을 복사/전송 등의 방법으로 무단유출하고, 이를 직접 사용하거나, 자신들의 다른 거래업체에게 제공하기도 한다.

외부인에 의한 유출의 경우, 외부인이 네트워크를 통하여 시스템을 해킹하고 바이러스/웜을 이용하여 전자정보를 유출하거나 사내 무단 침입하여 전자정보를 보관하고 있는 IT자산이나, 프린트/복사기를 통해 생성된 오프라인 문서를 유출한다. 유지보수 등을 위해 사내에 출입한 외부인이 업무시스템의 DB 등에 접근하여 대규모 전자정보를 유출하거나, IT자산/오프라인 문서를 유출하기도 한다. 또한 시찰, 견학 등의 기회에 무단촬영, 복사, 절취 등의 방법으로 유출하기도 한다.

경쟁사나 대기업은 기업내부자를 매수하거나, 핵심기술 보유자를 스카우트하거나, 투자, 공동연구, 납품 등을 제안하며 기술 자료를 요구한 후 계약을 파기하는 방법으로 유출하기도 한다.

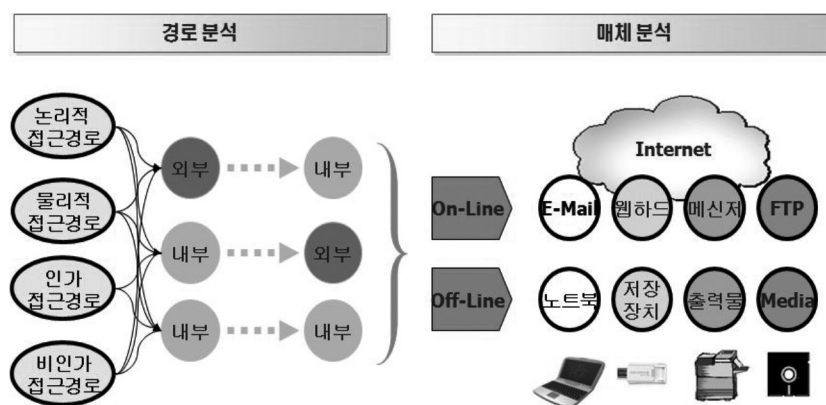
2. 유출 방법

기술 유출이 일어나는 방법은 크게 on-line과 off-line으로 나누어진다.

on-line 매체의 경우, IT 기술이 급속도로 발전함에 따라 이를 이용한 다양한 방법으로 유출이 일어나고 있는데, E-mail을 이용한 전자 문서의 전송, 웹 하드 등 P2P 사이트를 이용한 불법 공유, 메신저를 이용한 유출이 주요 이슈로 대두된다.

off-line의 경우, 기업의 감시망이 허술한 틈을 이용해 노트북이나 휴대용 저장매체를 불법 반출하거나, 최근에는 off-line문서에 대한 관리나 접근권한이 미흡한 것을 이용해 프린트나 복사물의 형태로 유출하는 경우가 많다.

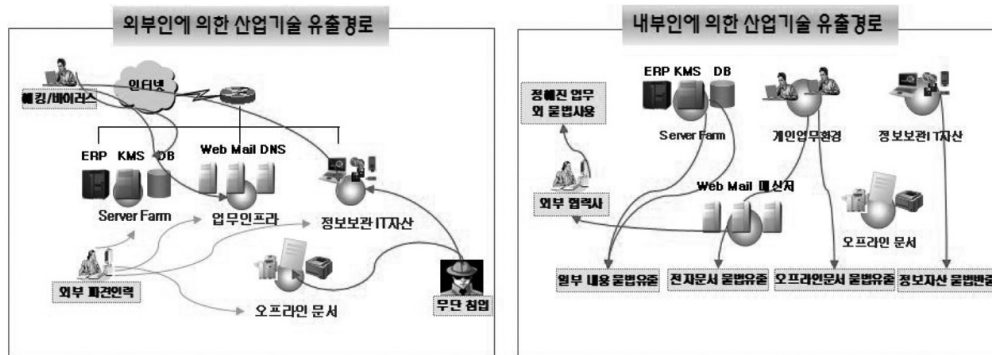
USB나 플래시 메모리 등 지능형 미디어를 이용한 기술 유출이 증가하고 있지만 현재 이에 대처할만한 기술이 미흡한 실정인기에 적극적 관리가 필요하다.



〈그림 4-1〉 기술 유출에 사용된 방법 분석

3. 유출 경로

현재 기술유출은 〈그림 4-2〉와 같이 불법적인 경로뿐만 아니라 합법적인 경로로도 유출되고 있다. 경쟁사는 현직 임직원에게 대한 금전적인 매수를 통한 인력 스카웃뿐만 아니라 산업스파이를 이용해 기술을 유출하고 있다. 첨단 기술을 확보한 기업의 거래업체를 통하여 부품 및 장비를 불법적으로 유출하기도 한다. 최근에는 합법적인 인수합병을 통해 기술전수를 이유로 핵심인력을 자사로 이동시키는 등 기술 유출 경로가 점차 다양해지고 있는 추세이다.



〈그림 4-2〉 내/외부인에 의한 기술 유출

제2절

기술유출 대응 프로세스

1. 기술유출의 대응계획

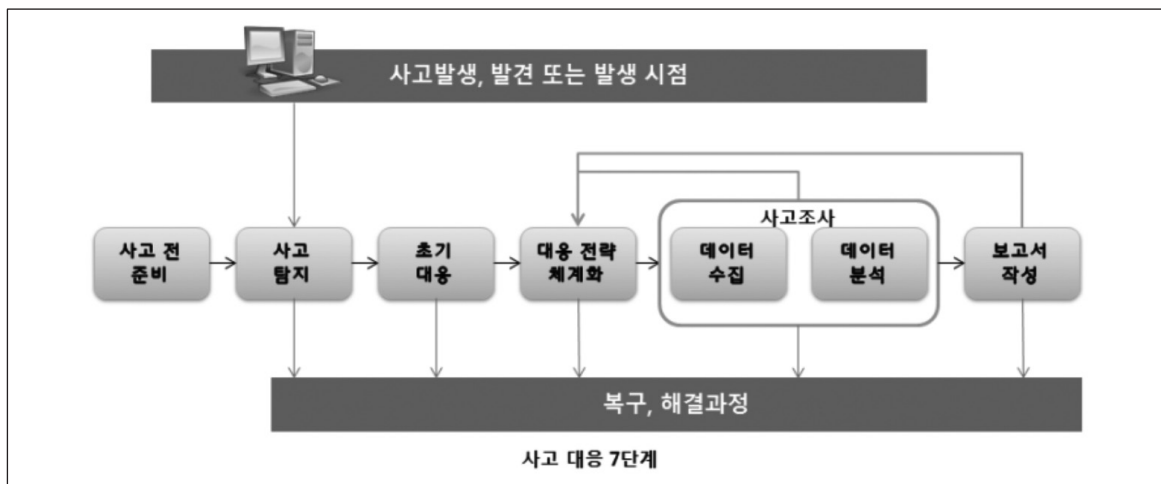
기술유출의 대응계획은 중소기업 기술의 유출 및 침해사고가 발생한 후에 취해지는 조치이지만, 예방적 차원에서 사고가 발생한 것으로 간주하여 계획을 세우고 그에 따라 훈련하여 실제 기술 유출이 발생 되었을 경우, 신속하고 능동적으로 대처할 수 있게 한다. 따라서 사고대응 및 복구계획은 매우 중요하다.

사고의 대응계획은 침해예방계획, 사고조치계획, 복구계획으로 구분 할 수 있는데, 우선 침해예방계획에는 평소 중소기업 기술의 유출 및 침해를 막기 위하여 지켜야 할 사항들이 포함되어야 하며, 모든 임·직원은 그러한 침해예방계획이 잘 지켜나갈 수 있도록 서로 교육하고 감독해야 한다. 사고조치계획에는 중소기업 기술이 유출 및 침해되었을 경우를 예상하여 부서 및 인력별로 조치해야 할 사항을 미리 규정해 두고, 사고 발생 시 조치에 따라 대응한다. 복구계획은 조치 중 복구와 관련된 내용을 따로 규정해 둬으로써 업무의 정상화를 위해 우선적으로 노력해야 할 사항들을 확인할 수 있도록 한다.

2. 기술유출 대응 프로세스



〈그림 4-3〉 사고대응 5단계



〈그림 4-3〉 사고대응 7단계

(1) 유출사실 발생에 따른 보고

- 중소기업이 기술에 대한 침해 또는 유출사실을 발견한 경우, 간단한 사실 관계를 확인 후 기업내부 보고체계에 따라 즉시 보고

※보고순서 : 발견자 ⇒ 소속부서장 ⇒ 상급 부서장 ⇒ 대표이사

(2) 기술유출에 대한 자체조사

- 기술유출이 의심되는 임직원 또는 부서를 파악하고 과거업무 내역 및 핵심기술 접촉 기록 등을 전체 적으로 파악한다.

※이메일, USB 등을 통한 자료반출 여부, 핵심기술에 대한 접근 및 수정 히스토리 조사 등

- 유출한 기술사용이 의심되는 회사에 대해 해당기술의 개발 및 출시 등의 동향을 파악한다.

※의심되는 회사와 관계되는 내부 임직원 또는 부서의 과거 및 현재 행적 등을 조사한다.

(3) 추가 기술유출 방지 등을 위한 응급조치 실시

- 영업비밀 침해를 자체적 확인결과 침해가 탐지되었거나 추가 침해가 예상 되는 경우 응급조치를 취해 추가 피해를 방지한다.

※내부직원 등이 접근할 수 있는 중요 문서, 파일 등을 즉각 회수하여 추가 유출 방지한다.

- 외부 직원 및 네트워크에 의한 기술유출일 경우에는 회사 내부접근 및 네트워크 접속 등을 차단한다.

(4) 침해사실 입증을 위한 증거확보

- 침해 현장상황 및 컴퓨터 하드디스크 등 관련 물품은 그대로 보존하고 사진·비디오, 진술서 등을 신속히 확보한다.

- 증거 신빙성을 위해 주체, 일시, 장소, 증거확보 경위 등도 포함해야 하고 진술서·확인서에는 본인 및 제3자의 서명도 필요하다.

※이러한 증거확보는 형사적 및 민사적 법적구제를 받기 위해 반드시 필요한 조치이다.

(5) 기술유출 침해에 대한 대응방법

- 중소기업의 기술유출에 대한 대응방안은 당사자간 합의에 의한 방법과 법적 구제방법이 있다.

- 결정방법은 기업내부의 의사과정을 통해 합리적으로 결정한다.

[당사자간 합의에 의한 방법]

- 중소기업 핵심기술 유출로 인한 피해가 경미하거나 핵심기술 유출을 외부로 알리고 싶지 않을 때 당사자 간 합의에 의해 해결
- 막대한 법률비용 및 소송에 소요되는 시간을 절약할 수 있는 장점을 가지고 있으며, 기술을 유출당한 회사의 이미지 손상을 막을 수 있음

• 기술분쟁, '조정'하고 '중재'로 해결

- 조정은 당사자간 합의유도를 통해 재판상 화해의 효력이 있으며, 중재는 중재부의 중재판정을 통해 법원의 확정판결과 동일한 효력 발생
- 중소기업 기술분쟁을 위한 조정 및 중재는 대·중소기업협력재단에서 제공
- 조정은 조정부 구성 후 3개월, 중재는 중재부 구성 후 5개월 내에 이루어지므로 신속·저렴·전문성 있게 분쟁을 해결

[법적 구제조치]

- 기술유출 상대방과 합의가 이루어지지 않은 경우, 법적 구제조치가 필요하며, 소송에 따른 비용적·시간적 손실이 발생할 수 있음
- 다만, 기술유출에 대해 당사자 간 합의나 조정·중재로 해결하지 않고 소송을 통해 구제받기로 결정한 경우, 법적 조치에 착수하였다는 사실을 일정 시점까지는 상대방 및 피해회사의 제한된 사람 외에는 알려서는 안됨. 영업비밀 사건의 경우 수사단계에서 압수수색을 통해 증거를 확보하는 것이 관건이므로, 압수수색이 완료되기 전에 수사 중이라는 사실이 알려질 경우 증거를 인멸할 위험이 있기 때문이다.
- 영업비밀 사건은 일반 경찰이 아니라 산업기술유출수사대(전국 8곳 즉, 서울·부산·대구·인천·울산·경기·충북·경남에 있음)에 고소하는 것이 적절하다.
- 또한 재판은 공개가 원칙임에 따라 소송을 통해 영업비밀 등의 핵심 기술이 공개될 가능성도 있음을 감안한다.
- 법적 구제 시, 기술을 유출당한 기업은 유출기술에 대한 개발 및 보유 사실에 대한 입증 필요하다.
- 기술임치제도를 이용하면 해당 기술에 대한 개발사실에 대해 법적으로 입증할 수 있다.

• 기술자료 임치제도

- 중소기업은 핵심기술 정보를 제3의 신뢰성 있는 기관인 대·중소기업협력재단에 안전하게 보관하고 기술 유출이 발생하였을 경우 임치된 기술자료를 이용하여 해당 기술의 보유 사실을 입증할 수 있다. 또한 중소기업과 함께 기술자료 임치제도를 이용한 대기업 등 거래기업은 중소기업이 폐업, 파산 등을 한 경우 기술자료를 교부받아 지속적인 유지보수 및 안정적인 사용이 가능하다.
- 임치의 대상은 생산방법, 설계도, 매뉴얼 등 기술상의 정보와 재무, 회계, 원가, 각종 보고서 등 경영정보를 포함한다.
- ※ 자세한 내용은 제6장 제2절 '중소기업기술보호 관련 지원제도' 참조

제3절

기술 유출 및 침해의 유형별 사례와 대응방안

1. 인력유출을 통한 기술유출

(1) 대기업으로의 이직

• 핵심인력이 순차로 대기업으로 이직한 사례

- 피해회사 A의 연구소와 고객지원과에 근무하던 과장 및 주임급 등 핵심인력 6명이 퇴사한 후 대기업 B로 순차 이직하여, A사의 연구조직이 붕괴되고, 영업상 비밀자료 등이 유출되어, 대기업 B사에서 A사의 거래처에 A사의 제품을 배제하도록 강요하는 등 막대한 영업 손실이 발생한 사례

▶ 기업유형

- 제조업

▶ 유출대상

- 핵심인력(연구소 소속)

▶ 유출방법

- 스카우트

▶ 조치사항

- 공정거래위원회에 신고하였으나, 대기업의 인력채용은 정상적인 채용절차이고 부당한 기술·인력 유출에 해당하지 않는 것으로 판단

▶ 대응방안

- 이직·창업의 주요한 동기가 경제적 사유이므로 '내일채움 공제'⁵⁾를 활용하여 임직원에게 대한 경제적 보상을 강화하여 중소기업 근로자의 장기 재직을 유도하고 기업에 대한 애사심을 높이는 방안을 고려해야 한다.

5) 내일채움공제 홈페이지(<https://www.sbcplan.or.kr>) 참조.

- 부정경쟁방지법 제10조에 따라 경업금지(전직금지)를 청구하는 경우에는 영업비밀성이 인정되어야 하고, 공정거래위원회의 불공정거래행위 중 ‘인력의 부당 유인·채용’에 해당하기 위해서는 인력을 부당 유인 채용하여 사업 활동이 심히 곤란하게 되어야 하는데, ‘사업 활동이 심히 곤란하게 된 경우’란 단순히 매출액이 감소되었다는 사실만으로는 부족하며 부도발생 우려, 매출액의 상당한 감소, 거래상대방의 감소 등으로 인해 현재 또는 미래의 사업 활동이 현저히 곤란하게 되거나 될 가능성이 있는 경우를 말하므로 요건 성립이 매우 까다롭다.
- 경업금지(전직금지) 약정을 체결한 경우, 영업비밀에 이르지 않더라도 피해회사만이 가지고 있는 지식이나 정보로서 제3자에게 누설하지 않기로 한 것이라면 보호할 가치 있는 사용자(피해회사)의 이익이 인정되므로, 재직 시 및 퇴사 시 경업금지(전직금지) 약정을 체결하는 것이 바람직하다.
- 다만, 경업금지약정이 항상 유효한 것은 아니므로, 약정서 체결시 회사의 중요한 정보자산에 대한 구체적 기재, 가능한 한 대가를 지급하며, 중요한 정보자산에 대해 기술보호노력을 기울이는 등의 조치로 경업금지약정서의 유효 가능성을 높이는 것이 바람직하다.

(2) 경쟁 중소기업으로의 이직

• 경쟁사로 이직하면서 기술자료를 무단 유출하여 이용한 사례

- 히터 제조기술을 보유한 A사에 재직하던 갑과 을이 퇴사 후 경쟁사인 B사로 이직한 후, A사에서 취득한 기술자료를 바탕으로 동일 제품을 제조하고, A사의 고객사에게 접근하여 판매하자, 형사 고소하였으나, 증거불충분으로 무죄가 선고된 사례

▶ 기업유형

- 제조업

▶ 유출대상

- 핵심인력, 히터 제조기술, 거래처 목록, 단가 등

▶ 유출방법

- 스카우트, 퇴사 시 무단반출

▶ 조치사항

- B사, 갑, 을을 부정경쟁방지법 위반으로 형사 고소하였으나, 법원은 A사가 기술정보와 경영정보를 비밀로 유지하기 위한 기술보호 노력을 하였다고 보기 어려워 영업 비밀에 해당한다고 보기 어렵다고 하면서 무죄를 선고.

▶ 대응방안

- 스카우트의 경우, 단순한 핵심인력의 전직을 넘어서서, 정보자산에 대한 무단유출 및 이직자가 담당하던 거래처를 찬탈당하는 일이 함께 발생하는 경향이 있으므로 피해가 확산된다.
- 영업비밀(기술정보, 경영정보)로 인정받기 위해서는 경제적 가치가 있고 공지되지 않은 정보라는 점만으로는 부족하고, 이러한 정보를 지키기 위해 회사에서 합리적인 기술보호 노력을 기울였다는 것이 인정되어야 한다.
- 따라서 영업비밀로 지켜야 하는 기술정보와 경영정보가 무엇인지 구체적으로 파악하고, 이에 대하여 대외비 표시, 접근권한 제한, 출입통제 등의 실질적이고 성실한 보안조치를 하고, 보안서약서나 전직금지약정서 등 각종 서약서에 이러한 영업비밀의 종류를 구체적으로 기재하는 것이 필요하다.

(3) 경쟁업체 창업

• 퇴사하면서 기술정보와 경영정보를 무단반출하고 경쟁사를 설립한 후 거래처를 찬탈한 사례

- 건설장비업을 영위하는 피해회사 A에서 연구소 실장으로 근무하던 갑과 연구소 연구원으로 근무하던 을과 병이 퇴사한 후 경쟁사 B를 설립하고, 무단 반출한 A사의 설계도면, 설계계산시트, 단가정보 등을 이용하여 유사품을 제작하고 납품하자, 형사 고소 및 민사소송을 제기한 사례

▶ 기업유형

- 건설장비 제조·판매업

▶ 유출대상

- 기술정보(건설장비 제작에 필요한 설계도면, 설계계산시트), 경영정보(A사의 매입처 정보, 매입단가추이정보, 수주 매출 분석, 수주 목표, 수주 전력 자료 등)

▶ 유출방법

- 회사에서 지급한 노트북을 퇴사 시 반납하지 않았으며, 외장형 하드 디스크에 복사하여 반출, A사에 재직 중인 직원으로부터 경영정보를 받음

▶ 조치사항

- 민사상 영업비밀 침해금지 가처분을 제기하였으나, 실제 기울인 기술보호 노력 관련 증거를 전부 다 제출하지 않고, 기술보호 노력의 증거로 보안서약서만 제출하였으므로 영업비밀로 인정되지 않아서 가처분 신청이 기각됨

- 산업기술유출수사대에 갑, 을, 병, B사를 고소하였는데, 무단 반출한 기술정보와 경영정보가 경제적 가치 및 비공지성은 인정되나 기술보호성은 인정되지 않는다는 이유로 부정경쟁방지법상 영업비밀 침해죄는 불기소처분이 내려지고, 형법상 업무상 배임으로만 기소되고 유죄판결이 선고됨
- 민사 본안소송으로 영업비밀 침해금지 및 손해배상 청구 소송을 하였는데, 기술보호성이 부정되어 영업비밀로 인정되지 않았고, 형사상 업무상 배임에 해당하므로 민사상 불법행위가 성립하여 B사가 무단 유출한 자료를 이용해 얻은 수익에 대해 손해배상을 받음

▶ 대응방안

- 퇴사 시 회사에서 지급한 업무상 노트북 등 회수를 철저히 해야 한다.
- 하나의 사건에 대해 형사고소, 민사 가처분, 민사 본안소송 등 수개를 진행하는 경우, 제일 먼저 내려진 결정이 다른 재판에도 영향을 줄 수 있으므로, 각 수사/재판 마다 증거의 성실한 제출과 충분한 법리 주장이 필요하다.
- 기술보호 노력을 기울이는 것도 중요하나, 기술보호에 대한 증거를 평소에 확보해두며(각종 서약서, CCTV 등 물리적 통제 관련 계약서와 사진, 보안솔루션 도입 시 관련 계약서 등 자료, 보안교육 시 촬영한 사진 및 참가자 서명자료, 보안을 독려한 내용으로 보낸 이메일, 영업비밀 관리규정 등), 소송에서 증거를 처음부터 성실히 제출하는 것이 필요하다.

2. 거래관계에서의 기술유출

(1) 대기업과의 거래

• 계약체결 협상 단계에서 제공한 기술 자료를 무단 이용한 사례

- 중소기업 A사는 개발한 특허기술의 상품화를 위해 대기업 B사에 자료를 송부, 이후 B사가 유사기술을 탑재한 휴대폰을 출시하자 A사가 형사고소 및 민사 소송을 제기하였으나 모두 패소한 사례

▶ 기업유형

- 소프트웨어 개발

▶ 유출대상

- 휴대폰 관련 기술

▶ 유출방법

- 계약체결을 위한 협상 단계에서 제공받은 기술자료 이용

▶ 조치사항

- A사는 특허법 위반으로 형사고소 및 민사 소송을 제기하였으나 모두 패소하여 막대한 피해가 발생.

▶ 대응방안

- 대기업으로부터 투자를 받거나 제품 납품 등의 계약 체결을 하기 전에, 대기업에게 기술정보를 제공하였다가 투자나 계약체결이 무산되는 사례가 빈번하므로, 이에 대한 대비가 필요하다.
- 대기업에게 기술정보를 제공하기 이전에, 제품이 출시되면 노출이 되는 기술정보의 경우에는 특허/실용신안 출원을 미리 해두는 것이 바람직하며, 영업비밀로 보유할 기술정보의 경우에는 미리 기술자료임치⁶⁾나 영업비밀 원본 증명⁷⁾을 받아두는 것이 바람직하다.
- 대기업에게 제공하는 기술정보는 최소한으로 하며, 기술에 대한 설명회나 발표회를 하는 경우에도 인쇄물이나 파일 형태의 기술 자료를 제공하는 것을 지양하는 것이 바람직하다.
- 대기업 측에서 기술정보를 요청하는 경우, 요청하는 기술자료, 요청사유, 이용목적이 무엇인지 등에 대해 이메일, 문자, 녹취 등 객관적인 증빙이 가능한 형태로 남겨두는 것이 바람직하다.
- 부득이 기술 자료를 제공해야 하는 경우에는 제공 전에, 비밀유지계약 (①제공하는 기술자료 명칭, ② 이용목적이 한정된다는 점, ③ 중소기업의 사전 서면동의 없이 사용이나 누설 금지, ④ 계약이 체결되지 않는 경우 반납 및 완전 삭제, ⑤ 제공한 기술정보에 적용·포함된 기술, 노하우 등을 변형·수정하여 기술을 개발하는데 사용할 수 없음 ⑥ 이를 위반한 경우 위약벌이나 손해배상예정 조항 등)을 체결하는 것이 바람직하며, 기술자료 제공은 이메일 첨부 등 제공하였음이 객관적으로 드러나는 방식으로 하는 것이 바람직하며, 인쇄물을 건네는 등의 입증이 어려운 방식은 부적절하다.

6) 기술자료임치센터 홈페이지(<http://www.kescrow.or.kr/index.html>) 참조

7) 영업비밀보호센터의 원본증명제도 소개 사이트(<https://www.tradesecret.or.kr/kipi/web/serviceIntro.do>)참조

(2) 중소기업과의 거래

• 거래처가 복제품을 만들어 손해가 발생한 사례

- 촬영기기 제조사인 A사는 거래처 B사와 거래 중 매출액이 감소하여 확인해본 결과, B사에서 A사 제품을 복제하여 판매하는 것을 확인하였으나, HW 부분은 제품을 통해 복제한 것으로 추정되나 A사가 특허 등을 등록하지 않았고, SW 부분은 내부자의 기술유출에 의한 것으로 의심되나 증거가 없어서 피해 보상을 받지 못한 사례

▶ 기업유형

- 제조업

▶ 유출대상

- 촬영기기 제조기술

▶ 유출방법

- H/W 모방, S/W는 내부자 유출로 의심

▶ 조치사항

- 없음

▶ 대응방안

- 기술정보 중 완제품으로부터 파악이 가능한 것(기계 작동원리 등)은 특허/실용신안으로 등록하여 권리확보를 하고, 외형의 경우 디자인 등록을 하여 권리확보를 하는 것이 필요하다.
- 소스코드, 제작도면, 회로도, 공정노하우 등 비밀로 보유할 기술정보는 영업비밀 원본 증명제도나 기술자료임치제도를 이용하여 해당시점에 기술을 보유하고 있었다는 점에 대한 증빙을 확보해 두는 것이 바람직하며, 유출방지를 위해 합리적 기술 보호를 기울이는 것이 필요하다.
- 거래처와의 계약서에, ① 제공하는 기술정보와 경영정보에 대한 비밀유지조항, ② 거래제품을 사전 서면 동의 없이 무단복제하지 않고, ③ 거래제품에 적용·사용된 기술, 노하우 등을 수정, 역설계(reverse engineering), 디컴파일(decompile) 또는 디스어셈블(disassemble) 할 수 없고, 새로운 또는 변형 기술을 개발하는데 사용할 수 없다는 취지의 내용, ④ 이를 위반한 경우 위약벌이나 손해배상 관련 조항 등을 포함하도록 하는 것이 필요하다.

(3) 협력업체에 의한 유출

• 외주협력사가 피해회사로부터 제공받은 소스코드와 개발 산출물을 다른 경쟁사를 위해 사용한 사례

- 피해회사 A는 휴대전화를 개발하여 미국의 통신 사업자에게 납품하는 등의 사업을 하는 회사이고, B사는 피해회사의 외주용역 회사로서 휴대전화의 일부 소프트웨어 개발에 참여하였음. 피해회사의 지사장과 연구소장을 하다 퇴직한 갑과 피해회사의 기구설계 담당자로 근무하다 퇴사한 을이 경쟁사인 C사를 설립하고, 미국 통신 사업자에 납품할 휴대폰 제조를 B사에게 외주로 맡겼고, B사는 피해회사와의 용역계약 당시 취득한 소스코드를 이용하여 휴대폰을 제작, 판매한 사례

▶ 기업유형

- 제조업

▶ 유출대상

- 휴대전화에 사용되는 어플리케이션과 플랫폼 소스코드

▶ 유출방법

- 외주 개발 용역 시 제공받은 소스코드와 용역수행으로 개발한 소스코드를 무단복제

▶ 조치사항

- 산업기술유출수사대에 갑, 을, 주식회사 C, 주식회사 B, B사의 사장과 부사장을 고소하였고, 압수 수색결과 피해회사의 소스코드를 무단 복제한 소스코드가 발견되었으며, 형사재판에서 B사와 B사의 사장과 부사장에 대해서는 유죄가, 나머지 피고인에 대해서는 무죄가 선고.

- 민사소송으로 손해배상을 청구하였고, 갑, 을에게 과실은 인정되어 갑, 을, C사 및 B사, B사의 사장, 부사장이 연대하여 수 억원을 배상하라는 판결이 선고.

▶ 대응방안

- 외주협력업체는 피해회사의 동종회사들과 거래하므로 침해가능성이 매우 높으므로, 외주협력업체에 대한 기술 보호도 중요하다.
- 외주협력업체와 사전에 비밀유지계약을 체결하고, 제공한 자료 및 용역수행 결과물의 소유권이 피해회사에게 있다는 점도 계약서에 명시하며, 용역수행이나 계약수행에 필요한 최소한의 자료만 제공하고, 계약종료 후에는 무단반출하거나 복제한 자료가 있는지에 대해 점검하고 피해회사의 시스템에 대한 접근권한을 철회하여야 한다.

3. 해외 기술유출

(1) 사례 1

• 퇴사자가 중국인의 제안으로 설계도면 등을 유출하고 기술지도한 사례

- 피해회사 A에서 설계팀 과장으로 근무하던 갑이 퇴사 시 설계도면 등 기술자료 일체를 USB에 저장하여 반출한 후, 중국인 을로부터 위 기술 자료를 이용하여 복제품을 제작하여 중국에서 판매해보자는 제안을 받고, 을에게 위 기술자료 일체가 저장된 노트북을 주고, 중국에 가서 기술지도를 하며, 그 대가로 수 천 만원을 지급받았으나, 복제품 개발에 실패하자, 중국인 을이 앙심을 품고 A사에게 범행을 알려준 사례

▶ 기업유형

- 제조업

▶ 유출대상

- 기계 제작도면 일체 및 기계 제작 노하우

▶ 유출방법

- USB에 저장하여 반출, 외국인에게 기술지도

▶ 조치사항

- 산업기술유출수사대에 고소하였고, 중국인이 임의 제출한 노트북, 카톡 대화자료, 공모 및 기술지도 관련 대화내용이 담긴 녹취록 등을 기반으로 갑에 대하여 징역 10월의 실형이 선고되고, 중국인 을에 대해 기소중지처분이 내려짐

▶ 대응방안

- 소규모회사라고 하더라도, 보안서약서 징구 등 기본적인 기술보호만으로는 영업비밀의 요건인 기술보호성이 인정되지 않는 경우가 있으므로, 지켜야 할 기술정보와 경영정보에 대해 실질적인 보안조치를 기울여야 한다.
- 피해회사는 소규모 회사(15명 내외)이나 기술정보를 지키기 위해 평소에 임직원에게 보안서약서 징구, 외주업체에 대한 비밀유지협약서, 출력물 형태의 영업비밀 자료를 시정장치 있는 캐비닛에 별도 보관, 설계도면 등 기술정보의 저장매체를 최소화하고, 이동식저장장치 등 사용제한에 대해 수시로 주의, CCTV 등 물리적 보안통제 등 기술보호노력을 성실히 하였고, 그 결과 재판에서 영업비밀로 인정받았다.
- 침해사실을 인지한 직후, 신속하게 범행경위를 파악하고, 증거자료 등 관련 자료를 수집함으로써 수사과 재판에서 유리한 고지를 점하는 것이 필요하다.

(2) 사례 2

• 퇴사자가 외국 업체로 이직 후 피해회사의 웹 하드에 무단 접근하여 유출한 사례

- 피해회사에서 연구소장으로 재직하면서 회로기판 개발업무에 종사하다가, 동종 업체인 말레이시아 소재 회사에 입사하여 디스플레이 부분 연구원으로 근무하던 갑이, 피해회사가 임차한 웹 하드의 아이디와 비밀번호를 알고 있음을 기회로, 위 웹 하드에 저장되어 있던 피해회사의 피디피(PDP)티브이 제조 관련 기능소프트웨어 파일과 서비스 매뉴얼 등을 갑이 사용하는 컴퓨터 하드디스크에 다운로드한 후, 위 말레이시아 소재 회사의 티브이 개발업무에 사용한 사례

▶ 기업유형

- 제조업

▶ 유출대상

- 소프트웨어 파일, 서비스 매뉴얼

▶ 유출방법

- 피해회사의 웹 하드에, 재직 시 사용하던 ID와 PW 이용하여 접속한 후 파일 다운로드

▶ 조치사항

- 피해회사는 갑에 대하여 형사고소 하였고, 수사기관은 하드 접속자 IP 추적, 웹 하드 접속 데이터 조사, 갑의 이메일 등을 조사하여 갑의 범행을 밝혀냈으며, 검찰은 갑에 대해 영업비밀 해외유출로 인한 부정경쟁방지법위반과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」위반으로 기소하였고, 법원은 갑에 대해 징역 1년 4월 및 집행유예 3년을 선고.

▶ 대응방안

- 퇴사자의 경우, 자료반납 뿐만 아니라 퇴사자의 회사 정보자산에 대한 접근권한을 모두 철회/삭제하였는지 반드시 확인해야 한다.

4. 경영정보 유출 및 전직금지 사례

(1) 사례 1

• 호텔에서 근무하던 자가 동료들 통해 고객명단, 회사의 실적표 등을 유출하고 경쟁호텔로 전직한 사례

- 피해회사는 호텔을 영위하는 회사인데, 판촉팀에서 대리로 근무하던 갑이 퇴사하여 경쟁사 호텔로 이직하고, 퇴사 직전 같은 판촉팀의 다른 직원에게 이동식저장매체(USB)에 피해회사의 객실단가와 수량 등을 저장하게 하고, 이메일로 고객사 예약담당자 성명과 전화번호 및 객실사용금액, 피해회사의 실적 등을 갑에게 전송하도록 하여 취득한 사안.

▶ 기업유형

- 호텔업

▶ 유출대상

- 거래선 자료 및 거래선 담당자 명단, 피해회사의 실적 분석표, 주간 실적미팅 자료

▶ 유출방법

- 같은 부서의 직원을 회유하여 usb와 이메일로 정보를 취득한다.

▶ 조치사항

- 갑을 상대로 민사소송으로 영업비밀 침해금지 및 전직금지 가처분을 제기.
- 법원은, 영업비밀 침해금지 청구에 대해서, 거래선 자료 및 거래선 담당자 명단 등은 호텔업 특성상 동종업계에서 일반적으로 알 수 있는 내용이므로 영업비밀이 아니고, 피해회사의 실적표나 주간 실적미팅 자료 등은 위 자료를 별도로 비밀로 분류하여 관리하거나 접근을 차단하거나 저장매체 특성에 따른 적절한 보안책임 체계를 두는 등으로 기술 보호를 한 사실이 없으므로 영업 비밀에 해당하지 않는다고 판단함.
- 법원은 전직금지 청구에 대해서, 퇴사 후 1년간 전직금지 약정을 하였으나, 영업 비밀에도 해당하지 않고, 대리로서 지위가 낮으며, 근무기간도 2년으로 짧고, 보수도 높지 않고 전직에 대한 대가도 지급하지 점 등을 고려할 때, 전직금지약정으로 보호할 가치가 있다고 보기에 부족하다고 하여 전직금지청구도 기각.

▶ 대응방안

- 동종 업계에 알려지지 않은 비공지된 정보라고 하더라도 영업비밀로 인정되려면 기술 보호노력을 기울여야한다.
- 전직금지약정을 체결한 경우에는 영업 비밀에 해당하지 않더라도 보호할 사용자의 가치가 있는 정보가 있다면 전직금지가 인정되나, 전직금지약정은 항상 유효한 것이 아니며, 전직금지약정의 유효가능성을 높이기 위해서는, 전직금지약정서에 보호할 정보자산에 대해 구체적으로 기재하고, 이러한 정보자산에 대해 보안에 대한 노력을 하며, 전직의 대가를 지급하는 등의 조치가 필요하다.

(2) 사례 2

• 정보를 무단유출하지 않았으나, 전직금지약정을 위반하고 경쟁사로 전직한 사례

- 해충방제사업을 하는 피해회사의 주임연구원과 서비스컨설턴트로 각 근무하던 갑, 을이 5년간 전직금지약정을 체결하였는데, 피해회사에서 퇴사한 후 경쟁사로 전직하자, 피해회사가 민사소송을 제기하였고, 갑은 3년, 을은 2년의 전직금지 및 수 천만 원 손해배상과 위반 1일당 50만원을 지급하라는 판결이 선고된 사례

▶ 기업유형

- 해충방제업

▶ 유출대상

- 무단유출은 하지 않았으나, 전직금지약정을 위반하고 경쟁사로 이직

▶ 조치사항

- 피해회사는 갑, 을을 상대로 전직금지, 손해배상 및 간접강제(전직금지 위반 1일마다 특정 금액을 지급하라)를 청구.

- 법원은, 피해회사가 수 십년 간 해충방제사업을 영위하면서 다른 회사가 단기간에는 취득하기 어려운 정보와 노하우를 보유하고 있으므로 보호할 가치 있는 이익이 있고, 피해회사가 임직원들에게 연구원용, 마케팅담당용, 파트장용 등 담당업무에 따라 ‘영업비밀 보유확인서’를 징구하였음. 위 영업비밀 보유확인서에는 영업비밀의 내용이 구체적으로 기재되어 있으며, 전직금지약정을 체결하고, 영업비밀 보호장려금을 지급하고 이에 대한 지급동의서를 징구한 사실 등을 고려하여 전직금지약정을 유효로 판단.

- 다만, 법원은 약정한 5년은 과도하게 장기라고 인정되므로 전직금지 기간을 갑은 3년, 을은 2년으로 제한하였고, 전직금지 1일당 50만원을 지급하며, 피해회사가 갑, 을과 체결해 둔 손해배상에정액 일부를 배상하도록 함.

▶ 시사점

- 회사의 보호할 가치 있는 정보가 무엇인지 구체적으로 파악하고, 전직금지약정서나 영업비밀 보유확인서 등을 징구할 때 위 정보가 무엇인지 구체적으로 기재하며, 전직금지의 대가를 지급하는 등의 조치를 하여 전직금지약정의 유효 가능성을 높이는 것이 필요하다.

제4절

판례를 통해 살펴 본 “기술보호 노력”의 의미와 정도

1. 기술보호 노력의 의미와 정도

(1) 합리적 기술 보호노력

- 중소기업기술을 부정경쟁방지법 영업비밀로 보호하기 위해서는 비공지성(비밀성), 경제적 유용성, 비밀관리성을 갖추어야 한다. ‘비밀관리성’ 요건과 관련하여 과거 “상당한 기술보호노력”을 요하던 것을 2015. 1. 28.부터 시행되는 개정 부정경쟁 방지법에서는 “합리적 기술보호노력”으로 완화하였다. 동법의 개정이유는 핵심기술을 유출당하고도 엄격한 비밀관리성 요건을 충족하지 못하여 구제를 받지 못하는 중소기업을 보호하기 위해서이다.
- “합리적 기술보호노력” 요건은, 충족되기 위한 명확한 기준이 있는 것이 아니라 불확정 개념이며, 기업의 규모, 자금력 등에 비추어 해당 기업이 기울인 관리적·물리적·기술적 보안조치를 종합적으로 고려할 때 합리적 기술보호를 기울인 것으로 볼 수 있는지를 상대적으로 판단하는 것이다.
- 그러나 “합리적 기술보호노력”은 불확정 개념이자 상대적으로 판단하는 것이므로 그 구체적인 내용은 결국 판례를 통해 형성될 수밖에 없다.
- 다양한 판례를 통해 법원이 기술보호노력 요건과 관련하여 판단하는 요소가 무엇이며, 영업비밀 유형별로 어떠한 조치를 취하여야 하는지 파악하여, 보안정책에 반영하는 것이 필요하다.

(2) 기술보호 노력이 인정되지 않는 경우

- 기술보호 노력이 인정되지 않는 경우에도, ‘불특정 다수의 사람에게 공개되지 않았고(비공지성), 사용자가 상당한 시간, 노력 및 비용을 들여 제작한(경제적 유용성) 영업상 주요한 자산’을, 근로자가 경쟁업체에 유출하거나 근로자 스스로의 이익을 위해 반납 또는 폐기하지 않는 경우, 형사상 업무상 배임에 해당하며, 민사상 불법행위에 해당한다.

• 대법원 2009. 10. 15. 선고 2008도9433 판결

- 영업비밀이 아니더라도 그 자료가 불특정 다수의 사람에게 공개되지 않았고 사용자가 상당한 시간, 노력 및 비용을 들여 제작한 영업상 주요한 자산인 경우에도 그 자료의 반출행위는 업무상배임죄를 구성하며, 회사 직원이 영업비밀이나 영업상 주요한 자산인 자료를 적법하게 반출하여 그 반출행위가 업무상배임죄에 해당하지 않는 경우라도 퇴사시에 그 영업비밀 등을 회사에 반환하거나 폐기할 의무가 있음에도 경쟁업체에 유출하거나 스스로의 이익을 위하여 이용할 목적으로 이를 반환하거나 폐기하지 아니하였다면, 이러한 행위는 업무상배임죄에 해당한다.

2. 기술보호의 구체적 방법과 정도

- 이하에서는, 기술보호 노력의 구체적인 방법과 정도에 대한 판례를 소개하고, 보안정책 수립시 반영할 내용을 안내한다.

(1) 회사의 일반정보와 영업 비밀을 구분할 것

- 일반적인 보안조치 뿐만 아니라, “회사가 영업비밀이라고 주장하는 정보자산에 대해” 실질적인 보안조치를 하는 것이 바람직하므로, 우선적으로 회사의 각종 자료와 정보 중 영업 비밀에 해당하는 것이 무엇인지 구체적으로 파악하는 것이 선행되어야 하며, 영업 비밀에 해당하는 정보자산에 대해 영업비밀 특성 등에 따라 구체적으로 어떠한 보안조치를 기울일 것인지 고려하여 보안정책 수립에 반영하는 것이 필요하다.
- 영업비밀을 목록으로 만들어 놓는 것이 바람직하다.
- 소규모 기업이라 하더라도, 비밀유지서약서 징구 등 기초적인 조치만으로는 기술보호노력 요건이 인정되지 않을 가능성이 높으므로 주의가 필요하다.

• 대전지방법원 천안지원 2011. 2. 17. 선고 2009고단1312

- 피해자 회사는 이 사건 공소사실에 영업비밀로 적시된 거래처 연락처, 제품의 도면, 수주 및 납품 현황, 품목별 다가현황 등의 정보를 일반적인 경영정보와 별도의 영업비밀로 분류하지 않았을 뿐만 아니라 그 정보의 비밀을 유지에 필요한 구체적인 보안장치나 규정도 전혀 두지 않았고, 위 정보는 피해자 회사의 사무실에 설치된 피고인이 사용하던 컴퓨터에 파일로 저장되어 있었는데 누구든지 컴퓨터를 켜고 그 파일을 열람하거나 복사할 수 있었던 것으로 보이며, 모든 관리직원들은 근거리통신망(LAN)으로 연결된 자신의 컴퓨터를 통해 별도의 비밀번호나 아이디를 입력할 필요없이 위 정보가 수록된 파일에 자유로이 접근하여 열람, 복사할 수 있었고 복사된 저장매체도 언제든지 반출할 수 있었다. (중략) 피해자 회사가 소규모 회사라는 점을 고려하더라도 영업비밀에 해당하지 않는다.

(2) 영업 비밀임을 표시·고지할 것

- 설계도면이나 회로도 등 영업 비밀에 기밀, 대외비, confidential 등 영업 비밀임을 표시하는 것이 필요하다.
- 영업비밀 표시를 함으로써, 직원이나 외부인이 해당 자료를 취득하여 반출하려는 경우 회사의 영업 비밀임을 안다면 반출을 스스로 중단할 수도 있으며, 설령 유출되더라도 영업 비밀임을 인정받는데 도움이 된다.
- 각종 보안서약서 징구, 보안교육 실시 등을 통해 영업 비밀을 고지하는 것이 바람직하다. 보안교육은 보안담당자가 실시, 외부 보안전문가 초빙, 온라인 형식의 교육 등 회사의 사정과 실시 당시 사정에 따라 다양하게 이루어질 수 있다.

• 서울남부지방법원 2008. 11. 6. 선고 2008고단1591 판결

- 예상 거래처의 구매의사, 사업주관 기관, 책정예산, 입찰정보, 사업가능성 등 자료들이 비밀로 표시되었다거나 피고인들에게 비밀이라고 고지를 하였거나 피고인들에게 비밀 준수 의무를 부과하였다는 사실을 인정할 아무런 증거가 없는 바, 비록 피해회사가 피고인들을 포함하여 총 4~5명으로 구성된 소규모 회사라 하더라도 피해회사가 위 자료들을 비밀로 유지하기 위하여 상당한 노력(구법상 요건)을 다하였다고 볼 수 없다.

(3) 접근가능성 있는 자에게 영업비밀 보호 의무를 부과할 것

- 임직원에게 대한 각종 보안서약서 징구하거나 외주업체와 비밀유지계약을 체결할 때, 단순히 영업 비밀을 누설하지 않겠다는 일반적인 내용보다는 영업 비밀에 대한 구체적인 기재(예 : 000에 관한 기술정보, 설계도면, 회로도, 배합비율, 00 관련 단가정보, 고객입찰정보)를 하는 것이 바람직하다.
- 입사 시 뿐만 아니라 재직기간동안 이벤트(연봉협상 시, 보직변경 시, 주요 프로젝트 수행 시 등) 등을 활용하여 보안서약서를 추가로 징구하는 것이 바람직하다.
- 영업 비밀을 회사가 지정한 장소(매체)가 아닌 다른 장소(매체)로 이동하는 경우(예: 출장 등의 경우에 노트북이나 이동식 저장매체 사용), 이에 대한 승인절차를 만들고, 별도의 보안서약서를 징구하는 것이 바람직하다.

- 퇴사하는 경우에도 보안서약서를 징구하고, 퇴사 직원이 사용하던 컴퓨터 하드디스크 포맷, 이동식 저장장치를 통해 이미 반출한 경우 삭제 또는 폐기처분하도록 하고 이를 확인할 수 있는 자료를 제출하도록 요구하는 것이 바람직하다.
- 거래업체, 공동작업, 업무 협의를 위해 회사를 방문하는 직원 등과 사전에 비밀유지계약을 체결하거나 보안서약서를 징구하는 것이 바람직하다.

• 의정부지방법원 2011. 9. 8. 선고 2009가합7325 판결

- 원고가 000을 포함한 원고 업체의 전 직원들로부터 이 사건 기술정보 등 영업비밀 준수에 관한 서약서(특히 위 서약서는 일반적인 비밀유지의무만을 담고 있는 것이 아니라, ***에 관한 일체의 영업비밀 사항을 누설하지 않겠다는 내용으로 특정되어 있었다)를 징구하는 한편, 그 기술정보를 엄격하게 관리하는 등 이를 비밀로 유지, 관리하여 온 점..(중략).. 등을 종합하여 보면, 이 사건 기술정보는 부정경쟁방지법 제2조 제2호 소정의 **영업비밀에 해당**한다.

• 대구지방법원 2012. 7. 19. 선고 2012고단470 판결

- 이 사건 자료들이 저장되어 있던 피해회사의 외장형 하드디스크에는 권한 있는 특정인에게만 부여하는 비밀번호 설정 등 대상자나 접근방법을 제한하는 어떠한 조치도 이루어지지 아니한 사실, 이 사건 자료들에는 대외비 표시 또는 기밀 자료 표시 등 비밀임을 나타내는 표시가 전혀 되어 있지 아니한 사실, 피해회사가 이 사건 자료들의 비밀유지에 관한 보안교육을 따로 실시한 바 없다는 점이 인정되고, **피고인은 피해회사에 재직할 당시 '회사의 영업 비밀에 대하여 대내 외는 물론 타인에게 결코 유출하거나 사용하지 않겠음'이라는 취지의 내용이 포함된 일반적인 보안서약서를 작성한 외에 별도로 이 사건 자료들에 대한 비밀을 유지하겠다는 비밀유지 각서를 작성한 사실이 없는 점** 등을 종합하여 보면, 이 사건 자료들이 **피해회사의 영업상 비밀에 해당한다고 단정하기 어렵고**, 달리 이를 인정할 증거가 없다.

(4) 보안규정을 제정·시행하고, 보안담당자를 지정할 것

- 회사의 보안에 대한 전반적인 사항(회사의 영업비밀 지정, 영업비밀 보관 장소 및 매체, 접근권한, 보안담당자, 보안사고 발생 시 대응 및 징계 절차 등)을 담은 보안규정을 제정하며, 제정에 그치지 않고 이를 실제로 시행하는 것이 바람직하다.
- 회사의 영업 비밀을 구분하고, 이를 체계적으로 관리하는 등 보안을 담당하는 사람을 지정하여 영업비밀 관리의 지속성과 전문성을 확보할 수 있음. 다만, 보안만 담당하는 직원을 별도로 두는 것은 적지 않은 비용이 필요하므로, 기업의 규모, 기업의 경제적 여건, 통제구역의 크기 등을 고려하여 다른 업무와 병행해서 보안을 담당하도록 하는 것도 가능하며, 총체적인 보안을 담당하는 자 이외에 각 부서별로 보안담당자를 두는 것도 방법도 효과적이다.

• 서울중앙지방법원 2011. 11. 30. 선고 2011노2694 판결

- 고소인 회사의 연구소에서는, 연구원들이 각자 담당하는 분야에 대한 개발과정에서 파일들을 고소인 회사에서 지급한 개인 PC에 보관하고, 연구개발이 끝나면 결과물을 중앙서버에 전송하여 보관한 사실, 고소인 회사는 2000. 7. 2. 기술보호 규정을 제정하였으나, 연구소 소속 직원들을 상대로 보안교육을 실시한 적은 없는 사실(고소인 회사의 총무 팀장이었던 000도 원심 법정에서 “고소인 회사에서 기술보호가 제대로 되고 있지 않았고, 보안담당책임자도 없었던 것으로 알고 있다”고 진술하였다), 고소인 회사에서는 당시 연구원들에 대하여 USB 등 개인 저장장치에 대해 제한을 가한 적이 없었고, 피고인의 입사 및 퇴사 시에도 피고인으로부터 보안서약서를 징구한 적도 없는 사실은 인정할 수 있다. 이를 종합하면, 고소인 회사가 기술보호규정을 제정하고 보안출입통제시스템을 운영하였으며 복도에 CCTV를 설치해 두었다는 점만으로는, 고소인 회사가 이 사건 파일 등을 상당한 노력을 들여 비밀로 관리하였다거나 객관적으로 이 사건 파일 등이 비밀로 유지 관리되고 있음이 인식 가능한 상태에 있었다고 보기 어렵고, 그밖에 이를 인정할 만한 증거가 없다.

(5) 영업 비밀을 정해진 장소(매체)에 보관하고, 이동을 원칙적으로 금지할 것

- 영업 비밀은 파일 등 데이터 형태와 출력물 형태로 존재하는데, 데이터 형태의 경우 서버나 회사가 지정한 컴퓨터 등 정해진 장소(매체)에만 보관하도록 한다.
- 출력물 형태의 경우, 책꽂이 등에 꽂아두는 등 누구나 열람할 수 있는 장소에 보관하여서는 안되고, 시정장치가 있는 별도의 캐비닛 등에 보관하도록 하고 보관 담당자를 지정하며, 출력물이 제대로 회수가 되는지(예: 설계도면을 생산 팀에서 사용한 후 회수, 배합비율이 기재된 작업 지시서를 생산 팀에서 사용한 후 회수)를 관리대장 등을 통해 관리하는 것이 바람직하다.
- 업무수행 과정에서 부득이 영업 비밀을 서버나 지정된 회사 컴퓨터 외의 컴퓨터에 보관하는 경우, 회사의 승인을 얻도록 하고(승인절차를 보안규정에 두며, 승인문서를 남기는 것이 적절하다.) 이에 대한 별도의 보안서약서를 징구하는 것이 바람직하다.
- 저장매체 반출은 금지시키되, 불가피한 경우에는 회사의 승인을 얻도록 하고 (승인절차를 보안규정에 두며, 승인문서를 남기는 것이 적절하다.) 이에 대한 별도의 보안서약서를 징구하는 것이 바람직하다.
- 임직원들이 상용 클라우드(예: N드라이브) 등 회사에서 지정한 매체가 아닌 매체에 영업비밀을 저장하는지 등에 대해 보안담당자 등이 주기적으로 점검하는 것이 바람직하다.

- 영업 비밀을 불필요하게 복사하거나 출력하는 것을 금지시키고, 이메일 전송을 통제하거나, 문서 출력 시 사용자 정보도 같이 출력되거나 프린터 내부적으로 출력 정보를 저장하는 시스템을 도입하는 것도 고려할 필요가 있으며, 시스템 도입이 어려운 경우, 위와 같은 복사/출력/전송 금지를 보안 규정에 두고, 보안서약서에도 관련 내용을 두며, 보안교육 및 수시 보안점검을 통해 불필요한 복사/출력/전송이 이루어지지 않도록 독려하는 것이 바람직하다.

• 부산지방법원 2009. 8. 13. 선고 2009노1314 판결

- 피해회사는 기술 자료의 비밀유지를 위하여 보안규정을 제정하고, 회사 내에 별도의 금속기술연구소를 설치하고 이를 통제구역으로 지정하여 관계자 이외에는 연구소에 출입할 수 없도록 하는 한편, 기술 자료가 담긴 컴퓨터 파일들을 연구소의 주 컴퓨터(이하 '메인 컴퓨터')와 보안책임자인 연구개발팀장의 컴퓨터에 저장하고, 메인 컴퓨터에 보안을 위하여 아이디와 비밀번호를 설정하였으며, 피해회사의 임직원들 중 연구소 직원들에게만 그 아이디와 비밀번호를 알려주어 위 메인 컴퓨터의 파일에 접근하여 이를 사용할 수 있도록 하고, 사내 네트워크로 메인 컴퓨터에 접속하더라도 공유로 설정된 자료만을 열람할 수 있으며, 기술 자료들을 열람하기 위해서는 아이디와 비밀번호를 입력하여야 한다. 또한 기술 자료인 각종 도면의 경우, 캐드(CAD)로 만들어진 도면 파일은 보안책임자 컴퓨터에 보관되고, 원본 도면은 연구소 내에 있는 지정 캐비닛에 보관, 관리되며, 도면이 필요한 임직원에게는 그 도면의 사본이 교부되는 데, 이때 보안책임자가 피교부자의 성명, 해당 부서명, 출도, 용도 등을 도면배포 관리대장에 기재한 다음에 이를 교부하고 사후에 이를 회수하는 것을 원칙으로 하고 있다. 그리고 작업표준서 등은 연구소 품질보증부에서 보관하고, 해당 사업부서에서 그 사본을 배포하여 해당 공정 작업장에서 그 사본을 참조하여 작업하도록 하고 있다. 또한 피해회사는 자재소요 현황자료, 원가분석자료, 매출 관련자료 등 영업자료의 비밀유지를 위하여, 위와 같은 영업자료 관련 업무를 담당하는 직원에게만 위 영업자료가 저장되는 컴퓨터의 아이디와 비밀번호를 부여하고, 임직원 중 영업 업무에 종사하는 제한된 임직원만이 이를 활용할 수 있도록 하고 있으며, 영업자료가 기재된 문서들은 지정 캐비닛에 넣어 보관하고 있다...(중략)... 영업비밀로 인정된다.

(6) 영업비밀 접근·사용 권한을 업무에 필요한 범위로 제한할 것

- 각 직원별로 업무수행에 필요한 영업 비밀에만 접근권한을 부여할 필요가 있다.(예: 설계팀원에게는 설계도면, 설계계산시트 등 설계 업무 수행에 필요한 자료에만 접근권한을 부여하고 단가정보 등 회계 관련 자료에 대한 접근을 차단할 것, 반대로 회계팀원에게는 회계업무 수행에 필요한 자료에만 접근권한을 부여하고 연구개발 자료에 대한 접근권한을 차단할 것)
- 예외적으로 다른 부서나 상위 직급에게만 허용된 자료에 대한 접근이 필요한 경우, 이에 대한 승인 절차를 만들어두고, 승인을 얻은 후 접근하도록 하는 것이 바람직하다. 이러한 승인절차를 보안규정에 두며, 승인문서를 구비하도록 하는 것이 바람직하다.

- 영업비밀이 저장된 시스템이나 폴더에 대한 로그인 암호는 개인별로 지정하는 것이 바람직하며, 로그인 암호를 공유하는 것은 보안조치로서 부적절하다.
- 종료된 프로젝트 관련 영업비밀을 별도로 분리하여 접근 권한자를 종전보다 제한하거나, 임직원 수가 많은 경우 직급에 따라 접근권한에 차등을 두는 것도 바람직하다.

• 서울고등법원 2009. 10. 30. 선고 2008노2666 판결

- 피해자 회사는 모든 직원들로부터 입사 시 ‘기밀 정보 및 지적소유권에 대한 서약서’와 ‘기술보호 동의서’를 작성하게 하고, 퇴사 시에는 재직 중 취득한 영업 비밀을 공개 또는 누설하지 않겠다는 ‘확인서’를 작성하게 한 사실, 피해자 회사는 휴대폰 회로도 등 기술 자료는 팀별, 관리자별로 서버컴퓨터에 저장하도록 하였고, 시스템 패스워드를 사용하게 하였으며, 프로그램 접근시에는 등급별로 상위자만 하위자의 정보를 확인할 수 있게 한 사실, 휴대폰 모델이 완성된 경우 개발 자료를 CD에 보관하거나 서버에 다른 디렉토리를 만들어 팀장급 이상만 열람할 수 있게 하였고, 출장 시나 퇴근 시에는 회사에 노트북을 반납하도록 한 사실, 연구 개발장소 출입도 출입카드를 통하여 통제한 사실, 피고인의 퇴사 시 양도해 준 컴퓨터의 하드디스크를 포맷할 것을 요구한 사실 등을 인정할 수 있는바, 영업비밀로서 관리되고 있었다.

• 대법원 2009. 9. 10. 선고 2008도3436 판결

- 회사 기밀유지 각서를 제출받은 사실을 알 수 있으나, 컴퓨터는 비밀번호도 설정되어 있지 않고 별도의 잠금장치도 없어 누구든지 위 컴퓨터를 켜고 이 사건 자료를 열람하거나 복사할 수 있었던 사실, 위 컴퓨터와 네트워크를 통해 연결된 피해회사 내의 다른 컴퓨터를 통해서도 별도의 비밀번호나 아이디를 입력할 필요 없이 누구든지 쉽게 공소외인의 컴퓨터에 접속하여 이 사건 자료를 열람·복사할 수 있었던 사실, 공소외인은 이 사건 자료를 정기적으로 CD에 백업하여 사무실 내 서랍에 보관해 두었는데, 공소외인이 그 서랍을 잠그지 않고 항상 열어두었기 때문에 누구든지 마음만 먹으면 그 백업CD를 이용할 수 있었던 사실을 알 수 있는바, 피해회사가 피고인으로부터 위와 같이 일반적인 회사 기밀유지 각서를 제출받은 사실만으로는, 피해회사가 소규모 회사라는 점을 고려하더라도, 이 사건 자료가 상당한 노력에 의하여 비밀로 유지되었다고 보기는 어렵다.

(7) 물리적 보안장치 설치·운영

- CCTV, 카드리더기, 지문인식장치 등 물리적 보안장치를 통해 회사 출입을 통제하는 것이 바람직하다.
- 개발실, 보관실 등 영업비밀이 생성되거나 보관된 장소 등 주요 장소는 다른 장소와 분리하고 출입이 필요한 인원에게만 출입을 허용하며, 이러한 통제구역에 대해 출입통제를 위한 물리적 보안장치를 적용하고, ‘출입금지’, ‘사진촬영 금지’, ‘출입통제구역’ 등 표식을 부착하는 것이 바람직하다.

• 서울고등법원 2009. 12. 24. 선고 2009노2223 판결

- 피해회사는 위 보안기준에 따라 전체 임직원을 대상으로 '기업 비밀보호 각서'를 작성하게 하였고, 회사 내의 업무상 책상 등에 보안생활 수칙 내용이 담긴 보안용 스티커를 부착하게 하였고, 2006. 1.경 임직원들을 상대로 보안교육을 실시하였다. 피해자 회사는 2007년경 서울 본사의 기술연구소에 지문인식기를 도입하여 전자 출입통제 시스템을 가동 중에 있고, 그 외 연구소나 공장 등에는 현장 촬영을 금지하는 표식이 부착되어 있고, 외부인들의 출입을 통제하고 있다. 피해회사는 전산보안을 실시하고 있으며, 2002년경 DRM 보안 시스템인 '트레저'를 도입하여 전산문서에 대한 보안을 한층 강화하고 있다. 피해자 회사는 타 기업 및 연구기관 등과 거래를 할 때는 비밀유지계약 체결을 통하여 영업 비밀을 보호 관리하고 있다...(중략) 이 사건 각 파일들은 피해자 회사가 영업비밀로서 관리하였다고 볼이 상당하다.

(8) 기술보호 노력에 대한 증거를 평소에 확보할 것

- 영업비밀이 유출되어 민·형사 소송을 제기하는 경우, 기술보호노력에 대한 입증책임은 피해회사에 게 있다.
- 보안서약서 등 보안관련 자료의 보관기간은 법정되어 있지 않고, 보안유지노력은 유출 당시(예 : 퇴사자가 유출한 경우, 퇴사시점)를 기준으로 입증해야 하므로, 평소 기술보호를 하면서 관련 증거를 확보하고 보관해두는 것이 적절하다.
- 보안규정 제정과 개정, 보안서약서 징구의 경우, 매번 관련 자료 원본 및 스캔자료를 보관하여 두는 것이 바람직하다.
- 보안교육을 실시할 때마다, 보안교육 일자 및 보안교육에 참여한 임직원의 서명날인을 한 문서를 작성하여 보관하는 것이 바람직하다.
- CCTV, 지문인식기, 시정장치가 있는 캐비닛 구입 등 물리적 보안장치나 보안프로그램 등 기술적 보안장치 도입 시, 관련 계약서 등의 원본 및 스캔자료를 보관해두며, 촬영일이 나오도록 현장 사진 촬영해 두는 것이 바람직하다.
- '출입금지', '사진촬영금지' 등을 부착한 곳을 촬영일이 나오도록 사진 촬영해 두는 것이 바람직하다.

- 기업의 규모, 경제적 여력, 영업비밀의 가치 등에 비추어, 영업비밀 보관/열람/사용/복사/전송 내역을 기록하고 관리하며, 컴퓨터를 사용하는 경우 사용자, 사용시간, 사용내역 등 확인, 문서 출력 시 사용자 정보도 같이 출력되거나 프린터 내부적으로 출력 정보를 저장하는 시스템을 도입하는 것도 고려할 필요가 있다.
- 대중소기업협력재단의 기술자료임치제도, 한국특허정보원 영업비밀보호센터가 운영하는 영업비밀 원본증명제도, 한국특허정보원 영업비밀보호센터와 한국 산업기술보호협회가 제공하는 보안 프로그램 도입을 고려할 필요가 있다.

제1절

내부 기술인력 관리 방안

기술인력은 기업의 경쟁력을 제고시키고 고부가가치를 창출하는 중요한 요소이다. 특히 우리나라와 같이 부존자원이 부족한 상황에서는 기술인력을 어느 정도 확보하느냐에 따라 국가경제의 성장여부가 달려 있다고 보아도 과언이 아니다. 또한 최근 중소기업의 핵심 기술이 인력의 이동에 의해 유출되는 사례가 증가하면서 숙련된 기술인력에 대한 중요성이 더욱 부각되고 있다. 그러나 아직까지도 많은 중소기업들이 기술인력에 대한 인식이 미비하여 인적 자원투자 및 지원에 인색하며, 인적자원의 효율적 관리가 이루어지고 있지 않아 많은 기술 인력의 부족과 낭비를 동시에 겪고 있는 상황이다.

1. 기술인력에 대한 관리의 필요성⁸⁾

우리나라 영업비밀 침해사례의 대부분은 임직원에 의한 것으로서 아무리 제도적 장치와 물리적 조치가 완벽하다고 하더라도 임직원 관리를 소홀히 하게 되면 오랜 기간 연구·개발한 노력의 성과는 내부 직원에 의하여 외부에 유출될 가능성이 매우 높다.

임직원 관리는 입사 시부터 퇴직 후 일정기간까지로 그 관리기간이 비교적 장기간이므로 효율적인 관리가 쉬운 일은 아니나, 최소한 입사 시 비밀유출금지 서약서 제출, 재직 시 주기적인 보안교육 실시, 퇴직 시 직업선택의 자유나 근로의 권리를 침해하지 않는 범위 내에서 동종 업체에 취업 및 경업금지의무 부과 등을 실시하여야 한다.

다만, 중소기업에 있어 임직원관리는 무엇보다도 중소기업 대표와 임직원간의 협력자적 동반관계가 중요하므로 평소에 중소기업 대표는 임직원에 대하여 각별히 관심을 가지는 한편, 앞서 설명한 바와 같이 임직원의 직무수행과정에서 발견 또는 창출된 영업비밀을 회사에 신고하여 관리할 수 있도록 하는 직무발명 보상제도를 도입하고, 신고된 영업비밀은 이에 상응하는 보상금을 지급토록 하는 함으로써 기술인력의 개발을 장려하고 기업의 경쟁력을 제고시킬 필요가 있다.

8) 인력관리 가이드_가이드_배포용_한국산업기술보호협회(2015.12), 3~16쪽

2. 기술인력 채용 시 조치

임직원의 신규 채용은 영업 비밀에 대한 인력관리의 시작이다. 따라서 채용시점부터 영업 비밀에 대한 보호의식을 가지고 재직기간 중 영업 비밀을 관리해 나갈 수 있도록 임직원을 교육시켜야 한다. 특히, 영업비밀과 직접 관련이 있는 연구·개발부서 및 영업비밀 관리직원에 대해서는 영업비밀 준수 서약서와 전직 및 퇴직 시 사용, 공개금지 및 경업금지 서약서를 징구해야 한다. 이와 같은 서약서에는 재직 중 취득한 중소기업의 영업 비밀을 유출하는 경우 손해배상은 물론 민·형사상 책임을 지겠다는 것, 재직 중 창출한 영업 비밀의 소유권은 회사에 귀속하는 것을 명기하여, 영업 비밀을 둘러싼 법적 분쟁여지를 사전에 차단하도록 한다.

신규 임직원이 다른 기업으로부터 전직하여 왔을 경우에는 이전 직장에서의 체결한 영업비밀 관리에 관한 계약 등을 주의 깊게 검토하고, 이 과정을 통해 타 회사의 임직원을 채용함으로써 부당한 스카웃 또는 영업 비밀 침해로 인한 제소를 당하는 일이 없도록 대비할 필요가 있다.

(1) 신규 입사자 채용 시 고려사항

신입사원 채용 시 이력서 및 지원서를 검토하여 지원자의 신원확인 및 관련된 추가정보를 확인하고, 면접을 통하여 요구조건에 부합하는 인재를 찾는 동시에 연구보안 문제에 영향을 끼칠 수 있는 성실성, 충성심과 같은 인성에 대한 검증도 수행하며, 특히 보안과제의 경우 연구책임자도 한다. 함께 면접에 참여하여 지원자에 대한 면밀한 검토를 수행한다.

(2) 고용 후 고려사항

- ① 영업비밀 유지 서약서 작성취업규칙에 기초한 비밀 보호 의무는 포괄적·일반적인 의무규정에 머무르고, 종업원에게는 공개된 정보 가운데 어떤 것이 보호 대상인지 불명확한 경우도 있다. 따라서 그 내용을 명확하게 한다는 관점에서 영업비밀 유지 서약서를 추가적으로 작성한다.
- ② 위와 같이 취업규칙 등의 사내 규정, 개별적 서약서나 계약서의 조항을 두더라도, 이를 당사자들이 엄수할 수 있도록 보안교육을 실시하는 것이 필요하다. 즉 보안업무 규정 또는 지침, 사내·외 발생 보안사고 사례 등을 중점적으로 교육하여, 보안에 대한 경각심을 제고한다. 이때 영상물을 이용하면 현실감과 이해력을 높일 수 있으며, 관심도 제고 차원에서 대중소기업협력재단 등에서 지원하는 외부 전문 강사를 초빙하는 것도 효과적이다. 보안교육 종료 후에는 확인란에 본인서명을 받거나 수료증을 발급함으로써 재직 또는 퇴직 후, 회사기밀 유출로 인한 법적 분쟁 시 회사 기밀을 보호하기 위한 회사의 노력을 입증하는 증거로 사용할 수 있다.

(3) 경력자 채용시 주의할 점**① 전입자의 계약관계 확인**

다른 회사에서 전직한 자를 채용할 때에는, 전직자가 전 직장에서 부담하고 있던 비밀유지의무나 전직 및 경업금지의무 내용을 확인한다. 중도채용이나 졸업 후 3년 이내인 자가 다른 회사로부터 전직하여 회사 직원이 될 경우, 해당 전입자가 특정 정보에 관하여 법적 의무를 지고 있어 문제에 휘말릴 소지가 있으므로 우리 회사의 정보와 전입자가 가지고 오는 정보가 뒤섞이지 않도록 주의할 필요가 있다. 구체적으로는 그 전입자가 가지고 들어오는 정보로 인하여 이직한 기업에 영업비밀 침해금지 청구에 의한 사업 중단 위험이나 어떠한 손해배상청구를 받을 위험이 발생시키지 않을지를 검증해야 한다.

또한 연구 개발자의 경우 이전 직장에서 비밀유지서약이나 경쟁업체 취업금지서약을 했을 가능성이 높으며, 이를 무시할 경우 경력자 본인은 물론 채용한 업체도 영업비밀 침해행위가 될 수 있다. 따라서 경력자를 채용할 때에는 기존 회사와 전직금지계약을 체결하였는지 여부를 확인하고, 되도록 전직회사와 동일한 업무에 종사하지 않게 하는 것이 바람직하다. 업무수행 중에 전직회사 비밀의 사용을 금지하는 서약을 입사 시에 받으면 전직회사의 영업비밀을 적극적으로 보호해 줌으로써 분쟁 예방에 노력한 근거로 사용할 수 있다.

경력자는 전직회사의 임직원들과 사적인 친분관계가 있으므로 고의가 아니더라도 정보를 제공할 개연성이 많으며, 위장 취업했을 가능성도 배제할 수 없으므로 일정 기간 동안 근무 태도를 예의주시할 필요가 있다.

② 채용 시 법적 대처방법

채용하는 회사의 고유 정보와 전입자가 가지고 오는 정보의 뒤섞임을 피하기 위한 법적 수단으로써 다음과 같은 사항이 기재된 서약서를 전입자로부터 받는 방법이 있다.

- 타사 영업 비밀을 승낙 없이 자사 내에 공개 혹은 사용하지 않을 것
- 타사에서 완성시킨 직무 발명 등을 자사 명의로 출원하지 않을 것
- 자사에서 취업하는 데에 있어 불합리한 경업금지의무가 없을 것

이들 서약서를 취득해도 여전히 위험이 있다고 생각될 경우에는 누설우려가 없어질 때까지 일정 기간 전 직장과의 관계가 거의 없는 업무에 종사시킴으로써 신중한 대응을 검토하는 것이 바람직하다.

3. 기술인력 실무상 조치**(1) 직무발명보상제도**

앞서 인적관리 부분에서 설명한 바와 같이 발명진흥법상 직무발명보상제도를 도입하여 기술인력의 개발을 장려하고, 적절한 보상체계 수립을 통해 회사에 대한 소속감을 고취시켜 기술인력의 유출을 예방할 수 있다. 이 제도는 회사와 기술인력의 이익을 동시에 만족시키므로 유용한 제도라고 할 수 있다. 기술인력이 직무발명을 한 경우 다음과 같은 절차를 밟도록 내부규정을 마련한다.

- ① 기술인력이 직무발명을 완성한 경우에는 지체 없이 그 사실을 사용자에게 문서로 알려야 한다. 2명 이상의 종업원등이 공동으로 직무발명을 완성한 경우에는 공동으로 알려야 한다.
- ② 기술인력으로부터 통지를 받은 사용자는 4개월 내에 그 발명에 대한 권리의 승계 여부를 기술인력에게 문서로 알려야 한다. 직무발명 승계에 대한 근무규정 또는 계약이 없는 경우에는 사용자는 기술인력의 의사와 다르게 해당 기술에 대한 권리를 승계할 수 없다.
- ③ 사용자가 4개월 내에 해당 발명에 대한 권리의 승계 의사를 알린 때에는 그때부터 그 발명에 대한 권리는 사용자 등에게 승계된 것으로 본다. 만일 사용자가 그 기간에 승계 여부를 알리지 아니한 경우에는 사용자 등은 그 발명에 대한 권리의 승계를 포기한 것으로 본다.
- ④ 기술인력이 직무발명에 대하여 특허를 받을 수 있는 권리를 사용자 등에게 승계하거나 전용실시권을 설정한 경우에는 정당한 보상을 받을 권리를 가진다.
 - 보상의 종류 : 발명보상(제안보상), 출원보상, 등록보상, 실시·처분보상, 출원유보보상 등
 - 출원유보 : 사용자가 직무발명을 승계한 후 영업비밀 등의 이유로 출원하지 않거나 출원을 포기 또는 취하하는 경우에 종업원에게 주어지는 보상
 - 보상형태와 보상액에 관한 내용을 종업원과 협의하여 규정한다.

(2) 핵심 연구 인력의 대외 활동에 대한 기술보호

핵심 연구 인력의 출장이나 타 회사 방문 시 사전교육을 실시하여 소지한 기밀문서나 본인이 취득하고 있는 기밀의 누출방지에 유의해야 하며, 출장 및 타사 방문 후 보고서 징구가 필요하다.

(3) 회의참석

내부 부서회의라 하더라도 해당 관련 핵심 기술과 관련하여 비인가자가 있으면 특히 발언에 유의하도록 사전교육이 필요하며, 부서자체의 핵심 기술 관련 사항을 무의식중에 사내회의에서 누설하지 않도록 유의한다. 외부 회의 참가 시 부득이 핵심기술 관련 내용을 밝힐 필요가 있으면 사전에 회의참석 관계인으로부터 비밀누설방지(영업비밀 보장) 각서를 징구하며, 핵심 기술 관련을 타인에게 교부하는 때에는 반드시 수령증을 받아 둔다.

(4) 내방객 접견

상담의 경우에 있어서 내방객에게 핵심기술 관련사항을 개시할 때에는 사전에 그 내용이 회사의 영업비밀임을 인식시키고 비밀보장 각서 등을 징구하되 가급적 필수적인 내용만 개시하고 불필요한 내용의 발설에 최대한 유의한다.

일반적으로 상담이나 의견청취 과정에서 타인으로부터 영업비밀을 개시 받으면 이를 전달받은 당사자는 상대방의 영업비밀을 존중할 의무를 지며, 그 당사자가 속한 전체가 영업비밀 보호 의무를 지게 되므로 당사자 독자적인 판단에 의하여 타인의 영업비밀을 청취하거나 전달받는 것은 상당한 위험이 따를 수 있다. 이는 상대방이 제시하려는 영업비밀과 같은 내용을 회사 내의 어느 부서에서 취급하고 있거나 나아가서 그 내용보다 더 좋은 기술을 개발하여 영업비밀로 간직해 놓고 있을 수도 있기 때문이다. 이때 사내 유사 영업비밀의 존재를 확인하지 못한 채 상담에 임하여 비밀보장 각서를 작성해 주고 내방객으로부터 영업비밀을 제시 또는 개시받았다면 회사 전체가 해당 영업비밀 보호 의무를 지게 되며, 향후 회사에서 그와 유사한 기술을 개발하였을 때 개시받은 영업비밀의 내용과 저촉되어 책임을 져야하는 일이 생길 수 있다. 즉 내방객 측에서 자사가 개시한 영업비밀을 그대로 이용하거나 이를 이용하여 기술을 개발했다고 주장하면 분쟁에 휘말릴 수 있는 것이다.

(5) 학회참석, 출판, 발표 등

- ① 학회 참석 발표 학회나 집회 등 불특정 다수인이 회합하는 장소 등에서는 영업 비밀보장 각서 등의 징구가 사실상 불가능하므로 이러한 회합에서의 학술이나 연구발표는 그대로 기밀의 누설, 개시 및 공개가 되므로 이점 각별히 유의할 필요가 있다. 학회 등의 참석에 앞서 요약문이나 초록의 작성 제출 등은 기밀보호를 불가능하게 하므로 기밀 내용이 개시되는 일이 없도록 각별히 주의하여야 한다.

- ② 기고

사내·외에 기고하는 경우도 학회참석 발표의 예에 준하여야 한다. 그러나 사내 한 잡지 등 간행물의 경우에 있어서는 사내 기술 및 정보의 정상적인 전파를 위하여 일부 기밀의 개시가 바람직할 때도 있다.

- ③ 연구논문 발표

연구논문은 발표 간행물 출판 시점에서 영업비밀보호가 종료된다는 점에 유의하여야 한다. 연구논문의 제출일로부터 출판일까지는 그 내용이 비밀로 간직될 수 있으나 발표되는 순간부터 영업비밀로서의 가치가 상실된다. (다만, 출판일이나 학술발표회로부터 6월내에 특허출원하면 신규성을 인정받아 출판이나 학술발표로 이미 공지된 내용이라도 특허를 받을 수 있는 방안이 있음)

(6) 파견근무, 연수

파견이나 연수 개시 전에 핵심인력에 대해서는 특별교육을 실시하여 기밀유지 지침에 따르도록 하며, 파견근무 시 휴대한 기밀문건의 및 파견된 기관의 영업비밀문건 등의 접촉 시 각서를 작성하여 영업비밀 보장 조치를 취하는 것이 중요하다. 피파견기관의 승인 없이 영업비밀 문건 등에 접근하면 영업비밀 탐지 혐의를 받을 염려가 있기 때문이다.

4. 퇴사 시 조치

퇴직 시에는 각종 프로젝트 등 실제로 접근한 영업 비밀에 대해 특정하는 것이므로, 입사 시나 재직 시에 비하여 비밀보호의무의 대상이 되는 정보를 특정하기가 쉽다. 따라서 구체적인 비밀보호의무 범위를 명시하여 계약을 체결하는 것이 가능하다.

그러나 이 시점에서 갑자기 계약 이야기를 들으면 퇴직자는 당혹감을 느낄 가능성이 있다. 그때까지 계약을 체결하지 않은 경우에는 퇴직 시에 비밀보호 계약을 체결할 가능성이 있음을 사전에 주지하고, 퇴직 시까지 무언가 계약을 체결한 경우에는 퇴직 시에 보호의무 대상이 되는 정보만 특정하는 방법과 일정 기간마다 계약 내용을 재검토하는 방법도 있다.

영업비밀 보유자 등 핵심인력이 경쟁업종 금지 기간 중 경쟁업체로 전직할 경우, 관련법규에 의해 처벌받는다라는 사실을 고지하고 퇴직 서약서에 동 내용을 명기한다. 퇴직자가 보유한 영업 비밀을 고려, 경업금지 업종·분야를 구체적으로 한정해야 향후 영업비밀 유출로 인한 법적 대응 시 유리함에 유의하여야 한다. 경업금지 기간은 업종, 제품의 라이프 사이클, 특허출원 상황 등을 통계적으로 정리하여, 합리적으로 결정한다.

5. 핵심 연구 인력의 퇴사 후 관리

핵심 연구 인력은 회사의 핵심기술을 알고 있는 경우가 많다. 따라서 퇴직 시에 비밀유지약정서, 전직금지 및 경업금지약정서를 작성하지만 핵심 연구 인력이 이를 위반하고 경쟁업체에 핵심기술을 누설한다면 법적인 제도를 통하여 조치를 취하더라도 회사에는 회복할 수 없는 피해가 생기게 된다. 따라서 퇴사하는 직원이 다른 마음을 먹지 못하도록 인적인 유대감을 유지하는 것이 중요하다.

(1) 퇴직 핵심 연구 인력에 대한 우호적 조치

퇴직직원 특히 핵심 연구 인력이 퇴직한 경우에는 어떠한 경우에도 회사와 등을 돌리지 않도록 다방면의 고려에 의한 조치를 취해야 한다. 상기한 퇴직절차에 의한 전직제한이나 경업금지의 부담을 주는 대신 계속해서 회사와 또는 동료 직원들과 인적 유대를 갖도록 관리를 할 필요가 있다.

이러한 관리의 방안으로 회사의 공식, 비공식 행사에의 초청과 함께 회사의 창립기념일이나 명절 때 아담한 선물(회사 제품이 있으면 회사 제품으로)을 하거나 사보 등을 우송하고 사보의 소식란을 현직 직원들과 함께 공유한다든가 하는 유대를 맺는 것이 좋다. 이는 회사의 핵심 기술의 유출을 상당부분 미연에 방지해주고 재직 중인 핵심 연구 인력의 연구 의욕을 고무시켜 연구개발 능력을 획기적으로 향상시킬 수 있다.

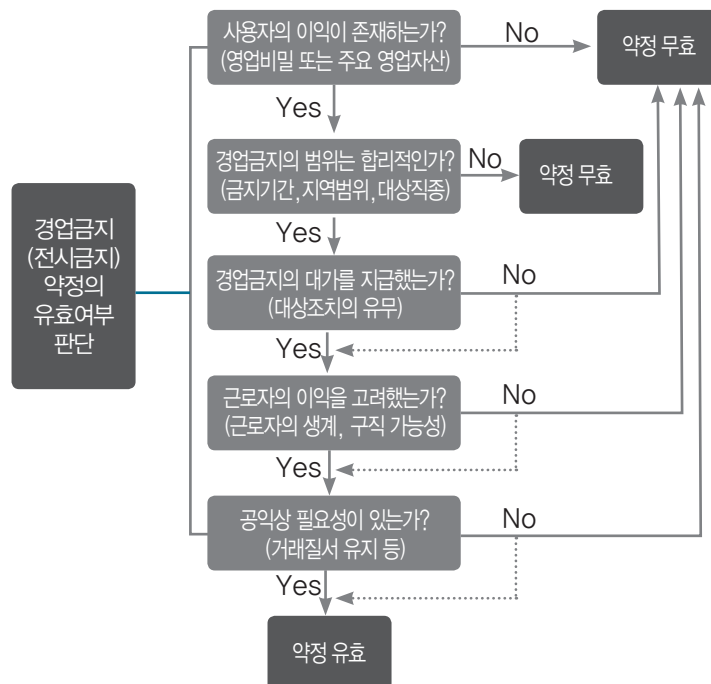
(2) 퇴직직원 사우회의 활용

퇴직한 핵심 연구 인력을 퇴직직원 사우회에 가입 포용케 하되 특히 취미별이나 지역 소그룹 등의 회합에 자주 나올 수 있는 분위기를 조성하고 회사는 지속적으로 소그룹이나 퇴직직원 사우회를 통하여 간접적으로 전직 핵심연구 인력을 관리할 수 있는 것이다.

6. 기술인력 이직에 따른 분쟁 시 조치

(1) 전직금지 및 경업금지약정의 필요성

퇴사자가 경쟁업체에 취업하여 비슷한 업무를 할 경우 회사에서 근무하면서 취득한 영업비밀을 누설할 우려가 있기 때문에 전직금지 및 경업금지약정을 체결하는 경우가 많다. 경업금지약정은 영업비밀의 보호를 위해 체결되는 경우가 많지만, 영업비밀이 아니더라도 영업상 주요한 자산으로서 보호할 가치 있는 사용자 이익이라고 인정되면 약정을 통해 근로자에게 경업금지의무를 부과할 수 있다. 또한 경업금지약정은 특정 업종에서만 필요한 것은 아니다. 기업이 보유하는 영업비밀을 보호하기 위하여 경업금지약정을 체결하는 경우가 많은데, 영업비밀에는 기술상의 정보뿐만 아니라 경영상의 정보도 포함되며, 최근 산업이 고도화됨에 따라 사실상 모든 기업이 영업 비밀을 보유하고 있기 때문에, 경업금지약정은 영업 비밀을 보유한 기업이라면 업종에 관계없이 모두 필요하다고 할 수 있다.



〈그림 5-1〉 경업금지약정의 유효 여부 판단에 관한 순서도

(2) 경업금지 약정의 유효성 판단 요소 및 실효성 있는 경업금지약정 체결을 위한 가이드라인⁹⁾

• 대법원 2010. 03. 11. 선고 2009다82244 판결

- 사용자와 근로자 사이에 경업금지약정이 존재한다고 하더라도, 그와 같은 약정이 헌법상 보장된 근로자의 직업선택의 자유와 근로권 등을 과도하게 제한하거나 자유로운 경쟁을 지나치게 제한하는 경우에는 민법 제103조에 정한 선량한 풍속 기타 사회질서에 반하는 법률행위로서 무효라고 보아야 하며, 이와 같은 경업금지약정의 유효성에 관한 판단은 보호할 가치 있는 사용자의 이익, 근로자의 퇴직 전 지위, 경업 제한의 기간·지역 및 대상 직종, 근로자에 대한 대가의 제공 유무, 근로자의 퇴직 경위, 공공의 이익 및 기타 사정 등을 종합적으로 고려하여야 한다.

- 보호할 가치있는 중소기업의 이익

※부정경쟁방지법상 영업비밀은 보호할 가치가 있는 중소기업의 대표적인 이익인 경우에 해당한다.

※중소기업 대표가 임직원에게 특수하게 훈련시킨 기술, 해당 중소기업 대표만이 가지는 특수한 지식, 중소기업 대표가 많은 비용과 노력을 들이거나 중소기업 대표의 기술과 노하우를 통해 형성된 고객관계 등도 보호할 가치있는 중소기업 대표의 이익에 해당할 수 있다.

※그러나, 임직원 스스로의 교육, 능력 및 경험 등을 통해 취득한 개인적 지식 및 기술로서 중소기업 대표에게 특수한 것이 아니라 업계 전반에 알려진 일반적인 지식 및 기술은 해당하지 않는다.

※임직원과 고객과의 개인적 신뢰관계는 임직원에게 체화된 인격적, 속인적 요소가 강하고 근로자의 통상적인 업무수행 과정에서 저절로 발생하는 측면도 있으므로, 엄격하게 판단해야 한다.

※경업금지약정서에는 '재직 중 취득한 모든 기술, 경영정보' 또는 '영업비밀'과 같이 일반적인 내용으로 기재하는 것보다, '해당 영업비밀이나 보호할 이익에 대한 명칭이나 개요 또는 형태(설계도면, 회로도, 소스코드, 배합비율 등), 관리번호가 있는 경우 그 번호, 프로젝트 명칭이나 산출물 내역' 등으로 구체적으로 기재하는 것이 바람직하다.

- 경업(전직) 제한 기간, 지역 및 대상 직종

※경업 제한 기간, 지역 및 대상 직종은 임직원에게 과도한 부담이 되지 아니하고 중소기업 대표의 이익 보호를 위해 합리적으로 필요한 범위 내라야 한다. 여기서 합리성 여부는 중소기업 대표와 임직원 및 공공의 이익을 비교 형량하여 결정되며, 개 사건의 구체적인 사실관계와 사정에 비추어 판단하게 된다.

9) 사법연수원, 부정경쟁방지법, 2015., 138~141쪽 참조

※법원은 경업(전직) 제한 기간, 지역 및 대상 직종이 합리적인 범위를 벗어나 과도하다고 판단되는 경우, 합리적인 수준으로 감축하게 된다.(전직 금지의 경우 통상 6개월-1년, 경업금지의 경우 1년 - 3년 인정)

- 임직원에 대한 대가 제공 유무

※대가지급은 경업금지약정의 유효성을 판단하는 독자적인 요소는 아니지만, 대가를 지급할 경우 약정의 유효성을 강화할 수 있다.

※대가를 지급하는 경우, 그 대가가 경업금지의무의 대가라는 것임을 분명히 기재하는 것이 바람직하다.

- 임직원의 퇴직 경위

※경업금지약정은 중소기업 대표측의 귀책사유 없이 근로관계가 종료된 경우 효력을 가짐

※회사가 별다른 이유 없이 임직원을 해고하였거나, 임직원이 정리 해고된 경우, 부득이하게 퇴직할 수 밖에 없었던 경우(임직원이 회사에게 약속이행을 촉구하자 회사가 특별한 이유 없이 임직원에게 직무정지를 명하고 이에 임직원이 퇴직) 등에는 경업금지 효력을 인정하기가 곤란하다.(서울고등법원 2005라278 결정)

※퇴직경위나 목적, 그로 인해 중소기업 대표가 입게 될 영향의 정도 등에 비추어 임직원의 배신성이 현저한 경우 전직금지 약정의 유효성이 인정되기 쉬움

- 경업금지약정서 체결 시기와 형식

※경업금지약정 체결 시기나 형식에 별다른 제한은 없으나, 취업규칙이나 근로계약서, 단체협약 등의 형식으로 체결된 경우 무효로 인정될 가능성이 있으므로, 별도의 경업금지약정서를 체결하는 것이 바람직하다.

※입사 시나 재직 중에 체결되기도 하나, 가능한 한 퇴사 시 개별적인 계약을 통해 체결하는 것이 바람직하다.

※경업금지약정의 내용은 담당 업무나 직급 등에 따라 임직원별로 다르게 하는 것이 바람직하다.(예: 기술팀 연구소장이나 팀장, 영업부 신입사원은 그 업무와 직급이 달라서 회사의 자산에 접근할 수 있는 범위가 다르므로, 이러한 점을 고려하여 경업금지약정서를 체결)

〈표 5-1〉 경업금지의무 위반에 대한 중소기업의 조치유형

징계	근로관계 존속 중 근로자의 경업 행위시 중소기업 대표는 임직원을 징계할 수 있다. 이는 임직원의 경업금지의무와 겸직(겸업)금지의무 모두를 위반한 경우가 많을 것이고, 중소기업 대표의 정당한 이익을 침해하게 되어 해고까지 포함해 징계사유가 될 수 있다.
영업비밀 침해금지 청구	근로계약 존속 중 근로계약 또는 영업비밀 유지약정, 부정경쟁방지법상의 영업비밀 침해행위를 원인으로 한 법이 정한 금지청구권에 의해 각각 구할 수 있다. 하지만 그 금지청구의 내용은 영업비밀 침해행위의 금지에 한정된다. 더 나아가 특정회사의 취업·전직 금지의 청구는 특별한 사정이 없는 한 제한된다.
경업금지청구	부정경쟁방지법을 근거로 하여 경쟁회사로의 전직금지나 경쟁회사에서의 퇴사명령을 구할 수는 없고, 유효한 경업금지 계약의 체결 시에만 그 금지를 청구할 수 있다. 유효한 계약상 경업금지 기간 내에 경업 사실이 발견되면 신속한 영업비밀 보호를 위하여 본안 소송과 별도로 전직 및 경업금지 가처분을 신청할 수 있다. 경업금지의 내용은 근로자의 직업선택의 자유 및 근로의 권리를 고려하여 필요한 최소한 범위 내에서만 할 수 있다.
손해배상청구	영업비밀 침해행위의 경우 근로계약의 존속 중에는 채무불이행에 따르거나 부정경쟁방지법상의 손해배상청구권을 행사할 수 있다.

제2절

프로젝트에 참여하는 기술인력 관리¹⁰⁾

국가 과제나 공동 개발 프로젝트에 참여하는 인력의 경우 해당 과제 또는 프로젝트가 종료되면 그 프로젝트를 구성하던 인력은 본래의 위치로 돌아가는 경우가 많다. 따라서 한 회사에만 속해있는 인력의 경우보다 비밀유출의 가능성이 더 커지며, 이를 방지하기 위하여 과제 또는 프로젝트를 추진하는 경우에 비밀유지 서약서 작성이 필수적으로 필요하다. R&D와 관련된 과제나 프로젝트가 비교적 장기간 수행되는 점을 살펴볼 때, 장기간동안 개발된 연구 성과가 한 순간의 비밀 유출로 인하여 무용지물이 되는 일이 없도록 인력관리에 각별히 주의를 기울일 필요가 있다.

1. 국가 R&D 사업참여 시 인력관리 및 보안 조치

최근 국가연구개발사업과 민간부문의 연구개발 사업으로 개발된 첨단기술이 해외로 유출되었다가 적발된 건수가 점차 있는 추세를 보이고 있으며, 전직 또는 현직 직원 또는 협력업체로 인해 발생하는 연구보안사고가 거의 92%를 차지하고 있다. 또한 전 세계적으로 과학기술경쟁력이 국가경쟁력의 중요한 요소로 인식됨에 따라 글로벌 차원의 과학기술 경쟁이 심화되면서 우리나라는 연구개발에 대한 투자가 날로 증가하고 그에 따른 최첨단 연구개발 성과물도 더불어 늘어가고 있는 실정이다.

10)인력관리 가이드_가이드_배포용_한국산업기술보호협회(2015.12), 27~36쪽.

2. 공동개발 프로젝트 추진 시 인력관리 및 보안 조치

공동연구개발을 위해 비밀유지약정을 체결한 후 아이디어와 개발 자료를 제공하였으나, 그 개발 프로젝트가 성공하지 못하고 중도 탈락한 경우 법적 분쟁의 소지가 많다. 특히, 법무지원 여력이 충분하지 않는 중소기업이나 벤처회사의 경우에는 귀중한 아이디어만 탈취 당했다는 허탈한 상황에 직면할 수도 있다. 중견기업이라고 해도 촉박한 개발 일정에 쫓기거나 법률비용을 아끼려는 마음에 법적 보호 장치를 소홀히 한 탓에 자신의 사업 아이디어를 보호할 수 없는 상황에 처할 수도 있다.

한편, 공동개발 제안을 받은 회사 입장에서는 공동개발 프로젝트를 성실하게 수행하여 그 결과를 평가하여, 계속 추진여부를 판단한 결과 그 프로젝트를 중단하기로 결정한 것에 불과한데, 이와 같은 중단 상황에서 발생 가능한 법적분쟁에 미리 대비하지 않는 탓에 심각한 리스크가 있는 법적 분쟁에 휘말리는 경우도 많다.

우리나라 기업 사이에도 흔히 발생하는 사안이지만, 특히 한쪽 당사자가 미국회사인 경우에는 영업비밀 침해 또는 계약 위반 등을 이유로 천문학적 손해배상을 청구하는 경우도 있다. 최종 승패를 떠나 미국 소송은 법률비용만으로도 우리나라와는 비교가 되지 않는 큰 부담이다.

따라서 공동개발 프로젝트의 경우 추진하기 전에 분쟁을 예방하기 위한 상호 합의 및 계약서와 보안유지 서약서 작성이 필수적이다.

3. 해외 진출기업 기술개발 시 인력관리 및 보안조치

한국 기업이 현지 국가에 R&D센터를 설립한 경우, 그곳에서 신기술의 연구개발 등이 이루어지기 때문에 기술비밀 유출은 더욱 심각한 문제로 대두된다. 기술유출 유형을 살펴보면, 대부분 전, 현직 내부 직원에 의해서 기술비밀 유출이 발생하며, 인수합병(M&A), 공동사업 등을 통하여서도 자연스럽게 기술 비밀이 유출되는 경우가 있다.

특히, 내부 직원에 의한 기술 유출 유형에서는 경쟁업체로부터 뇌물, 파격적인 연봉, 고위 직책 등의 제안을 받고 기술을 유출하는 것이 가장 전형적인 형태로 핵심 기술을 다루는 핵심 인력을 보호 및 유지하려는 노력을 아끼지 않아야 할 것이다.

(1) 내국인과 현지인의 업무구분

해외에 진출한 국내 기업의 경우 근로자의 대부분이 현지인이므로 기술유출 및 침해의 위험성이 매우 높다. 이에 연구개발(생산현장) 근로자의 대부분이 현지인이더라도 핵심기술 및 시설의 보호담당은 내국인이 맡아야 한다.

(2) 핵심기술 비공개 원칙

핵심기술을 블랙박스화하여 현지인들의 모방을 방지하도록 해야 한다. 산업분야마다 차이가 있긴 하겠지만, 핵심 부품 모듈화를 통해 분해 및 재제작을 어렵게 하여 역 엔지니어링(reverse engineering)을 원천적으로 봉쇄한다거나, 전체적인 제조 프로세스를 통한 영업비밀의 유출을 방지하기 위하여 현지 연구원에게는 단위별 프로세스만 알 수 있도록 공개해야 하는 등 핵심기술에 대한 비공개를 원칙으로 해야 한다.

(3) 지식재산 관리 강화

센터 내 지식재산 전담 관리 조직을 두어 보유 기술을 체계적으로 관리할 수 있도록 해야 한다. 이곳에서 지식재산과 관련된 정책을 세우고 시행할 수 있도록 해야 하는데, 공개할 기술에 대해서는 특허 출원 및 등록을 통해 권리를 확보해야 할 것이며, 연구개발 프로세스 상 발생하는 기술상의 비밀이나 노하우에 대해서는 회사가 영업비밀로 보호할 것인지를 판단하여 기술비밀이 유출되지 않도록 철저히 관리해야 할 것이다.

(4) 현지 연구원들의 관리방안

R&D의 경우, 특히 주의할 점으로는 R&D는 단순한 기술사용에 그치는 것이 아니라 연구개발의 창조성 높은 업무를 하는 곳이기 때문에, 연구개발에 종사하는 현지 연구원들을 어떻게 관리하는 지가 중요한 문제가 된다.

이에 현지 연구원의 관리수단으로써 비밀유지계약 체결, 입사에서 부터 퇴사까지 단계별 보안 관리, 사내 비밀관리규정마련 및 철저한 시행, 이직방지대책 마련 등이 중요한 포인트가 된다.

(5) R&D센터 내의 보안체계 구축

현재 국내 기업 중에서도 R&D센터 내의 제대로 된 보안체계를 갖춘 기업은 그리 많지 않다. 그만큼 R&D센터 내의 보안 시스템을 갖추는 것은 비용이나 관리 측면에서 많은 부담이 되기 때문에 쉽게 보안 환경을 구축하기는 어려운 실정이다. 그러나 현지에서의 핵심기술에 대한 기술비밀 유출은 자국에서보다 용이하게 이루어질 수 있는 환경이므로 관련 보안 체계를 구축하여 철저히 관리해야 할 것이다

(6) 보안 시스템 구축

기술비밀 유출은 크게 2가지인 내부자의 유출이나 외부자의 침입으로 인한 유출로 구분할 수 있다. 외부자의 침입은 바이러스 백신의 설치, 침입탐지 및 메일 모니터링 시스템의 운용, 방화벽 설치 등과 같은 물리적인 보안 시스템을 갖추는 것으로도 어느 정도 기술비밀 유출을 방지할 수 있을 것이다.

그러나 현지에 R&D센터를 설립하게 되면 아무래도 현지인(내부자)에 의한 기술비밀 유출 가능성이 커지므로 이러한 점을 염두에 두어 보안 시스템을 구축해야할 것이다. 게다가 현지인에 의한 내부에서의 기술비밀 유출은 해당 기업뿐만 아니라 국가적으로도 막대한 손실을 입힐 수 있으므로 심각성이 더욱 크다.

내부자에 의한 주요 유출 경로는 메일이나 파일 공유 시스템, 노트북의 반/출입을 통한 정보유출, USB 등과 같은 이동저장매체, 메신저, 인쇄물 등을 통한 유출 가능성을 고려해 볼 수 있다. 이에 다음 표와 같은 방지 방안을 참고해두어야 한다.

〈표 5-2〉 정보저장 매체별 정보유출 방지

계약 고려사항	기술 유출 및 보호 관리방안
PC	불법적 외부 접속을 차단하며, 운영체제 업그레이드 및 바이러스 백신 등과 같은 PC 보안 툴의 자동 관리를 중 앙 집중 방식으로 구축한다.
메일	첨부 파일을 통제하며, 메일 모니터링 시스템을 수시로 업그레이드 한다.
USB 등의 이동 저장매체	외부로 내부 정보 유출을 방지하기 위하여 사용금지하 도록 권하며, 이동저장매체 접촉 부분을 원천봉쇄 한다.
메신저	메신저를 사용하지 않는 것을 권장하며, 사용 시 별도 의 모니터링 프로그램을 구동한다.
프린터(인쇄물)	내부 주요문서에 사용권한을 부여하여 출력을 제어하며, 인쇄물에는 담당자, 날짜 등의 정보를 포함한 워터마크 가 삽입되도록 한다.

(7) 사전 승인 제도

외부로 메일을 보낼 경우에도 모든 내용을 승인 받아야 가능하도록 하거나 현지 인력이 외부 인력과 접촉 시, 필요 이상으로 회사 정보를 논의하지 않도록 교육하며, 필요 시 사전에 책임자 및 보안 부서에 통보하여 승인을 받을 것을 의무화해야 한다.

(8). 보안 교육 실시

아무리 보안 시스템 및 체계가 잘 갖추어 있다고 해도, 내부 직원들이 의도적으로 기술비밀을 유출하려고 들면 막을 방도가 없을 것이다. 이를 방지하기 위해 현지 내부 직원 보안 교육은 매우 중요하며, 주기적으로 실시해야 할 것이다.

4. IT 외주인력 보안 통제

중소기업의 경우 기업 규모 상 IT업무를 기업내부에서 담당하기 힘든 경우가 많다. 따라서 IT와 관련된 업무를 외부업체에 외주용역을 주는 경우가 많다.

IT 외주 인력의 경우 회사의 소속된 사람이 아니므로 관리하기가 더욱 까다롭기 마련이다. 하지만 회사 내부의 IT업무를 담당하는 외부 인력의 관리를 소홀히 해서는 안된다. 첨단과학기술 시대인 만큼 IT와 관련된 보안이 매우 많고 회사 내부의 영업비밀 등도 전산화하여 보관되어 있는 경우가 많기 때문에 외부 용역업체와 계약을 체결할 때 보안유지에 특별히 신경을 써야 하며, 회사에 배정된 외주 인력도 별도의 보안유지 서약서를 받는 것이 보안유지를 위해 필요하다.

제3절

기술인력 교육 운영방안 ¹¹⁾

기술정보의 유출 기법은 나날이 발전하고 있으며 이와 더불어 핵심기술이 외부에 유출되는 기술보호 사고도 매년 증가하고 있는 추세이다. 이처럼 기술유출 사고가 줄어들지 않는 가장 주된 이유는 임직원들이 기술보호에 대한 의식이 부족하여 기술보호관리 규정을 제대로 숙지하지 않기 때문이다.

따라서 기술보호 사고를 미연에 방지하거나 기술보호 사고가 발생한 경우 경제적 피해를 최소화하기 위해서는 전 직원을 대상으로 기술보호관리 교육을 정기적 또는 수시로 실시하여 임직원들이 규정을 제대로 숙지하고 실천할 수 있도록 하여야 한다.

11) 국가연구개발사업 기술보호 표준 매뉴얼, 미래창조과학부, 2015.8.

1. 기술보호 규정 제정 및 교육

(1) 보안 교육 실시

기술보호 담당자는 중소기업의 환경과 상황을 고려하여 기술보호관리 교육 시기와 실시횟수, 교육 내용 및 교육 방법 등에 관한 사항 등을 포함하여 기술보호교육 계획을 매년 초에 수립하여야 한다.

(2) 기술보호 교육 실시 횟수

(정기교육)기술보호 교육은 시행 계획에서 정한 바에 따라 매년 정해진 시점에 정기교육을 실시하되, 최소한 매년 1회 이상 시행하여야 한다.

(수시교육)신입 및 경력 직원이 입사한 경우 또는 기술보호 규정이 개정된 경우와 기술보호 사고가 발생한 경우를 포함하여 중소기업 대표자 또는 기술보호 담당자가 기술보호 교육이 필요하다고 인정한 경우에는 해당자를 대상으로 수시로 교육을 실시하여야 한다.

(3) 기술보호 교육 시행 방법

기술보호 교육을 실시하는 방법은 집합교육, 온라인 교육, 유인물 배포 등 교육시기와 중소기업의 교육 여건에 따라 기술보호 담당자가 효율적인 보안교육 방법을 선택하여 실시하여야 한다.

기술보호관리 교육을 실시하기 전에 전 직원을 대상으로 교육 실시 관련 내용을 사전에 공지해야 한다.

〈표 5-3〉 기술 보호 교육 유형

교육 방법	장 점	단 점
집합교육	<ul style="list-style-type: none"> • 학습자의 성실성과 참여도 관리가 용이 • 교습자와 학습자간 상호작용 가능 • 온라인교육 대비 시스템 구축을 위한 초기 비용 불필요 • 체험적 요소가 중요한 학습과정에는 적절 	<ul style="list-style-type: none"> • 교육시간, 공간, 이동에 따른 제약사항 발생 • 교육장소, 교육 부대비용 증가 • 일회성 교육으로 학습 효과 저조
온라인 교육	<ul style="list-style-type: none"> • 교육 시간과 공간 제약 없이 교육 대상자들이 편리한 방식으로 교육 수강 • 자료공유가 쉽고 최신 정보 제공 • 학습자의 심리적 부담 최소화 • 지속적인 반복학습이 가능하여 학습효과 증대 	<ul style="list-style-type: none"> • 학습자의 성실성과 참여도 관리의 어려움 • 교습자와 교육 대상자간 상호작용 부족 • 시스템 구축에 따른 과다한 초기비용 발생 • 교재개발 시스템 운영등 지속적인 투자 필요 • 체험적 요소가 중요한 학습과정에는 부적절
유인물 배포	<ul style="list-style-type: none"> • 교육시간, 장소, 이동에 따른 제약 없이 교육 가능 • 교육 비용이 가장 저렴 • 수시 반복 학습 가능 • 학습자의 심리적 부담 최소화 	<ul style="list-style-type: none"> • 학습자의 성실성과 참여도 관리의 어려움으로 학습효과가 가장 저조 • 교습자와 교육 대상자간 상호작용부족 • 체험적 요소가 중요한 학습과정에는 부적절

(4) 기술보호 교육 사후관리

기술보호관리 교육은 모든 임직원이 참석하는 것을 원칙으로 하여야 하며, 부득이한 사유로 교육에 참여하지 못한 임직원은 차후에 별도 교육을 실시하거나 유인물 배포, 전자메일로 유인물 발송 등 교육내용을 숙지할 수 있도록 조치해야 한다. 교육대상자들로부터 설문조사를 실시한 후 미비한 사항에 대한 개선책을 마련하여 다음 교육계획 수립 시 반영해야 한다.

2. 기술보호 우수자에 대한 조치

기술보호 사고를 예방하기 위해서는 정기적인 보안교육도 중요하지만 임직원들이 이러한 교육내용을 몸소 실천하는 것이 더 중요하다. 따라서 정기 또는 불시 보안 점검을 실시하여 직원들의 사기진작 및 공로를 치하하기 위하여 기술보호 우수자들에게 포상을 실시하여야 한다. 이를 통해 임직원들의 적극적인 참여를 유도하고 임직원들의 보안 의식을 제고할 수 있다.

(1) 기술보호 우수자 선정 및 포상 기준 마련

중소기업 자체적인 사칙에 의거한 기술보호 우수자 선정 및 포상 기준을 수립하는 편이 바람직하다. 선정 기준은 자체적으로 실시한 정기 또는 불시 기술보호관리 점검을 통하여 기술보호 이행 성적이 우수한 임직원을 선정해야 한다.

(2) 기술보호 우수자 선정 절차 수립

기술보호 우수자는 자체 기술보호심의회 또는 인사위원회 등의 심의를 거쳐 선정하여야 한다. 기술보호 담당자는 심의에서 최종 확정된 보안우수자 후보를 중소기업의 대표자에게 보고하여 최종 승인을 받아야 한다.

(3) 기술보호 우수 사례 확산

기술보호 우수자는 내부 게시판에 통하여 전 직원들에게 공지하고 우수 사례를 임직원들에게 공유할 수 있도록 게시판 또는 유인물을 제작·배포하여 보안의식 수준을 제고 하여야 한다.

3. 기술보호 위반자에 대한 조치

기술보호 규정¹²⁾을 위반하여 중요한 기업의 기술 및 관련 연구정보 혹은 성과물이 무단으로 외부에 유출되는 유출사고를 일으킨 위반자는 그에 상응하는 처벌을 받아야 한다. 이를 통해 기술보호 사고에 대한 경각심을 불러일으키는 효과를 기대할 수 있다.

〈표 5-4〉 기술보호 위반자 기준

1. 기술정보 및 비밀정보 유출

- (1) 기술정보 누설
 - 개인의 목적(영리·비영리)을 위하여 고의로 핵심 연구 산출물 및 성과물 등을 외부로 유출한 경우
 - 핵심 연구 산출물 및 성과물 등을 외부로 유출하는데 가담한 경우
- (2) 기술정보 분실
 - 보안과제 또는 대외비에 해당하는 연구 산출물 및 성과물을 분실한 경우
 - 분실 신고 등을 제대로 이행하지 않는 등 적절한 조치를 취한 않은 경우
- (3) 연구보안사고 발생 사실 노출
 - 연구보안사고에 대한 조사가 완료되기 전에 관련 정보를 외부로 유출한 경우

2. 연구개발정보 관리 위반

- (1) 연구개발기술보호등급 관리 위반
 - 연구 산출물 및 성과물에 대한 보안등급을 부여하지 않은 경우
 - 연구 산출물 및 성과물의 보안등급을 과소 또는 과대 분류한 경우
- (2) 연구 산출물 관리 위반
 - 연구 산출물 및 성과물을 방치하거나 비밀보관한다.에 보관하지 않은 경우
 - 연구 산출물 및 저장매체를 복구할 수 없도록 완전하게 폐기하지 않은 경우
 - 보안과제 및 대외비의 연구 결과물(보고서 등)을 제한 없이 외부로 배포한 경우
 - 승인받지 않은 비밀자료 및 대외비 문서를 열람하거나 복사하는 경우
- (3) 연구개발 성과물관리 확보 소홀
 - 보안과제 및 핵심기술에 대한 성과물의 영업비밀 또는 특허권, 지식재산권 확보를 등한시하여 기술적·경제적 손실이 발생한 경우

3. 출입통제 위반

- (1) 인가되지 않은 제한구역 또는 통제구역을 출입한 경우
- (2) 노트북, 외장형 디스크, USB 등 저장매체를 사전 허가없이 반·출입한 경우
- (3) 촬영제한구역에서 사전 허가 없이 사진을 찍거나 동영상을 촬영한 경우
- (4) 정기적 출입자로부터 보안서약서를 받지 않은 경우
- (5) 보안과제와 관련하여 외부방문자 출입 시 직원이 방문자와 한.꺼 동행하지 않은 경우

12) 기술보호 규정이란 기업별 특성에 맞는 정보보호 및 운영에 관한 보안규정을 말하며, '보안정책서' 또는 '보안지침서' 등에 표현된 규칙 등을 말한다.

제1절

기술보호 핵심 수칙

1. 기술보호를 위한 관리규정을 갖추고 실시해야 합니다.

기술보호 관리 규정을 제정하여 영업비밀 분류 및 취급, 종업원의 의무, 영업비밀 보관·파기, 출입자 통제 등에 관하여 정리하고 관리해야 합니다.

2. 보안관리 전담인력은 반드시 지정해야 합니다.

보안담당자를 지정하여 기술보호 감사를 정기적으로 실시해야 합니다.

3. 전 직원을 대상으로 정기적인 기술보호 교육을 실시해야 합니다.

반기별 또는 분기별로 정기적인 교육을 통해 기술보호 중요성을 알려주세요.

4. 전 직원 비밀유지서약서, 핵심직원은 전직금지서약서를 체결해야 합니다.

모든 직원과 비밀유지서약서 체결, 핵심개발자 및 임원과 전직금지서약서 체결해 기술을 지켜야 합니다.

5. 핵심기술 인력이 퇴직할 경우 철저한 사후관리를 해야 합니다.

인력의 퇴직시 영업비밀 인수인계를 철저히 하고, 서류/기술정보 반납 및 파일삭제 확인서를 받고 영업비밀 준수 의무 및 처벌규정 상기시켜 주셔야 합니다.

6. 중요 기술은 영업비밀로 분류하고 별도로 관리해야 합니다.

기업자산(기술) 중 영업비밀을 파악하고 등급(극비/비밀/대외비)을 부여하고 표시하여 관리해야 합니다.

7. 중요서류는 별도 보관하고 접근·복제·반출은 철저히 관리해야 합니다.

중요서류는 별도 잠금장치가 있는 곳에 보관하고, 자료를 임의로 복제와 반출할 수 없도록 관리번호를 부여한 후 관리해야 합니다.

8. 중요설비·장치가 설치된 곳은 통제구역으로 설정하고 관리해야 합니다.

개발 및 제조설비 지역은 '출입통제구역'으로 정하고, 카메라 및 스마트폰의 반입을 금지하며 감시카메라를 설치해야 합니다.

9. 중요한 기술은 특허나 기술자료 임치로 보호해야 안전합니다.

개발한 기술을 특허등록하고, 영업비밀은 기술자료 임치로 보호해야 안전 합니다.

10. 정보시스템에 대한 보안을 철저히 해야 합니다

네트워크 인증, 데이터 암호화, 비밀번호의 주기적 변경, 허가된 USB 사용하기, 기술지킴이(보안관제) 서비스를 활용해 기술자료를 지켜야 합니다.

【 행동 수칙 】

행동수칙 1(기술보호를 위한 관리규정을 갖추고 실시)

- ① 중소기업이 보유하고 있는 기술을 보호하기 위해 필요한 것 가운데 가장 기본이 되는 것이 바로 중소기업 기술보호규정이다. 중소기업이 보유하고 있는 기술을 보호하기 위해 필요한 것 가운데 가장 기업별 특성에 맞는 기술보호에 관한 규정을 제정한다.
- ② 제정된 중소기업 기술 보호 세부규정은 임직원들에게 공지하고, 주기적으로 제·개정하며, 그 효력이 발휘될 수 있도록 한다.
- ③ 기술보호규정은 기술정보가 담긴 문서의 분류 및 취급, 출입자 통제, 인적자원 관리, 정보시스템 관리, 보안사고 대응절차 등을 담고 있어야 한다.

행동수칙 2(보안관리 전담인력은 반드시 지정)

- ① 중소기업의 규모에 따라 기술보호를 위한 보안전담조직을 두거나 기술보호 담당자를 지정한다.
- ② 기술보호 담당자는 영업비밀에 대해 관리적, 물리적, 기술적인 보안조치를 취하고, 정기적인 교육을 실시하며 관련 규정들을 정비한다.
- ③ 기술보호 담당자 외에 각 부서별로 보안담당자를 지정하여 기술보호 효율성을 높인다.

행동수칙 3(정기적인 기술보호 교육을 실시)

- ① 중소기업 기술유출 사례의 대부분은 임직원에게 의한 것이므로 제도적 장치와 물리적 조치와 아울러 임직원의 인식제고를 위하여 반기별 또는 분기별로 교육을 실시한다.
- ② 출입통제, 문서보안, PC보안 등 보안규정이나 지침의 내용을 숙지시키고, 출퇴근 시 스크린 및 방송 등을 통해 보안인식을 고취시킨다.

행동수칙 4(전 직원 비밀유지서약서, 핵심직원은 전직금지서약서를 체결)

- ① 기술보호의 경각심을 고취시키고, 향후 기술유출 사고 발생 시 입증자료로 활용하기 위하여 내부 모든 직원들에게 비밀유지서약을 징구한다.
- ② 비밀유지서약서는 입사 시뿐만 아니라 공동프로젝트, 투자계약, 라이선스 거래, 납품, 외주인력 활용 등에 있어서도 징구하여야 한다.
- ③ 핵심기술인력과 임원 등에게는 전직금지약정 또는 경업금지약정을 사전에 체결하여야 한다. 약정 시 전직(경업)금지 기간 및 분야를 특정하고 퇴직 시 적절한 보상을 지급한다.

행동수칙 5(핵심기술 인력이 퇴직할 경우 철저한 사후관리)

- ① 핵심 연구인력은 회사의 핵심기술을 알고 있으므로 퇴직 시 비밀유지의무, 전직금지 및 경업금지약정서를 징구하고 범위반시 조치에 대해 숙지시킨다.
- ② 핵심 임직원이 퇴직한 경우 회사와 우호적인 관계를 유지하도록 다방면의 조치를 취하고 일정기간 경쟁사에서 기술개발 일을 하는지 등을 모니터링한다.
- ③ 임직원이 퇴직을 할 경우 사전에 기술자료에 대한 철저한 인수인계를 실시하고, 관련 서류 및 파일 등 일체를 반납하고 회사 외부에 저장되어 있는 문서 등을 폐기하도록 하고 확인서를 받아 둔다.

행동수칙 6(중요 기술은 영업비밀로 분류하고 별도로 관리)

- ① 중소기업이 보유하고 있는 주요 기술정보 자산을 연구개발 - 제조-판매-기타 영업활동 프로세스별로 파악하고 일반정보와 영업비밀을 구분한다.
- ② 기술정보의 이력을 체계적으로 관리하기 하여야 하며, 정보 유통현황을 파악해야 한다. 즉, 임직원들의 기술정보 흐름 및 중요 정보 저장 매체의 위치 등을 파악해야 한다.
- ③ 기밀정보는 명칭, 관리번호, 비밀등급, 등록일, 보존기간, 기록매체, 비치장소, 관리책임자를 표시하여 목록을 작성한다.
- ④ 분류된 모든 기술정보자산은 담당자가 년 1회 주기적으로 업데이트하여 목록을 검토한다.

행동수칙 7(중요서류는 별도 보관하고 접근·복제·반출은 철저히 관리)

- ① 핵심 기술 관련 문서 등 자료는 시정장치가 있는 캐비닛에 별도 보관한다.
- ② 각 직원별로 업무수행에 필요한 기술자료에만 접근권한을 부여하고, 영업비밀 열람/사용/복사/전송 등을 업무에 필요범위에서만 허용한다.

- ③ 접근권한 제한과 열람/사용/복사/전송 등 내역을 관리할 수 있는 방안을 마련하거나 솔루션을 도입하여야 한다.

행동수칙 8(중요설비·장치가 설치된 곳은 통제구역으로 설정하고 관리)

- ① 기술을 보호하기 위해 가장 기본적인 방법은 주요 사무실, 연구소, 중요 설비 및 장치 설치장소, 지역 등을 외부인 및 관련 없는 내부인의 출입 통제 구역으로 지정 하는 것이 중요하다.
- ② 침입방지를 위해서 대상기관이 보유하고 있는 시설을 분류하여 그 분류에 따라 접근 권한에 차등을 주고, CCTV 등 물리적 보안 장치를 적용한다.
- ③ 외부인의 출입 관리 시 휴대폰 카메라사용을 금지하고, 직원들의 휴대폰 카메라 사용에 대해서도 최대한 제한한다.

행동수칙 9(중요한 기술은 특허나 기술자료 임치로 보호)

- ① 중소기업이 경쟁사가 알지 못하는 유용한 기술을 개발한 경우 특허(실용신안) 또는 영업비밀로 보호할지 결정하여 권리화하여야 한다.
- ② 특허의 등록요건을 만족하는 신기술이고 기술의 주기가 짧고 제품 출시 시 공개되는 기술인 경우에는 독점배타적 권리인 특허(실용신안)으로 보호하는 것이 바람직하다.
- ③ 경제적 가치를 가지는 유용한 기술상 경영상 정보는 영업비밀로 유지하되 부정경쟁방지법에서 요구하는 합리적 노력으로 비밀로 유지하여야 한다.
- ④ 기술자료 임치제도를 활용하여 기술상의 비밀정보를 보호하고 향후 분쟁 시에 입증자료로 활용한다.

행동수칙 10(정보시스템 보안 철저히)

- ① 네트워크 보안을 위해 암호화된 패킷을 사용하고, 보안프로그램을 설치한다.
- ② 임직원 PC의 비밀번호 및 중요 데이터는 주기적으로 변경·업데이트하고, 허가된 USB만을 사용한다.
- ③ 중소기업청이 지원하는 보안관제서비스, 기술유출방지시스템 구축 등 지원사업을 활용한다.
- ④ 기업 내부에서 CD, USB, 플래쉬카메라 등 전자매체에 관리번호를 부여하고 정보의 저장 가능한 외부 매체에 대해서는 최소한으로만 사용하도록 제한하고 외부 유출에 대해 관리한다.
- ⑤ DRM/포렌식을 적용하여 기술유출을 예방하고 증거자료를 확보하기 위한 기술을 차용한다.

제2절

관련 법령 및 중소기업기술보호 지원제도

1. 기술보호 관련 법령

정부는 국내 기업의 기술유출 방지를 통한 경쟁력을 제고하기 위해 여러 법률을 제·개정하여 보호하고 있다. 대표적 법률로 「중소기업기술보호 지원에 관한 법률」, 「산업기술의 유출방지 및 보호에 관한 법률」, 「부정경쟁방지 및 영업비밀 보호에 관한 법률」 등이 있으며, 타 법률 등에서도 부분적으로 기술보호 관련 조항을 마련하고 있다.

〈표 6-1〉 중소기업기술보호 관련 법률

구분	주요 보호대상 및 내용	주무부처
중소기업기술보호 지원에 관한 법률	- 중소기업기술보호에 관한 지원 정책 - 분쟁조정·중재 지원	중소기업청
중소기업 기술혁신 촉진법	- 중소기업이 개발한 핵심기술	
대·중소기업 상생협력 촉진에 관한 법률	- 기술자료 임치제도(기술탈취 방지) - 정당한 이유 없는 기술자료 요구 금지	산업통상자원부
산업기술의 유출방지 및 보호에 관한 법률	- 산업기술/국가핵심기술(기업·연구소·대학) - 국가핵심기술의 지정, 수출승인(신고) - 산업기술의 부정 취득 등 금지	
대외무역법	- 전략물자에 대한 수출 통제	
외국인투자 촉진법	- 국가안보와 관련된 외국인투자 제한	
산업 발전법	- 산업적 가치가 높은 중요한 기술을 개별 법률의 목적에 따라 보호	
부정경쟁방지 및 영업비밀보호에 관한 법률	- 영업비밀 보호(기업) - 영업비밀의 부정 취득 등 금지	특허청
발명진흥법	- 직무발명제도 - 사용자에게 의한 직무발명 권리 승계와 직무발명 보상	
특허법	- 자연법칙을 이용한 기술적 사상의 창작으로 고도한 것 - 산업 상 이용가능성, 신규성, 진보성 포함한다.	특허청
형법	- 절도죄, 업무상 배임·횡령죄, 증거 인멸죄 등	법무부
저작권법	- 인간의 사상 또는 감정을 표현한 창작물	문화체육관광부

「중소기업기술보호 지원에 관한 법률」주요내용 (제정 '14.5.28 / 시행 '14.11.29)

- 제1장 총칙(제1조~제4조)

※목적, 정의, 정부 등의 책무, 다른 법률과의 관계

- 제2장 중소기업기술보호에 관한 지원계획의 수립 및 추진(제5조~제8조)

※중소기업기술보호 지원계획 수립(3년), 정책자문, 중소기업기술보호역량 강화를 위한 실태조사, 보호지침 제정 등

- 제3장 중소기업기술보호를 위한 지원 사업(제9조~제13조)

※임치제도를 활용한 담보 지원 사업 및 국가연구 개발사업 성과물의 보호 지원, 중소기업기술보호 진단 및 자문, 해외진출 중소기업기술보호 지원 사업 추진 등

- 제4장 중소기업기술보호의 기반 조성(제14조~제22조)

※중소기업기술보호전담기관 지정, 보안기술 개발의 촉진 및 보급, 기술보호 전문인력 양성, 관제서비스, 보안시스템 구축 지원
※중소기업기술보호에 관한 국제협력 활성화, 대·중소기업간 상생협력, 중소기업기술보호 기여자 포상 등

- 제5장 분쟁조정 및 중재(제23조~제28조)

※중소기업기술 분쟁조정 및 중재위원회 설치 및 운영 등

- 제6장 보칙 및 제7장 벌칙(제29조~제34조)

※필요한 경우 조세감면 기능, 비밀유지 의무 및 위반에 대한 벌칙 등

2. 중소기업기술보호 관련 지원제도**중소기업청**

1) 기술보호 통합상담센터(대·중소기업협력재단 02-368-8787)

- 중소기업 기술보호 전담기관(대·중소기업협력재단) 내 통합상담센터를 구축하여 종합 상담기능 수행 및 유관기관 연계(무료)

2) 기술보호 전문가 상담·자문 (대·중소기업협력재단 02-368-8787)

- 보안 및 법률분야의 중소기업 기술보호 전문가가 기업 현장으로 방문하여 중소기업의 보안수준 및 실태, 문제점 등을 진단하고 해결방안 제시(무료)

3) 기술자료 임치제도(대·중소기업협력재단 02-368-8787)

- 중소기업의 핵심기술 정보를 제3의 신뢰성있는 기관으로 안전하게 보관(임치)하여 기술유출 발생 시 임치한 기술에 대한 보유사실 입증

4) 기술자료 입치 활용지원(대 · 중소기업협력재단 02-368-8787)

- 중소기업이 입치한 기술을 활용하여 담보대출을 통한 중소기업 사업화 자금을 마련하고 또한 기술 거래를 지원

5) 기술자료 입증서비스 - 원본증명 서비스(대 · 중소기업협력재단 02-368-8787)

- 중소기업이 핵심기술을 디지털화 하여 보관하고 해당 자료에 대한 전자지문과 타임 스탬프를 인증 받아 향후 중소기업이 핵심기술에 대한 개발시점 및 내용 등에 대해 입증이 필요하면 해당 입증

6) 중소기업기술 분쟁 조정 · 중재(대 · 중소기업협력재단 02-368-8787)

- 해당분야의 전문가로 구성된 중소기업 기술분쟁 조정 · 중재위원회의 조정부 또는 중재부가 기술유출 피해를 입은 중소기업 대상으로 신속하고 원만하게 분쟁해결 지원

7) 기술유출 방지시스템(중소기업기술정보진흥원 042-388-0758~60)

- 중소기업의 보안인프라에 대한 정밀진단 및 설계후, 기업환경에 적합한 보안시스템 구축 지원(물리적 · 기술적 보안솔루션)

8) 기술지킴 서비스(한국산업기술보호협회 02-3489-7050~3)

- 24시간 보안관제 업무부터 help desk 운영까지 다양한 서비스를 무료로 지원하며 내부정보유출방지서비스 및 악성코드탐지서비스 신청 시 해당 소프트웨어 프로그램 무상 제공

산업통상자원부

1) 국가핵심기술 체계적 지원관리 · 운영 (한국산업기술보호협회, 02-3489-7032)

- 산업기술보호 인력관리 가이드, 해외기술수출 통합가이드라인 배포
- 국가핵심기술 온라인지원시스템을 통한 국가핵심기술 관련 정책 · 법률, 기술유출 사례 · 통계, 제도 및 절차 등 정보 제공

2) 국가핵심기술 통제관리 기반 구축, 국가핵심기술 위원회 운영(한국산업기술보호협회 02-3489-7032)

- 국가핵심기술 보유기관 대상, 보안닥터(보안전문가) 현장방문을 통해 보유기관의 기술유출 취약점 점검 및 애로사항 해결 지원
- 보안관리사 운영 · 공인화

3) 산업기술 분쟁 조정 운영 및 지원(한국산업기술보호협회 02-3489-7033)

- 산업기술 유출 분쟁에 대한 신속한 조치 및 조정을 위해 산업 기술분쟁 조정위원회 운영
- 분쟁예방 상담안내 및 정보 지원

4) 대·중소기업 보안역량 동반성장 기반 확대 프로그램(한국산업기술보호협회 02-3489-7034)

- 국가핵심기술 및 주요 첨단기술 보유 대·중소기업간 컨소시엄 대상 보안역량 동반성장 활성화 지원 프로그램 운영
- 대중소기업간 컨소시엄을 구성하여 기술유출 교육 진행, 기술유출의 취약점을 점검하여 개선안을 제시하는 업무

5) 산업기술보호 인식확산 및 지원서비스(한국산업기술보호협회 02-3489-7012)

- 산업기술보호 해피콜센터 상담(기술보호상담) 관련 정보지원 시스템 운영
- 국가핵심기술 수출신고대상 여부, 영업비밀 보호서약서 표준안, 시제품 반출의 수출 승인신고 여부 등 검토

특허청

1) 영업비밀 보호 컨설팅(한국특허정보원 영업비밀보호센터 대표번호: 1566-0521)

- 기업이 자사의 영업비밀 관리상 문제점을 파악하고 개선할 수 있도록 영업비밀 전문가가 실태 진단 및 실현 가능한 관리방안 제시(무료)

2) 영업비밀 보호교육(한국특허정보원 영업비밀보호센터 대표번호: 1566-0521)

- 영업비밀 보호문화 확산 및 기업의 영업비밀 관리·분쟁 대응 능력 배양을 위해 설명회, 기업방문 등 영업비밀 보호 교육 실시(무료)

3) 영업비밀 원본증명 서비스(한국특허정보원 영업비밀보호센터 대표번호: 1566-0521)

- 영업비밀 보유자가 해당 영업비밀 보유에 대한 입증이 필요한 경우, 영업비밀 원본존재 여부, 보유자 및 보유시점을 입증해주는 서비스(유료)

4) 영업비밀 보호·관리 시스템(한국특허정보원 영업비밀보호센터 대표번호: 1566-0521)

- 영업비밀 자료를 효율적으로 관리하고, 비밀취급 인가를 받은 사용자만이 비밀문서를 접근·활용할 수 있도록 하는 영업비밀 관리 전문 시스템(무료)
- 영업비밀 자료 등록·분류, 원본증명 서비스 연계, 접근자 권한 설정, 취급이력 관리, 이력·통계 관리 기능 등을 구현한 영업비밀 자료 관리 시스템

5) 초동대응 법률자문 지원(한국특허정보원 영업비밀보호센터 대표번호: 1566-0521)

- 영업비밀 전문 변호사로 구성된 민간 자문단이 영업비밀 피해와 관련하여 부경법 적용 가능여부, 법률 검토에 필요한 자료목록, 소송비용 견적 등 상담(무료)
- 센터 내 변호사를 통해 초동 대응 피해에 대한 상담 진행, 전문가 인력 풀에서 인력 배치, 1회 50만원 비용 지원

공정거래위원회

1) 기술자료 제공 요구 금지(공정거래위원회 044-200-4591)

- 기술자료 제공 요구행위는 원칙적으로 금지되며 원사업자가 정당한 사유를 입증한 경우에 한하여 기술자료 제공 요구 가능

2) 기술자료 유용 금지(공정거래위원회 044-200-4591)

- 원사업자가 정당하게 기술자료를 취득한 경우에도 동 기술자료를 본인 또는 제3자를 위하여 유용불가

3) 기술자료 관련 분쟁조정제도(한국공정거래조정원, 1588-1490)

- 분쟁당사자(원·수급사업자)간 신속한 피해구제를 위해 하도급법에 의거 설치된 분쟁조정협의회에서 분쟁 해결 지원
- 한국공정거래조정원에서 운영하는 다양한 분쟁조정 중, “하도급 분쟁조정”에 해당
- 정당한 이유 없이 수급사업자에게 기술자료를 제공하도록 요구했을 경우

경찰청

1) 산업기술유출 수사활동 강화(산업기술유출 수사지원 센터 1566-0112)

- 국가 핵심기술 해외유출 방지 및 중소기업 보호를 위한 단속 강화
- 국내 기업의 산업기술·영업비밀 해외유출 피해에 대한 집중 수사로 국가 산업경쟁력 제고에 기여

- 대기업/중견기업의 지위를 악용한 중소기업 기술탈취 행위 등 수사를 통해 中企 기술보호 활동 전개
- 기업·기업단체 등 대상 산업기술유출 예방홍보 교육 실시
 - 社內 보안전문가 양성과정 교육 및 기술유출 피해기업 합동간담회 등 개최
- 관계기관 협력 강화, 피해기업 대상 보안실태 합동진단 등 기술유출 예방을 위한 공동 대응책 발굴

기술보호상담 통합포털(www.ultari.go.kr)을 통해 영업비밀 보안서약서,
보안지침 등 중소기업 기술보호 서식 및 자료 다운로드 가능

중소기업 기술보호 지침

발행처 : 대·중소기업·농어업협력재단
주소 : 서울시 구로구 디지털로 32길 29 키콕스벤처센터 4층
대표전화 : 02)368-8787



중소벤처기업부



대·중소기업·농어업협력재단