

[데이터 경제 시대의 도래, 기업이 대비해야 할
주요 법안서]

18차시. 기업의 점검사항 및 대비

학습목표
<ul style="list-style-type: none">▪ 학습내용: 해당 차시에서 학습할 학습주제(목차)를 제시해 주세요.▪ 학습목표: 해당 차시 학습을 통해 <u>학습자들이 달성해야 할 목표</u>를 학습내용과 연계하여 작성해 주세요.

▶ 학습내용

1. 기업의 영업비밀 관리체계 수립
2. 기업의 영업비밀 관리 및 보호 대책

▶ 학습목표

1. 기업의 영업비밀 관리체계 수립에 대해 설명할 수 있다.
2. 기업의 영업비밀 관리 및 보호 대책에 대해 설명할 수 있다.

학습내용
<ul style="list-style-type: none"> ▪ 학습내용의 위계 파악을 위해 일관성 있는 번호 체계로 작성해 주세요.

VI. 기업의 점검사항 및 대비

1. 기업의 영업비밀 관리체계 수립

(1) 기본 방침

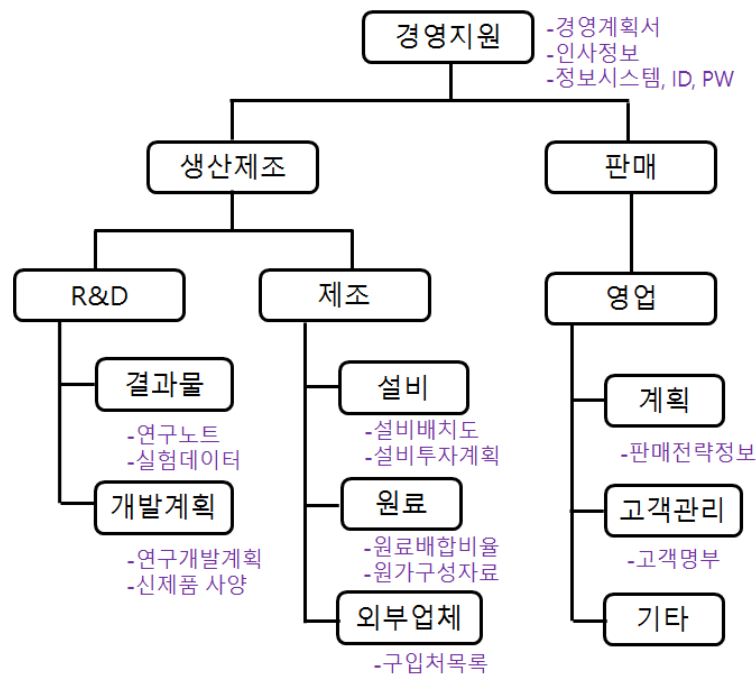
영업비밀 관리를 할 때에는 물리적, 인적, 제도적 관리를 신속하고 정확하게 실시할 수 있도록 하여야 한다. 즉, 영업비밀의 유출을 방지하기 위해서는 그 영업비밀을 물리적으로 관리하고 여기에 접근하는 자를 인적으로 관리하는 것에 더하여, 제도적으로 기업 시스템을 관리하여야 한다. 영업비밀 관리의 기본 방침은 영업비밀 관리에 관한 조직의 의사를 간결하고도 이해하기 쉬운 형태로 문서화하여 전 종업원에게 주지시키는 것이다. 또한 조직의 최고 책임자가 실시 상황을 확인하고 이를 재검토하며, 개선하여 사건 발생을 방지하는데 노력하여야 한다.

(2) 실시 계획

영업비밀 관리의 기본방침만으로는 반드시 구체적인 영업비밀 관리 절차가 분명해진다고는 할 수 없기 때문에, 구체적인 영업비밀 관리 목적과 목표를 정하여 이를 달성하기 위한 실시계획을 별도로 책정하여 실행할 필요가 있다. 영업비밀의 관리에 있어 실시계획으로 중요하고도 긴급한 과제에 대응하는 것으로부터 시작하여 점차적으로 영업비밀 유출 위험을 경감시켜나가는 방향으로 관리 체계를 수립하여야 한다. 영업비밀 관리체계를 수립할 때에는 현재의 관리수준을 파악하고 목표관리수준을 설정하는 것이 효과적이다. 현재의 관리상황 및 관리수준을 파악하는 방법으로써, 각 영업비밀별로 별첨의 서식을 마련하여 각 항목별 비밀 관리가 잘 될 수 있도록 한다. 이 서식은 특허청이 판례 분석을 바탕으로 실제 비밀관리성을 인정받을 수 있도록 꼭 필요한 요소들을 포함시켜 서식을 완성한 것이다.

(3) 기업 업무 프로세스별 영업비밀 관리 및 보호

기업의 영업비밀을 효과적으로 관리하기 위해서는 생산, 판매, 경영지원 등 각 업무 프로세스별로 해당 부서가 해당 영업비밀을 파악하고 관리하여야 한다. 또한 해당 업무의 중요 정보가 영업비밀로서 보호할 가치가 있는지에 대해서도 판단하여야만 한다. 다만, 종업원이 기업 내의 모든 영업비밀을 관리하도록 하는 것은 업무 효율을 저하시킬 수 있으므로 해당 업무 관련 영업비밀만을 철저히 관리하도록 조치하여 업무 효율을 높일 수 있어야 한다.



1) 생산·제조 단계

① R&D

정보의 내용	구체적 예	유출될 경우 발생할 수 있는 문제
실험 데이터, 분석 데이터	실험 데이터 파일, 분석 데이터 파일	타사의 데이터를 자사의 신제품 개발 및 개량에 이용 가능(실패 데이터는 보다 실현 가능성이 높은 목표 설정, 비용 절감이 가능)
연구 재료, 연구 시료	화합물, DNA칩, 생물조직	타사의 연구대상을 입수하여 자사의 신제품 개발에 이용 가능
연구 개발의 성과(기술 정보, 기술적 지견)	연구 보고서, 미발표의 연구논문, 기술회의 의사록, 기술 데이터	타사의 미발표의 연구개발의 성과를 이용하여 자사 제품의 개량 또는 신제품의 신속한 시장투입이 가능

발명 내용	특허 신청서, 저축조사 보고서, 발명기록	발명 관련 자료, 실험 데이터를 이용하여 자사의 제품의 개발 및 개량을 실시하고 시장 경쟁을 유리하게 전개 가능
신제품이나 연구 개발 계획	신제품 개발 계획서, 연구개발 계획서, 신제품 개발 계획	타사 신제품의 개발 목표, 연구테마, 연구 개발의 대상 등을 분석하여, 자사의 연구 활동을 유리한 방향으로 개선 가능
신제품의 개발 체제, 조직	신제품 개발 담당자 세부 조직도	타사의 신제품 개발을 위한 조직, 업무 분담, 역할, 배치 등으로부터 타사의 개발내용을 분석하여 자사의 개발에 이용 가능
신제품의 사양·설계 내용	시제품(샘플), 시작도면, 신제품사양·규격서, 설계도, 사진	타사의 신제품 사양에 관한 정보를 이용하여 자사의 대항제품을 신속하게 개발 가능

② 제조

정보의 내용	구체적 예	유출될 경우 발생할 수 있는 문제
설비 투자 계획	설비 투자 계획서, 설비 사양서	타사의 설비 투자 계획 등을 알고 자사의 설비 투자 내용을 개선 가능
각종 제품의 생산 계획, 생산 능력	생산 계획서, 설비 사양서	타사의 생산 계획이나 생산 능력을 알고 자사 제품의 가격 설정이나 공급량 조정에 유리한 결정 가능
제조 설비의 배치, 제조 공정, 설비 조작 방법	설비 배치도, 공장 레이아웃, 제조 매뉴얼, 공정 매뉴얼, 관리 프로그램	타사의 설비 배치를 분석하여 제품의 제조방법, 공정, 시스템을 이해하고 동등 제품이나 경쟁 제품의 제조에 이용 가능
제조 설비·공구·금형의 설계 내용	사양서, 설계도, 설계의 전자 데이터, 사진, 모형, 부품도	타사의 독자적인 사양의 설비 내용을 알고 설비에 포함되어 있는 제조 노하우를 이해하여 쉽게 경쟁 제품을 제조 가능
원료 규격 및 검사방법, 사용재료 및 재료의 배합 비율	원료 등의 규격서, 검사 매뉴얼, 배합 비율	제품 등을 제조하기 위해 어떤 재료를 어떤 비율로 사용하는가에 대한 정보를 알고 쉽게 유사 제품을 제조 가능
각종 제품 등의 품질 관리 방법	품질 관리 매뉴얼	양질 또는 균질의 제품 제조를 위한 독자적 수법을 알고 동일 품질의 제품을 쉽게 생산·출하 가능
각종 제품 등의 원가 정보	원가 계산서, 원가 구성 자료	타사 제품의 원가를 알고 자사 제품의 가격 결정 등 판매 전략 수립에 이용 가능
시장 부적합이나 품질 클레임 대응 및 관리의 방법	시장 부적합·클레임 대응 매뉴얼, 처리 보고서, 품질 관리 기록	타사의 정보를 통해 자사의 품질 관리에 이용 가능
구입처나 위탁처에 관한 정보	구입처 리스트, 위탁처 리스트	타사의 구입처를 알고 비용, 품질, 개발, 안정 공급 등의 측면에서 보다 유리한 구입처를 개척 가능

2) 판매 단계

정보의 내용	구체적 예	유출될 경우 발생할 수 있는 문제
단기·중장기 판매계획	판매 계획서 및 각종 자료	타사의 계획을 알고 대항 수단을 검토하여 자사의 판매계획이나 판매촉진방법을 유리하게 결정 가능
판매 전략에 관한 정보	기획서, 계약서, 교섭 상대방과의 연락이나 협의 기록	타사와의 판매 제휴, 판로의 결정·변경, 대리점 정책 등에 관한 정보 등을 알고 자사가 경쟁 우위에 설 수 있는 판매 체제 등의 판매 전략을 기획 가능
시장 정보	조사보고서, 통계표, 설문조사 분석 리포트	타사가 조사한 제품·기술에 관해 조사·분석해서 얻은 시장 동향·고객 수요 동향·타사 동향 등의 정보를 이용하여 자사의 제품과 타사의 제품 간 차별화 가능
고객(기업)에 관한 정보	고객 명부, 고객 데이터, 고객 카드, 단골 기업 파악, 방문 기록	타사의 영업활동의 성과를 축적한 것으로 구입자를 구체적으로 파악하여 자사의 고객으로 유도 가능
제품·서비스의 가격에 관한 정보	원가 계산 자료, 가격표, 판매 수수료 일람표, 견적서, 발주서, 청구서	원가, 판매가격, 구입가격, 희망소비자가격, 할인 한도액 등의 설정 방법·기준 등 타사의 원가 등의 구성을 알고 자사의 최적의 대항책을 준비 가능
신제품에 관한 정보	신제품 사양서, 판매 계획서, 상표등록 준비 자료	타사가 신규로 시장에 투입하는 제품의 외관사양, 브랜드네임, 출원 전의 상표, 판매 시기 등의 정보를 알면 대항책을 기획하여 경쟁을 유리하게 전개 가능
발표 전의 광고·선전 정보	기획서, 발표용 자료	타사의 신제품 판매에 관한 구체적인 광고·선전 방법을 알고 자사의 경쟁 상품의 광고·선전을 유리하게 기획 가능
반품·클레임 처리에 관한 정보	클레임 처리 등을 위한 사내 문서, 원인 분석 데이터, 클레임 처리 보고서	취급 제품의 반품 품목, 수량, 반품원인, 고객으로부터의 각종 클레임 등의 정보 및 그 처리에 관한 정보 등을 이용하여 자사의 상품 개발을 보다 효율적으로 행하고, 경쟁 우위 판매 전략 구상이 가능
프랜차이즈의 경영 노하우	시스템 매뉴얼, 상품 진열 매뉴얼, 상품 리스트	프랜차이즈 비즈니스를 보다 효율적으로 전개 가능

3) 경영 지원

정보의 내용	구체적 예	유출 공개 시 발생하는 문제
경영 계획	중장기 경영계획서, 단기 경영계획서, 신규 사업	타사의 경영 계획, 주력 방침, M&A, 합병, 회사분할, 주식교환, 사업 이전, 업무 제

공표전의 중요한 경영에 관한 정보	계획서, 신제품 계획서 임원회, 경영 회의 등에 사용된 계획서 등의 자 료, 의사록, 계약서 등	휴, 해산, 자회사 설립 등의 중요한 구조 적 변경 등을 알고 유리한 경영 전략 수 립 가능
결산에 관한 정 보, 각 항목별 수 지정보, 자금계획	재무제표, 제품별 수지표, 자금 계획서	타사의 공표전의 재무 구조나 자금 상황 을 알고 자사의 경쟁 전략을 유리하게 계 획 가능
종업원 개인에 관한 정보	종업원명부, 급여명세표, 인사고과표	유능한 종업원에 관한 인사정보는 헤드헌 팅의 기초 데이터가 됨
정보 시스템	시스템 설계 및 구성도, 네트워크 구성도, 운용 매뉴얼, 백업 매뉴얼	타사의 기존 시스템의 구조를 파악하고 이와 동등하거나 그 이상의 기능을 가진 시스템을 단기간에 구축 가능
정보 시스템 접 근 계정 정보	계정 리스트, 패스워드 파일	타사의 비밀 정보를 쉽게 입수 가능

2. 기업의 영업비밀 관리 및 보호 대책

(1) 관리규정 제정

영업비밀을 효과적으로 보호하고 관리하기 위해서는 비밀관리에 관한 명문화된 규정을 제정하여 시행하여야 한다. 기업은 규정에 영업비밀 관리의 기본 방침, 실시계획 외에 영업비밀에 관한 각종 규정(영업비밀 관리체계, 영업비밀의 분류 및 취급, 종업원의 의무, 영업비밀 관리용기 및 보관장소의 지정, 영업비밀 관리기록부의 비치 및 활용, 출입자의 통제 등에 관한 사항 등)을 작성하여 문서화하여야 한다.

(2) 영업비밀 분류 및 표시

영업비밀로 관리할 정보에 비밀관리성을 여러 등급으로 나누어 각기 다른 수준의 관리체계를 구축하여야 한다. 예를 들어 경영상 매우 중요한 정보로 영구 보존하고 접근과 취급에 특별한 제한이 필요한 경우에는 ‘극비’, ‘극비’로 분류된 정보만큼 중요하진 않지만 기업의 경영에 큰 위협이 될 수 있어 장기적으로 보존해야 할 경우는 ‘비밀’, 일반적인 정보이지만 외부에 유출될 경우 악용의 소지가 있는 경우는 ‘사외비’ 등으로 구분하여 관리한다. 한편 해당 정보가 영업비밀로 관리하는 정보라는 것을 객관적으로 인식 가능하도록 하기 위하여, 영업비밀이 기록된 매체에 비밀이라는 것을 표시하여야 한다. 비밀 표시의 방법으로는 ‘비밀’ 등의 스탬프를 찍거나 스티커를 붙이는

방법이 대표적이며, 전자정보의 경우에는 영업비밀을 표시하는 데이터를 전자정보 자체에 입력하거나 파일 접근 암호를 설정하거나, 파일 자체를 암호화 하는 방법 등이 가능하다.

(3) 접근권한자 지정

영업비밀에 접근할 수 있는 접근권한자를 지정하는 것도 비밀관리성의 중요한 요소이다. 접근권한자는 본인이 취급하는 영업비밀의 중요성과 그 업무를 명확하게 인식하고 있어야 한다. 접근권한자가 비밀관리의 중요성을 인식하지 못하고 있는 경우에는 아무리 엄중한 비밀관리방법을 채택하더라도 실효성이 떨어질 수밖에 없다.

(4) 인적 관리

우리나라 영업비밀 침해의 대부분은 종업원에 의한 것으로 나타나고 있다. 아무리 제도적 장치와 물리적 조치가 완벽하다고 하더라도 종업원 관리를 소홀히 하게 되면 오랜 기간 연구개발한 노력의 성과가 종업원에 의해 외부에 유출될 수 있다. 종업원 관리는 예를 들어, 입사시 비밀유출금지 서약서 제출, 재직시 주기적인 보안교육 실시, 퇴직시 직업선택의 자유나 근로의 권리를 침해하지 않는 범위 내에서 동종업체 취업 및 경업 금지의무 부과를 실시하여야 한다. 단, 기업에 있어 인적관리는 무엇보다도 사용자와 종업원 간의 협력자적 동반관계가 중요하므로 평소에 사용자는 종업원에 대하여 각별히 관심을 가지는 한편, 종업원의 직무수행과정에서 발견 또는 창출된 영업비밀을 회사에 신고하여 영업비밀로 관리할 수 있도록 하는 영업비밀 신고제도를 도입하고, 신고된 영업비밀은 이에 상응하는 보상금을 지급토록 하는 제도도 아울러 마련함으로써 기업의 창의적 영업활동을 촉진시키고, 영업비밀의 개발촉적으로 기업 경쟁력을 제고하는데 기여토록 할 필요가 있다.

특히, 영업비밀과 직접 관련이 있는 연구·개발부서 및 영업비밀 관리직원에 대해서는 영업비밀 준수 서약서와 전직 및 퇴직시 사용·공개금지 및 경업금지 서약서를 징구해야 한다. 이와 같은 서약서에는 재직 중 지득한 회사의 영업비밀을 유출하는 경우 손해배상은 물론 민·형사상 책임을 지겠다는 것, 재직 중 창출한 영업비밀의 소유권은 회사에 귀속하는 것을 명기하여, 영업비밀을 둘러싼 법적 분쟁여지를 사전에 차단하도록 한다. 신규 직원이 다른

기업으로부터 전직하여 왔을 경우에는 이전 직장에서의 체결한 영업비밀 관리에 관한 계약 등을 주의 깊게 검토하고, 이 과정을 통해 타회사의 종업원을 채용함으로써 부당한 스카웃 또는 영업비밀 침해로 인한 제소를 당하는 일이 없도록 대비할 필요가 있다. 그리고 연구·개발부서의 직원 또는 영업비밀 관리부서의 직원이 퇴직예정이거나 퇴직시 사전에 영업비밀 인수인계에 대한 만전을 기하는 한편, 퇴직 직원에게 영업비밀의 사용 또는 공개행위는 영업비밀 침해행위에 속한다는 관련 법률 규정을 설명하고, 재직 중 연구·개발 및 관리하였던 영업비밀 관련 서류는 모두 반납하도록 하여야 한다. 또한 퇴직자가 보유한 영업비밀을 특정하고 경업금지 업종·분야를 구체적으로 한정하여야 한다. 단, 경업금지 기간은 해당 영업비밀의 중요성, 업종 및 업무 내용 등을 고려하여, 종업원의 직업선택의 자유를 부당하게 침해하지 않는 합리적인 기간을 1~2년 내에서 설정하여야 한다.

(5) 거래처 관리

영업비밀에 관한 라이선스 계약의 당사자가 상대방의 영업비밀의 가치를 평가하기 위해 협상 단계에서 공개를 요구하는 경우, 거래처와의 계약이 성립하기 이전에도 계약 사항의 협의를 위해 영업비밀을 공개할 필요가 발생할 수 있다. 이 경우 계약단계에 이르지 않을 경우를 대비하여 중요한 영업비밀을 제공하는 것을 신중하게 고려해야만 한다.

계약서에는 영업비밀의 유출에 관해 상대방의 경각심을 일깨우고, 만약 비밀 유출이 발생할 경우 법적수단을 강구하겠다는 의사를 명확히 하기 위하여 영업비밀에 관련된 조항(영업비밀의 목적 외 사용 금지, 제3자에 대한 공개 금지, 철저한 비밀 관리유지, 손해배상 등)을 삽입하도록 한다. 구체적으로는 의 내용이 포함되어야 한다. 영업비밀을 공개하는 기업뿐만 아니라 공개를 받는 기업 쪽에서도 법적 분쟁의 소지를 남기지 않기 위하여 상대방으로부터 취득할 영업비밀의 범위와 사용목적, 공개 범위를 계약서에 명확하게 규정하는 것이 필요하다.

(6) 협력업체 등 외부 보안 관리

협력 업무의 성격상 협상 단계에서부터 기업의 중요한 영업비밀을 공개할 필요성이 큰 경우가 많으므로, 구체적인 협상 단계 이전에 상호 비밀유지계

약을 체결하도록 한다. 협력업체가 비밀을 유출하는 사태를 방지하기 위하여 담당자에게도 비밀유지 서약서를 징구하여야 하며, 자사와의 계약 종료 후에도 동종 타사에 접촉할 기회가 많은 점을 고려하여 계약종료 후에도 일정기간 비밀유지의무를 부과하는 내용을 계약서에 명시하도록 한다.

(7) 제품 구매자 및 관계기관 등의 보안 관리

제품 구매 상담 및 공장 견학 등으로 기업을 방문하는 외부인도 상담 또는 견학과정에서 지득한 영업비밀을 유출할 위험이 있다. 따라서 제품 소개 또는 구매 상담의 자료 및 홍보 팸플릿 등에는 중요한 영업비밀을 노출하지 않도록 주의하여 기재하도록 하고, 견학에 관해서도 중요 시설 접근을 막는 등 적절한 코스를 지정하도록 한다. 또한 정부기관 및 지자체 등의 관계기관에 연구비 또는 연구프로젝트의 획득 등을 위하여 자사의 기술 정보 등의 영업비밀을 제공하는 경우에도 해당정보가 비밀임을 명확히 표시하고 관련 기관에도 “대외비”에 준하여 취급하여 줄 것을 요구하도록 한다.

(8) 서류 및 전자매체의 관리

영업비밀을 기재한 서류 등은 원칙적으로 접근권한자 이외의 사람이 접근 불가능한 장소에 문을 잠그고 보관하여야 한다. 접근권한자가 영업비밀이 기재된 서류 등을 외부로 가지고 나가는 것이나, 복제하여 소지하는 것을 인정하는 경우에는 반출 및 복제에 관한 규정을 두고 이를 업무상 필요한 경우에 제한하는 것이 바람직하다. 영업비밀이 전자 데이터로 저장되어 기록된 전자매체의 관리도 기본적으로 서류 등의 관리와 마찬가지로, 관리번호를 부여하고 일반 정보와 분리하여 출입이 통제된 구역이나 시건장치가 달린 캐비닛 등에 보관하는 것이 바람직하다. 영업비밀이 저장된 컴퓨터에 대해서는 접근을 최소화함과 동시에 반드시 패스워드를 사용해야만 접근할 수 있도록 하고, 수시로 패스워드를 변경하여 담당자 외에는 접근이 불가능하도록 해야 한다. 이메일에 관해서는 외부발송 이메일 크기를 일정규모 이하로 제한하고, 이를 초과할 경우에는 해당 부서장의 승인을 받도록 조치하여 영업비밀 유출을 방지해야 한다. 기업이 보유하고 있는 영업비밀은 내부 직원에 의해서도 유출되지만 외부인에 의해서도 유출될 수 있으며, 외부인으로부터 영업비밀을 보호하기 위한 물리적 조치의 가장 기본적인 방법은 연구·개발 장소

및 영업비밀 관리 장소에 대한 통제구역의 설정이라 할 수 있다.

3. 기업의 영업비밀 관리규정 표준 제정안

영업비밀 보호 및 관리를 위한 활용 표준은 해당 기업의 규모와 업종, 영업비밀의 특성, 영업비밀 관리조직 및 담당자의 유무, 영업비밀 관리의 적정성 등을 고려하여 특허청에 의해 작성되었다. 표준서식은 일반적 기업에 적용되는 다양한 서식을 표준화한 것이므로, 개별 기업의 구체적 사정에 따라 서식의 내용이 수정되거나 변경될 수 있다. 표준서식을 활용하여 임직원 등에게 비밀유지 서약서 등을 받는 것은 영업비밀을 보호하기 위한 최소한의 조치 중 하나일 뿐이며, 그 자체로 영업비밀 보호 노력을 충분히 했다고 볼 수 없다. 따라서 영업비밀 보호를 위한 합리적인 노력을 다하였음을 인정받기 위해서는 영업비밀의 표시, 등급분류, 관련 교육 시행, 출입 제한 등 다양한 조치가 함께 이루어져야 한다.

영업비밀로 보호받으려면 ‘합리적인 노력’이 필요하다. 이를 위해서는 임직원으로부터 비밀유지서약서를 받았는지의 여부, 영업비밀 관리 규정 등을 제정, 시행했는지 여부, 영업비밀 관리 또는 사용 대장을 작성했는지 여부 등은 법원이 어떤 정보가 상당한(합리적인) 노력에 의하여 비밀로 유지되었는지의 여부를 판단할 때 흔히 고려하는 요소이다. 또한 ‘상당한 노력에 의하여 비밀로 유지된다’는 것은 정보가 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고, 정보에 접근할 수 있는 대상자나 접근 방법을 제한하거나 정보에 접근한 자에게 비밀준수의무를 부과하는 등 객관적으로 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태인 것을 말한다(대법원 2011. 7. 14. 선고 2009다12528 판결, 대법원 2014.08.20. 선고 2012도12828 판결 등).

따라서 영업비밀 보유자는 다른 영업비밀 보호를 위한 노력과 함께 임직원이나 외부인으로부터 비밀유지서약서 또는 비밀유지계약서 등을 징구하고, 영업비밀 관리 규정 등을 제정해야 한다.

(1) 영업비밀 관리규정(안)

영업비밀의 분류, 표시, 취급자 등을 총칙 부분에 규정하고, 영업비밀의 창출 및 사용, 영업비밀 서약서의 징구, 시스템 보안 등에 관한 사항을 규정한다. 영업비밀 관리규정에는 영업비밀 관리대장, 비밀유지서약서, 비밀유지계약서 등의 양식을 별지 서식으로 정해두는 것이 바람직하다.

영업비밀 관리규정

제1장 총칙

제1조(목적) 이 규정은 주식회사 ABC(이하 '회사'라 함)의 정보자산, 보안 사항, 영업비밀 및 기타 지식재산권의 관리 및 보호에 관한 필요한 사항을 정하여 회사의 발전을 도모함을 목적으로 한다.

제2조(정의) 이 규정에서 사용되는 용어의 정의는 다음과 같다.

1. '정보'라 함은 회사의 경영 또는 활동에 필요한 일체의 지식을 말한다.
2. '정보자산'이라 함은 '정보와 정보시스템'을 포괄한 개념을 말한다.
3. '정보시스템'이라 함은 회사가 보유하고 있는 컴퓨터, 전산시스템, 네트워크, 소프트웨어 및 각종 영상매체시설물 등 '정보'를 관리하는데 필요한 모든 자산을 말한다.
4. '영업비밀'이라 함은 회사가 보유 또는 보유할 정보로서 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로, 합리적 노력에 의하여 비밀로 유지된 생산방법·판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.
5. '지식재산권'이란 인간의 창조적 활동 또는 경험 등에 의하여 창출되거나 발견된 지식·정보·기술, 사상이나 감정의 표현, 영업이나 물건의 표시, 생물의 품종이나 유전자원, 그 밖에 무형적인 것으로서 재산적 가치가 실현될 수 있는 것에 관한 권리를 말한다.
6. '임직원'이라 함은 회사에 재직하는 임원과 직원을 말한다.

제3조(보안업무의 분류) ① 회사의 모든 '정보'에 대해 '일반업무'와 '보안업무'로 구분하고, '보안업무'는 다시 '시스템보안업무'와 '일반보안업무'로 구분된다.

② '시스템보안업무'는 컴퓨터, 정보통신망 등 주로 컴퓨터를 통하여 진행되는 정보시스템에 관한 보안업무를 말하며, '일반보안업무'는 그 이외의 모든 부문의 정보보안업무를 말한다.

제4조(적용범위, 보호대상) ① 이 규정은 회사에 신규채용·재직·퇴직하는 모든 임직원과 외부 협력업체와 파트너 기타 회사를 출입하는 모든 사람에게

적용한다.

② 이 규정은 회사가 보유하고 있는 다음 각 호를 그 보호대상으로 한다.

1. 영업비밀 그 자체
2. 영업비밀이 화체된 물건 및 물체(예시 : 서류, 도면, 복사물, 자기테이프, 컴퓨터, CD, DVD, USB, 외장HDD, 전화기, 자재, 생산품 등)

② 이 규정은 회사가 보유하고 있는 다음 각 호를 그 보호대상으로 한다.

1. 영업비밀 그 자체
2. 영업비밀이 화체된 물건 및 물체(예시 : 서류, 도면, 복사물, 자기테이프, 컴퓨터, CD, DVD, USB, 외장HDD, 전화기, 자재, 생산품 등)
3. 영업비밀 생산설비와 장비
4. 영업비밀 통제구역
5. 지식재산권
6. 기타 회사 기밀과 관련된 정보자산

제2장 영업비밀의 보호관리

제5조(보안업무의 조직 및 기능) ① 회사는 영업비밀 기타 정보자산의 관리와 보호를 위하여 회사 내 모든 보안업무를 총괄 담당하는 보안관리책임자를 지정한다.

② 보안관리책임자의 직무는 다음 각 호와 같다.

1. 부서별 영업비밀 보호 및 관리에 관한 계획 수립 및 조정
2. 소관 영업비밀의 등급분류
3. 영업비밀에 관한 교육 실시
4. 영업비밀 보유현황 조사 및 관리 감독
5. 비밀유지계약 및 서약서 등의 집행
6. 보안관련 규정 및 지침 수립, 조정
7. 기타 회사의 영업비밀 보호 기타 보안에 관하여 필요한 사항

③ 보안관리책임자는 분기별로 대표이사에게 보안업무의 현황을 보고하여야 하며, 임직원이 중요한 영업비밀을 개발하거나 창출하였을 경우에도 같다.

④ 회사의 각 부서장은 부서업무와 관련된 영업비밀(제6조의 1급 비밀을 제외함)의 관리책임자로서 제2항 제1호 내지 제5호 및 제7호의 직무를 수행할 의무와 책임을 가진다.

⑤ 보안관리책임자는 각 부서장과 보안업무에 관한 협력체계를 수립하고 사

내 주요 보안상황을 공유하며, 필요한 사항에 대해서는 전 임직원에게 공지한다.

제6조(영업비밀의 분류와 기준) ① 회사는 영업비밀에 대해 그 중요성과 가치의 정도에 따라 ‘1급 비밀’, ‘2급 비밀’, ‘3급 비밀’ 등 3단계로 분류하고, 필요 시 그 분류를 변경할 수 있다.

② ‘1급 비밀’이란 경쟁사 또는 대외로 유출될 경우 회사가 막대한 손해를 입을 수 있는 다음 각 호의 영업비밀을 말한다.

1. 회사의 원천기술 및 이에 대한 지식재산권 출원과 관련된 사항
2. 세계 초일류 기술, 국방, 안보관련 기술 또는 국가핵심기술과 관련되는 사항
3. 회사의 영업전략, M&A 기타 회사의 핵심 영업비밀에 해당하는 사항

③ ‘2급 비밀’이란 경쟁사 또는 대외로 유출될 경우 회사에 피해를 줄 수 있는 영업비밀 중 ‘1급 비밀’에 해당하지 않는 영업비밀을 말한다.

④ ‘3급 비밀’이란 ‘1급 비밀’ 또는 ‘2급 비밀’이 아닌 ‘영업비밀’을 말한다.

⑤ 영업비밀은 다음 각 호의 기간 동안 보존한다. 다만, 회사의 보안관리책임자 또는 각 부서장은 각 영업비밀의 특성을 고려하여 다음 제2호, 제3호의 보관기간보다 장기간을 보존기간으로 지정할 수 있다.

1. 1급 비밀 : 영구보존
2. 2급 비밀 : 10년
3. 3급 비밀 : 5년

제7조(영업비밀 표시 및 보관) ① 영업비밀은 그 표지에 ‘대외비’ 표시와 함께 각 등급에 따라 아래와 같이 구분하여 표시하여야 한다.

1. 1급 비밀 : 대외비 | 1급
2. 2급 비밀 : 대외비 | 2급
3. 3급 비밀 : 대외비 | 3급

② 영업비밀이 화체된 서류, 물건 등은 일반 문서, 물건 등과 분리하여 별도의 보관함, 금고 등 보안장치를 구비하고 있는 용기에 넣어 특별히 관리하여야 한다.

③ 영업비밀이 포함되어 있는 전자문서는 일반 전자문서와 분리하여 비밀번호를 설정하고, 영업비밀 취급자격이 있는 자 이외에는 열람할 수 없는 방법으로 보관하여야 한다.

제8조(영업비밀 통제구역 설정) ① 영업비밀의 보호와 중요시설장비 및 자재의 보호를 위하여 필요한 경우 일정한 범위를 통제구역으로 지정하고, 필요 시 CCTV와 시건장치 기타 통제구역을 보호하기 위한 장치나 설비를 설치한다.

② 제1항의 통제구역에는 외부에서 인식할 수 있는 적절한 방법으로 ‘통제구역’임을 표시하고 회사로부터 사전에 허가 받은 관계자 이외의 출입을 통제하여야 한다.

③ 제1항의 통제구역에는 출입자 명부를 비치하여 출입자를 기록·보존하여야 하고, 필요할 경우 출입자로부터 영업비밀 보호에 관한 각서 또는 서약서를 징구하여야 한다.

제9조(관리대장) 각 영업비밀의 관리책임자는 제7조 제2항에 의하여 관리하고 있는 영업비밀에 대하여 등급별로 영업비밀 관리대장(이하 ‘관리대장’이라 함)을 비치하고 변동사항 등에 대한 기록을 유지·관리하여야 한다.

제10조(취급자격) 제6조에 의하여 분류된 영업비밀의 취급자격은 다음 각호와 같다.

1. 1급 비밀 : 대표이사, 대표이사가 지정한 임직원, 보안관리책임자
2. 2급 비밀 : 1급 비밀 취급자, 해당 영업비밀이 속한 담당부서의 부서장 및 실무 담당자
3. 3급 비밀 : 2급 비밀 취급자와 동일

제11조(보안점검) ① 보안관리책임자는 영업비밀을 취급하는 각 부서에 대하여 정기적으로 보안점검을 실시하여야 한다.

② 보안관리책임자는 영업비밀 보호를 위하여 필요한 경우 대표이사에게 그 사유를 보고한 이후 특정 임직원 및 부서를 선정하여 불시에 보안점검을 실시할 수 있다.

제12조(복구) 각 영업비밀의 관리책임자는 영업비밀에 대한 위험이 발생하거나 발생할 우려가 있음을 알게 된 때에는 지체 없이 보안관리책임자 및 관련부서에 이를 통보하고 즉시 필요한 조치를 취하여야 한다.

제13조(물품의 반입, 반출) ① 회사의 자산 및 물품을 반입, 반출하는 임직원은 보안관리책임자 또는 관련부서 부서장의 사전승인을 얻어야 한다.

② 컴퓨터 등 정보처리장치(휴대용을 포함하며, 이하 ‘정보처리장치’라 함) 및 USB메모리, 외장 HDD 등 전자기록매체(이하 ‘전자기록매체’라 함) 등을 사용하고자 하는 임직원은 사전에 보안관리책임자 또는 담당부서장의 승인을 얻어야 하며, 회사의 업무를 위해서만 사용하여야 한다.

③ 컴퓨터 또는 전자기록매체를 반입, 반출하는 경우, 이를 사용하는 사용자는 관련 규정에 따라 반입 및 반출일자, 기기사양, 사용용도, 사용자 정보 등을 작성하여 담당 부서장에게 제출하고, 담당 부서장은 이를 직접 확인한 이후 사용자가 제출한 서류를 보안관리책임자에게 제출하여야 한다.

④ 보안관리책임자는 제3항의 서류를 별도로 보관하고, 회사 내의 컴퓨터 및 전자기록매체 등의 존재 및 사용현황을 수시로 확인하여야 한다.

제14조(비상대책) ① 영업비밀 관리책임자는 화재나 자연재해 등 비상상황에 대비하여 복사본 작성이 필요한 영업비밀에 대해서는 보안관리책임자와 협의하여 복사본을 작성하고, 이를 별도의 장소에 보관하여 정기적으로 관리하여야 한다.

② 보안관리책임자는 화재나 자연재해 및 회사의 기밀유출 등의 비상상황 발생시 회사의 피해를 최소화하기 위한 관련 규정 및 지침을 수립하고, 이를 전체 임직원에게 공지하여야 한다.

제3장 영업비밀의 생성과 취득

제15조(영업비밀의 창출 및 귀속) 임직원이 직무와 관련하여 연구·개발하거나 취득한 영업비밀은 회사의 소유이며, 해당 임직원은 이를 회사에 귀속시켜야 한다. 다만, 임직원이 자신의 일반적 지식, 경험, 기술에 근거하여 창출한 영업비밀에 대해서는 특별한 약정이나 규정이 있을 경우 그 약정이나 규정에 따르고, 그 약정이나 규정이 없을 경우 해당 임직원의 소유로 한다.

제16조(영업비밀 신고) ① 임직원이 재직 중 영업비밀을 창출한 경우에는 관련 부서의 장에게 신고하여야 한다.

② 임직원이 본 규정의 적용을 받지 아니하는 타인과 공동으로 회사의 업무와 관련된 영업비밀을 창출한 경우에도 제1항의 규정에 따라 신고하여야 한

다.

제17조(보상) 임직원이 창출한 영업비밀 중 이로 인하여 회사의 이익이 발생하고 상당한 가치가 있는 영업비밀에 대해서는 직무발명에 준하여 보상금을 지급하여야 한다.

제18조(취득) 임직원이 영업비밀을 외부로부터 취득하였을 경우 관련부서의 부서장에게 신고하고, 관련부서의 부서장은 이를 관리대장에 기재하여 임직원이 창출한 영업비밀과 같은 방법으로 관리한다.

제4장 영업비밀의 사용

제19조(사용) ① 회사의 영업비밀은 제10조에 따라 영업비밀 취급자격이 인정되는 영업비밀 관리책임자의 승인을 얻어 사용할 수 있다.

② 회사의 영업비밀을 사용하거나 이를 반출하는 경우에는 사전에 영업비밀 관리책임자에게 신청하여야 하고, 위 관리책임자는 신청인의 영업비밀 취급 자격을 확인한 이후 그 자격이 인정되는 경우에 한하여 영업비밀 사용대장(이하 ‘사용대장’이라 함)에 신청내역을 기재한 이후 해당 영업비밀을 반출하거나 사용토록 하여야 한다. 이때 제1급비밀의 사용 또는 반출에 대해서는 사전에 보안관리책임자의 동의를 얻어야 한다.

제20조(양도) ① 영업비밀을 양도할 때에는 관련부서와 협의를 하고 영업비밀 관리책임자, 보안관리책임자 및 대표이사의 승인을 얻어야 한다.

② 영업비밀 관리책임자는 영업비밀을 양도한 후에도 필요에 따라 관계기록을 폐기하지 않고 영업비밀의 유지 및 관리를 수행해야 한다.

제21조(부서간 사용) 회사 내부의 부서간 영업비밀을 대여·사용·유통하기 위하여 이송할 때에는 제19조에 따라 부서 책임자간에 인수인계 절차를 거쳐야 하며, 영업비밀을 이송 받은 부서의 책임자는 해당 영업비밀의 사용이 종료되는 때에는 즉시 인수인계절차를 거쳐 해당 영업비밀을 원래 보관하고 있던 부서에 반환하여야 한다.

제22조(이송방법) ① 영업비밀을 사내에서 대여·사용·유통을 위하여 이송할

때에는 밀폐포장이나 용기 등을 사용하여야 한다.

② 부득이 영업비밀을 통신수단에 의하여 이송할 때에는 보안이 설정된 파일 등을 활용하거나 주요내용 부분은 이를 분리하여 이송하는 등 필요한 보안조치를 취하여야 한다.

제23조(관리, 폐기) ① 회사의 영업비밀은 영업비밀별 관리기준에 따라 관리한다.

② 더 이상 활용가치가 없는 영업비밀은 일정한 절차에 의해 폐기할 수 있으며, 폐기 후에도 필요한 경우에는 계속하여 보호·관리한다.

제5장 임직원의 영업비밀 보호의무

제24조(입사 시) 회사가 신규로 채용한 임직원에게 대해서는 비밀유지서약서를 작성하여 제출하게 하여야 한다.

제25조(재직 중 영업비밀누설 금지) ① 임직원은 재직 시 취득한 영업비밀에 대하여는 이 규정에 따라 취급·관리해야 하며 허가 없이 이를 유출·공개 또는 사용할 수 없다.

② 연구개발 결과, 신제품 등을 발표하거나 전람회 등에 출품하여 부득이 하게 영업비밀을 공개하게 되는 경우에는 사전에 해당 영업비밀의 관리책임자 및 보안관리책임자의 승인을 얻어야 한다.

③ 회사는 임직원의 재직 중에 정기적으로 비밀유지서약서를 징구할 수 있으며, 프로젝트 참여 등 필요 시에는 비밀유지서약서를 징구할 수 있다.

제26조(퇴직 시) ① 회사의 임직원이었던 자는 회사의 사전승인 없이 재직 시 취득한 영업비밀을 공개·유출 또는 사용할 수 없다.

② 임직원이 퇴직할 경우 그 임직원이 보유하고 있는 모든 영업비밀을 반납 받고 비밀유지서약서를 징구하여야 한다.

제6장 협력업체 등에 대한 비밀관리

제27조(협력업체 기타 제3자) 협력업체 기타 제3자에게 영업비밀을 제공하거나 영업비밀과 관련된 업무를 하게 할 경우 해당 협력업체 기타 제3자로

하여금 비밀유지서약서를 작성하여 제출하도록 하여야 한다.

제28조(공동 프로젝트, 기술제휴계약) ① 회사가 외부 기관 등에 연구개발 프로젝트를 의뢰하거나, 외부 기관과 사이에 기술제휴계약을 체결함에 있어서 회사의 영업비밀을 공개해야 하는 경우, 외부 기관의 참여 임직원에게는 비밀유지서약서를 제출 받고, 외부 기관과 사이에는 비밀유지계약서에 따라 비밀유지계약을 체결한 이후에 영업비밀을 공개하여야 한다.

② 회사는 외부 기관과의 협의에 따라 제1항의 비밀유지서약서 또는 비밀유지계약서 내용 중 일부를 변경할 수 있다.

제7장 시스템 보안관리

제29조(컴퓨터 사용) ① 회사 내 모든 컴퓨터 사용자는 불법 소프트웨어를 사용해서는 안 되며, 불법 소프트웨어를 사용함으로써 인한 모든 책임자는 사용자 본인에게 있으며, 회사는 책임이 없다.

② 회사 내 모든 컴퓨터 사용자는 바이러스 침입 및 해킹을 방지하기 위한 소프트웨어와 각종 보안 솔루션을 설치하고, 정기적으로 백업 및 업데이트 관리를 하여야 한다.

제30조(통신망 사용) ① 임직원들은 회사 내에서 공통으로 사용하는 통신망을 사용하여야 한다.

② 보안관리 부서 및 보안관리책임자는 회사의 영업비밀 보호 및 업무 효율성 확보를 위해 인터넷상의 특정 사이트 접속을 통제할 수 있다.

③ 임직원들은 회사에서 사용을 금지한 이메일을 사용해서는 안 된다.

④ 임직원들은 외부로 문서를 발송할 경우에는 부서장의 사전 승인을 받아야 한다. 단, 전결권한이 있는 임직원은 그렇지 아니하다.

제31조(시스템 관리) ① 보안관리책임자는 회사의 보안시스템을 연1회 이상 정기적으로 점검하고, 그 결과를 전체 임직원에게 공개한다.

② 임직원들은 회사의 보안시스템에 대한 문제를 발견한 즉시 보안관리책임자에게 그 사실을 신고하여야 한다.

③ 시스템보안에 대해서는 이 규정에 의하는 외에 별도로 규정하는 바에 따른다.

제8장 영업비밀 침해구제

제32조(구제조치) ① 보안관리책임자 및 각 부서장은 회사의 영업비밀을 침해 당했을 때에는 지체 없이 관계법령 및 사규에 의한 필요한 구제조치를 취하여야 한다.

② 보안사고 발생시 업무담당자와 보안관리책임자 등 관련자는 사건 조사 및 해결에 성실히 협력하여야 한다.

제33조(영업비밀누설자에 대한 징계) 영업비밀 누설자에 대해서는 제32조의 규정에 의한 조치를 취함과 동시에 별도로 사규에 따라 징계할 수 있다.

제34조(관련자에 대한 징계) 영업비밀 누설을 부주의나 과실로 알지 못하였거나 막지 못한 관계자에 대해서도 사규에 의해 징계할 수 있다.

제9장 보칙

제35조(교육) ① 보안관리책임자는 전체 임직원에게 대해서 정기적으로 영업비밀에 관한 교육을 실시하여야 한다.

② 영업비밀 교육은 외부에 위탁하여 실시할 수 있다.

부칙

1. 이 규정은 20__년 __월 __일부터 시행한다.
2. 이 규정 시행 전부터 보유하고 있는 영업비밀 중 주요 영업비밀에 대해서는 규정 시행 후 1개월 이내에 등급분류(재분류)를 하여 등급을 지정(재지정)한다.

[별첨] 등급별 취급 규정

1. '1급 비밀'을 기록한 문서, 도면, 사진, 서적, 자기 테이프, FD, CD, 컴퓨터 서버 등 (이하 '기록매체')의 취급은 다음과 같다.

(1) 보관

- 기록매체는 영업비밀 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 시건 장치가 있는 보관함에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 정보시스템 기기를 통제 구역 내에 설치한다. 만일 해당 정보시스템 기기를 통제 구역 내에 설치할 수 없는 경우에는 관리책임자는 타인의 접근을 방지하기 위한 최선의 보안조치를 취하여야 한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.

(2) 열람

- 관리책임자의 허가 없이 기록매체를 열람할 수 없다.
- 해당 정보에 접근이 허락되지 않은 자는 기록매체를 열람할 수 없다.
- 전자화된 정보의 화면 표시는 입실이 제한되고 해당 정보의 보유자가 실재하는 장소에서 타인에게 보이지 않도록 각별한 주의를 기울이며 실시되어야 한다.
- 관리책임자는 영업비밀 사용대장에 열람자명, 일시 등을 기록한다.

(3) 복제

- 관리책임자의 허가 없이 기록매체를 복제할 수 없다. 이때 복제물은 원본과 동등하게 '1급 비밀'로 취급해야 한다.
- 전자화된 정보의 복제는 관리책임자만이 실시할 수 있다.
- 관리책임자는 영업비밀 사용대장에 복제자명, 일시, 목적 등을 기록한다.

(4) 반출

- 관리책임자의 허가 없이 기록매체를 반출할 수 없다.

- 관리책임자의 허가가 있을 경우에도 허가를 받은 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 관리책임자는 영업비밀 사용대장에 반출자명, 일시, 목적, 반환시기 등을 기록한다.

(5) 폐기

- 기록매체는 사용 후 기록매체를 배부 받은 자의 책임 하에 적절한 방법에 의해 폐기하도록 한다.
- 전자화된 정보는 관리책임자의 승인을 얻어 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 폐기하도록 한다.
- 관리책임자는 영업비밀 관리대장에 폐기 일시 등을 기록한다.

2. ‘2급 비밀’ 기록매체의 취급은 다음과 같다.

(1) 보관

- 기록매체는 영업비밀 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 시건 장치가 있는 보관함에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당정보시스템 기기를 통제 구역 내에 설치한다. 만일 해당 정보시스템 기기를 통제 구역 내에 설치할 수 없는 경우에는 관리책임자는 타인의 접근을 방지하기 위한 최선의 보안조치를 취하여야 한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.

(2) 열람

- 기록매체는 중대한 필요성이 인정되는 경우 기록매체 소지자의 책임 하에서 관계자에게 열람시킬 수 있다.
- 전자화된 정보의 화면 표시는 타인에게 보이지 않도록 주의를 기울이며 실시되어야 한다.
- 관리책임자는 영업비밀 사용대장에 열람자명, 일시 등을 기록한다.

(3) 복제

- 기록매체는 중대한 필요성이 인정되는 경우 기록매체 소지자의 책임 하에 복제하는 것이 가능하다. 단, 복제물은 원본과 동등하게 ‘2급 비밀’로 취급해야 한다.
- 전자화된 정보의 복제는 관리책임자의 승인을 얻어 기록매체를 배부 받은 자의 책임 하에 실시할 수 있다.
- 관리책임자는 영업비밀 사용대장에 복제자명, 일시, 목적 등을 기록한다.

(4) 반출

- 업무상 필요성이 인정되는 경우에만 기록매체를 반출할 수 있다.
- 이 경우 기록매체를 반출한 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 관리책임자는 영업비밀 사용대장에 반출자명, 일시, 목적, 반환시기 등을 기록한다.

(5) 폐기

- 기록매체는 사용 후 기록매체를 배부 받은 자의 책임 하에 적절한 방법에 의해 폐기하도록 한다.
- 전자화된 정보는 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 폐기하도록 한다.
- 관리책임자는 영업비밀 관리대장에 폐기 일시 등을 기록한다.

3. ‘3급 비밀’ 기록매체의 취급은 다음과 같다.

(1) 보관

- 기록매체는 영업비밀 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 보관해야 한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.

(2) 열람

- 전자화된 정보의 화면 표시는 타인에게 보이지 않도록 주의를 기울이며 실시되어야 한다.

(3) 복제

- 기록매체는 중대한 필요성이 인정되는 경우 기록매체 소지자의 책임 하에 복제하는 것이 가능하다.
- 전자화된 정보의 복제는 중대한 필요성이 인정되는 경우에만 기록매체를 배부 받은 자의 책임 하에 실시할 수 있다.
- 관리책임자는 영업비밀 사용대장에 복제자명, 일시, 목적 등을 기록한다.

(4) 반출

- 기록매체를 반출한 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 관리책임자는 영업비밀 사용대장에 반출자명, 일시, 목적, 반환시기 등을 기록한다.

(5) 폐기

- 기록매체는 사용 후 기록매체를 배부 받은 자의 책임 하에 적절한 방법에 의해 폐기하도록 한다.
- 전자화된 정보는 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 폐기하도록 한다.
- 관리책임자는 영업비밀 관리대장에 폐기 일시 등을 기록한다.

[별지] 영업비밀 관리/사용대장

- 영업비밀의 체계적 관리를 위해서는 아래 예시와 같은 관리/사용 대장의 작성이 필수적이다. 중소기업의 경우 엑셀(excel) 파일로, 영업비밀 관리 시스템이 갖춰진 기업의 경우 시스템 상에서 기록되는 것이 일반적이다.

■ 영업비밀 관리대장

[illegible]

■ 영업비밀 사용대장

[illegible]

2. 시스템 보안 규정

- 이 규정은 영업비밀 보호 및 관리 활동이 전산 시스템과 불가분적으로 결합됨에 따라 전산 시스템 보안에 관한 사항을 별도로 정한 것이다.

시스템 보안 규정

제1조(목적) 이 규정은 회사의 정보시스템과 정보통신의 보안에 관한 필요한 사항을 정하여 회사의 발전을 도모함을 목적으로 한다.

제2조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. ‘전산실’이란 업무용 전산장비와 공용 네트워크장비가 보관되는 장소를 말한다.
2. ‘시스템관리자’란 업무 및 연구목적으로 보유하고 있는 정보통신시스템의 운용 및 관리 책임이 있는 해당부서의 부서장을 말한다.
3. ‘홈페이지’란 회사의 대표홈페이지 및 회사의 업무와 관련하여 제작하여 대외 서비스하는 모든 것을 말한다.
4. ‘정보보안, 정보보호’란 정보통신 수단에 의하여 처리, 저장, 소통되는 정보를 보호하거나 해킹 등 외부 위협으로부터 취약요인을 제거하기 위한 각종 수단과 방법을 말한다.
5. ‘정보통신시스템’이란 업무처리 혹은 연구목적 수행을 위해 네트워크에 연결하여 다수 인원이 이용하는 서버 및 정보통신장비를 말한다.
6. ‘보조기억매체’란 디스켓, 이동형 하드디스크(HDD), USB메모리, CD (Compact Disk), DVD(Digital Versatile Disk), 휴대폰 등 자료를 저장할 수 있는 일체의 것으로 개인용 컴퓨터 등의 정보통신시스템과 분리할 수 있는 기억장치를 말한다.

제3조(시스템보안 범위) 시스템 보안 관리는 다음 각 호와 같다.

1. 전산실 보안
2. 정보자료
3. 개인용 컴퓨터(데스크톱, 노트북, 태블릿, 스마트폰 등)
4. 이메일 및 유무선 통신망
5. 홈페이지 등 공개용 웹서버, SNS(블로그 등) 관리
6. 무선랜
7. 정보통신망 신설, 증설 및 정보시스템교체 등을 실시할 경우 보안성 검토
8. 그 밖의 시스템 보안업무에 관한 사항

제4조(전산실 보호대책) 전산실 운영부서장은 전산실을 제한구역으로 하고 다음 각 호의 대책을 강구하여야 한다.

1. 방재대책 및 외부로부터의 위해 방지
2. 전산자료 또는 장비 별 취급자 지정운영
3. 항시 이용하는 출입문은 한 곳으로 정하고 이중문과 보안 장치 설치
4. 그 밖의 전산업무 비관련자 출입 제한 등

제5조(정보자료 보안관리) ① 시스템관리자는 전산자료 및 보안이 요구된다고 판단되는 전산자료의 유출, 파괴 또는 변조 등에 대비하여 다음 각 호와 같이 보호대책을 강구한다.

1. 전산자료 보유현황 관리
2. 장비 반·출입 통제
3. 정보통신망 불법접근 및 컴퓨터바이러스 피해 예방
4. 중요자료의 백업체계 수립 시행
5. 최신 소프트웨어 보안 패치(patch) 적용

② 시스템관리자는 인위적 또는 자연적인 원인으로 인한 정보통신시스템의 장애 발생에 대비하여 시스템 이원화, 백업관리, 복구 등 종합적인 재난복구 대책을 수립·시행하여야 하며 재난복구 시스템은 다음 각호와 같다.

1. 중요자료의 이중화 백업 시스템 구축
2. 서버와 물리적으로 이격된 공간에 별도의 백업 시스템 구축
3. 실시간 백업시스템 구축

③ 시스템관리자는 정보통신시스템을 이용하기 위한 사용자계정을 발급하고 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 한다.

④ 시스템관리자는 비밀번호 등 사용자 식별 및 인증이 없는 사용자계정은 사용하지 못하게 하며 퇴직 시 사용자 계정을 즉시 폐쇄한다.

⑤ 주요 정보통신시스템의 운영체제에 직접 접근할 수 있는 권한은 시스템 관리자에게만 허용하고 일반 사용자계정 부여는 제한 한다.

⑥ 일반사용자의 정보통신시스템 보유자료 이용은 시스템관리자가 허용한 응용프로그램을 통해 이용함을 원칙으로 하며 업무별, 자료 별 중요도에 따라 사용자 별 접근권한을 차등 부여하여야 한다.

⑦ 시스템관리자는 비인가자의 정보통신시스템 침입 사실을 인지한 경우에는 시스템 보호를 위한 접속차단 등 초동조치를 취하고 전산부서장에게 연

락하며 전산담당부서장은 대표이사 및 보안관리책임자에게 보고하여야 한다.

⑧ 시스템관리자는 정보통신시스템에 대하여 외부업체의 원격 유지보수 작업을 허용하여서는 아니된다. 다만, 부득이한 경우에는 필요한 보안대책을 강구 후 허용할 수 있으며, 이때에도 원격 유지보수 내용을 확인 감독하여 반드시 기록으로 유지하여야 한다.

⑨ 주요 정보통신시스템은 시스템관리자에 의거 일일 점검하여야 하며 점검 내용은 다음 각 호와 같다.

1. 장비의 전반적인 운영 상태 점검
2. 장비 장애발생의 사전 방지를 위한 예방 점검
3. 장비 로그 분석 및 그 결과에 따른 적절한 대처
4. 소프트웨어의 적절한 활용여부, 불법소프트웨어 설치여부, 보안 패치 적용, 버전의 업그레이드를 수행 및 점검
5. 장애가 발생하였거나 장애 발생이 우려될 경우 적절한 대처 또는 전문 정비업체 의뢰

제6조(보조기억매체 보안관리) ① 보조기억매체의 관리책임자는 사용자의 소속부서장이 되며 관리책임자는 업무용 보조기억매체를 보조기억매체 관리대장 작성을 통해 관리(등록, 파기, 반출, 반입)하여야 하며, 등록되지 않은 매체는 사용할 수 없다.

② 중요 자료는 반드시 암호가 설정되거나 보안프로그램이 적용된 보조기억매체에 저장한다.

③ 암호가 설정되거나 보안프로그램이 적용된 보조기억매체를 사용할 경우 공인기관 등의 보안적합성 검증을 받은 제품을 사용한다.

④ 보조기억매체 분실 시 사용자는 즉시 관리책임자에게 보고한다.

⑤ 전산담당부서에서는 필요 시 각 부서의 관리대장을 점검을 할 수 있다.

⑥ 연구원은 보조기억매체를 관리하기 위하여 관리시스템을 활용할 수 있으며 보안정책 및 운영기준은 다음 각 호와 같다.

1. 이 시스템의 목적을 위해 전 직원은 회사에서 사용하고자 하는 개인용컴퓨터는 보조기억매체 관리를 위한 클라이언트 프로그램을 설치해야 한다.
2. 회사에서 유출되는 모든 자료에 대하여 동 시스템을 이용하여 조사할 수 있다.
3. 이 시스템을 이용하여 회사에서 외부로 유출(전송)되는 모든 자료는 일정 기간 보관할 수 있다.

4. 이 시스템에 등록되지 않은 보조기억매체의 사용은 통제될 수 있다.
- ⑦ 제6항의 관리시스템을 이용하여 수집한 자료는 정보유출의 확인 작업 등 회사의 정보보안 목적 이외에 어떤 목적으로도 공개하면 안 된다.

제7조(개인용 컴퓨터 보안관리) ① 소속 부서장은 회사 소유의 개인용 컴퓨터(데스크톱, 노트북, 일체형, 태블릿, 그 밖의 형태의 정보처리기기를 포함)의 취급자 및 보안 관리책임자를 지정하여야 한다.

② 회사 소유의 개인용 컴퓨터로 전산망을 사용하고자 하는 직원은 전산부서에 등록요청을 하여야 하며 전산부서의 등록에 의하여 사용한다. 또한 이미 사용 중인 개인용 컴퓨터를 교체하는 경우에도 이와 같다.

③ 개인 소유의 개인용 컴퓨터를 주요정보가 처리, 보관되는 연구원 내부에 반입하여 사용할 수 없다. 다만, 부득이한 경우에는 소속 부서의 장의 승인을 받아 반입할 수 있다.

④ 회사 소유의 개인용 컴퓨터를 수리 또는 교체하는 경우 정보자료를 모두 삭제하거나 하드디스크를 분리 제거 후 수리의뢰 하여야 한다.

⑤ 개인용 컴퓨터 사용자는 암호 설정 및 백신프로그램을 설치하여 보안에 만전을 기한다.

⑥ 소속부서장은 이동 가능한 개인용 컴퓨터(노트북, 태블릿, 일체형 등)의 반출입에 대해 이동 가능 정보기기 관리대장을 이용하여 관리(등록, 이관, 반출, 반입)한다.

⑦ 연구원은 전체 개인용 컴퓨터의 전산보안을 강화하기 위하여 패치관리시스템 및 보안관리 클라이언트 프로그램을 이용할 수 있고, 업무에 사용되는 모든 개인용 컴퓨터는 보안관리 클라이언트 프로그램을 의무적으로 설치해야 하며 미설치 개인용 컴퓨터는 외부망 접속을 차단할 수 있다.

제8조(이메일 및 통신망 이용) ① 시스템관리자(전산부서)는 기술정보 보안을 위하여 내부통신망을 이용하여 대내외로 수발신하는 이메일 등을 통해 전송되는 자료에 대해서는 일정기간(3년 이내) 내역을 보존하여야 한다.

② 시스템관리자(전산부서)는 직원 및 근무자의 업무용 이메일 사용을 위한 개인별 이메일계정(ID)을 부여하여야 하며 직원이 퇴직할 경우 즉시 이를 폐쇄하여야 한다. 다만, 업무협력 등 특별한 사유가 있을 경우 소속 부서장의 요청이 있을 때는 3개월 범위에서 폐쇄를 유보할 수 있다.

③ 시스템관리자(전산부서)는 스팸메일, 바이러스메일 등을 차단하기 위하여

스팸 메일차단시스템을 운영한다.

- ④ 시스템관리자(전산부서)는 저장된 자료를 정보유출의 확인 작업 등 회사의 정보보안 목적 이외에 어떠한 명목으로도 공개하여서는 안 된다.
- ⑤ 인터넷의 사용은 연구원 업무와 관련된 것들에 한정되어야 하며, 시스템 관리자(전산부서)는 업무와 관련이 없는 사이트 접속 및 프로그램에 대해서는 사용을 제한할 수 있다.
- ⑥ 내부통신망에 접속하여 개인용 컴퓨터 등의 자료를 복사(다운로드) 하고자 하는 경우 보안관리책임자 또는 소속부서장의 승인을 받아야 한다.
- ⑦ 내부 직원은 회사에서 제공하는 통신망 사용을 원칙으로 하고 별도의 통신망 사용이 필요한 경우 외부망 사용 신청서를 이용하여 전산담당부서에 신청한 후 사용한다.

제9조(홈페이지 등 공개용 웹 서버 관리) ① 시스템관리자는 홈페이지 등 공개용 웹 서버는 방화벽 등 침입차단시스템을 설치하여 내부망의 전산자원을 보호하여야 한다.

- ② 시스템관리자는 서버에 접근할 수 있는 사용자계정을 제한하며 불필요한 계정들은 삭제한다.
- ③ 시스템관리자는 홈페이지 구축·운영 시 자체 보안성 검토를 거쳐 내용을 구성하며 이후 개인정보와 같은 중요 자료가 공개되지 않도록 한다.
- ④ 시스템관리자는 보안사고에 대비하여 서버에 저장된 자료의 철저한 백업 체계를 구축한다.

제10조(무선 랜 관리) ① 무선 랜 사용은 제한함을 원칙으로 한다.

- ② 무선통신장치 설치 시 전산담당부서의 승인을 받은 후 설치하며 비인가자의 무선 랜 접속을 방지하기 위해 시스템인증 및 암호화 등의 보안설정을 한다.

제11조(정보보안의 책임) ① 개인이 보유하고 있는 자료 등의 정보의 보안에 관한 책임은 사용자 및 소속부서장에게 있다.

- ② 서버 및 공용 정보통신기기에 대한 보안의 책임은 시스템관리자에게 있다.
- ③ 소속부서장은 정보보안 업무수행을 위하여 이 규정의 범위 내에서 부서 실정에 적합한 별도의 대책을 마련하여 시행할 수 있다.

부칙

이 규정은 대표이사가 승인한 날로부터 시행한다.

[별지] 보조기억매체 관리대장(등록/폐기)

보조기억매체 관리대장(등록/폐기)

[관리책임자 : ○○○]

연번	관리번호	매체형태	등록일자	관리자	불용처리일자	불용처리내용
1	정보지원-1	일반USB	2016.11.1	홍길동	2016.12.1	고장으로 폐기
2	정보지원-2	외장HDD	2016.11.1	홍길동	2016.12.1	고장으로 폐기
3	정보지원-3	보안USB	2016.11.1	홍길동	2016.12.1	고장으로 폐기

보조기억매체 관리대장(반출입)

연번	관리번호	매체형태	사용일자	사용자	용도
1	정보지원-1	외장HDD	2016.11.1	홍길동	세미나 발표

[별지] 이동 가능 정보기기 관리대장(등록/폐기)

이동 가능 정보기기 관리대장(등록/폐기)

[관리책임자 : ○○○]

[illegible]

이동 가능 정보기기 관리대장(반출입)

[illegible]

[별지] 외부망 사용 신청서

외부망 사용 신청서

업무와 관련하여 회사 내에서 아래와 같이 외부망을 사용하고자 신청하며
보안사고가 나지 않도록 보안관리를 철저히 하도록 하겠습니다.

- 아래 -

☐ 외부망 사용 현황

1) 사용 외부망

- 통신사: SK브로드밴드 / KT / LG유플러스 / 기타 ()
- 형 태: 유선 / 무선

2) 사용기간 :

3) 사용목적 :

☐ 보안관리 사항

- 1) 외부망에 연결된 PC/노트북 등에는 회사 내부망에 접속할 수 없도록 통제한다
- 2) 외부망 사용자 중 외부업체 직원 등은 내부 업무용 자료에 접근할 수 없도록 통제한다.
- 3) 외부망에 연결된 PC/노트북 등에는 중요한 업무용 자료를 보관하지 않는다.

20 . . .

사용자:

소속부서:

책임자: (인)

부서장: (인)