14_실무에 적용하기 위한 영업비밀 관리 규정 구축 방법

#1
이번 시간에는 영업비밀 관리 규정 구축 방법을 알아보겠습니다.
영업비밀을 보호하기 위해 기업 내에 영업비밀 관리 규정을 구축하는 것은 매우 중요합니다. 왜냐하면, 영업비밀 관리 규정은 직원들에게 어떤 정보가 영업비밀로 분류되는지, 그리고 이를 어떻게 다루어야 하는지에 대한 명확한 가이드라인을 제공하기 때문입니다. 더불어 관리 규정을 통해 내부 직원에 대한 교육을 진행할 수 있어 영업비밀 침해를 예방하는 데 큰 도움이 됩니다. 그렇다면 영업비밀 관리 규정에는 어떤 내용이 들어가야 할까요?

#2
※ 영업비밀 관리의 목적
'목적' 항목은 해당 규정의 전반적인 목표와 그 이유를 명확하게 설명하는 부분입니다. 여기서는 규정이 왜 필요하고, 이를 통해 무엇을 달성하려고 하는지를 설명합니다.

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

#3
※ 지식재산권을 함께 규정하는 이유
기업(회사)의 주요 기술 정보나 영업 정보는 영업비밀로 보호할 수도 있지만, 특허, 실용신안권 또는 디자인권으로도 보호할 수 있습니다. 이는 기술적인 발전이나 창작물에 대한 보호를 위한 다양한 방법이 존재하기 때문입니다.

보안규정의 핵심은 결국 회사의 핵심 자산을 보호하는 것입니다. 기업의 핵심 기술 정보나 영업 정보는 경쟁 우위를 가져다주는 중요한 자산이기 때문에 적절한 보호조치가 필요합니다. 이를 통해 경쟁사나 외부인의 무단 접근이나 유출을 방지하고, 기업의 경쟁력을 유지하는 데 도움이 됩니다.

하지만 현실적으로 직원들은 영업비밀인지 특허발명인지를 명확하게 구분하지 않을 수 있으며, 업무상 사용하고 외부로 유출할 수도 있습니다. 따라서 기업

은 직원들에게 적절한 교육과 보안 규정을 제공하여 영업비밀과 지적재산권에 대한 이해를 높이고, 보안 사고를 방지하기 위한 조치를 강화해야 합니다. 이는 기업의 중요한 자산을 보호하고 유출을 방지하는 데 큰 역할을 합니다.

#4

※ 보안업무 분류

※ 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.

이렇게 구분함으로써, 각각의 보안업무에 따른 다른 접근 방식과 관리 방법을 적용할 수 있습니다. 예를 들어, 시스템 보안 업무는 기술적 보안 조치를 중점적으로 고려해야 하는 반면, 일반 보안 업무는 물리적, 관리적 보안 조치 등이 중요할 수 있습니다.

#5

※ 적용 범위 - 회사 내 적용

신규 채용자나 재직자뿐만 아니라 퇴직한 임직원에게도 회사 내 관리규정이 적용됩니다. 이는 관리규정을 통해 영업비밀을 보호하기 위함입니다. 물론, 재직자나 퇴직자에게 영업비밀 보호를 명확히 하기 위해 관리규정 외에도 영업비밀서약서 등을 함께 적용할 수 있습니다. 이를 통해 보다 강력한 보안 조치를 취할 수 있습니다.

#6

※ 적용 범위 - 외부 협력 업체 및 파트너 회사 적용

외부 협력 업체나 파트너 회사의 경우, 회사 내부의 영업비밀 관리규정이 그대로 적용되지 않습니다. 다른 회사나 업체는 독립된 법인이기 때문에 자사의 내부 규정만으로는 즉시 효력을 발휘하지 않습니다. 따라서 이러한 경우에는 관련 계약서에 비밀유지 규정을 명시하고, 양측이 합의한 후에 그 효력을 발휘합니다. 이를 통해 외부 협력 업체나 파트너 회사와의 비밀유지를 보장할 수 있습니다.

#7
※ 보안업무 조직 및 기능 정의
보안업무와 관련하여 별도의 보안관리책임자를 지정하여 규정할 수도 있습니다. 보안관리책임자의 지정과 직무 규정은 영업비밀 보안을 강화하는 데 도움이 됩니다. 하지만 중소기업에서는 보안관리책임자를 별도로 지정하기 어려운 경우가 많습니다. 이런 경우에는 실제로 회사 대표가 보안책임자로서 역할을 수행합니다.

#8
※ 보안관리책임자 지정의 이점
보안관리책임자가 회사 내부에 존재하면 다양한 이점이 있습니다.
첫째, 보안관리책임자는 일관성 있는 교육을 제공함으로써 모든 직원이 영업비밀에 대한 중요성을 이해하고 적절한 보호 조치를 취할 수 있도록 합니다.
둘째, 보안관리책임자는 회사의 영업비밀 보유 현황을 정확하게 파악하고, 이를 철저히 관리 감독함으로써 비밀유지를 보장합니다. 이런 역할을 통해 회사는 영업비밀의 보안성을 강화하고, 이를 외부에 인정받을 수 있습니다.

#9
※ 영업비밀 분류 및 보존 기간
규정을 설정할 때는 회사 내부에서 적절한 기준을 설정하여 영업비밀을 분류하는 것이 중요합니다. 예를 들어, 1급 비밀, 2급 비밀, 3급 비밀 등으로 분류하고, 각 등급별로 어떤 정보가 해당하는지 명확하게 정의할 수 있습니다. 이때, 각 등급별로 분류하는 것은 별지를 활용하여 표로 정리하면 보다 명확하고 쉽게 이해할 수 있습니다.

또, 각 등급의 영업비밀에 따라 보존 기간을 개별적으로 설정하는 것이 유용합니다. 예를 들어, 1급 비밀은 영구 보존, 2급 비밀은 10년간, 3급 비밀은 5년간 보존하도록 규정할 수 있습니다. 그러나 이러한 보존 기간은 법률에 의해 정해진 것이 아니므로, 회사 내부의 상황에 따라 유연하게 변경될 수 있습니다. 또한, 영업비밀로 분류된 정보는 원칙적으로 계속적으로 보호되어야 하므로, 매년 검토가 필요하며, 공개될 수 있는 정보는 영업비밀로 분류하지 않는 것이 바람직합니다.

#10

※ 영업비밀 표시와 보관

※ 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 관리해야 한다.

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

#11

※ 비상대책 규정

※ 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 발생 시 회사의 피해를 최소화하기 위한 관련 규정 및 지침을 수립하고, 이를 전체 임직원에게 공지하여야 한다.

다만, 비상대책 규정은 보안규정에 별도로 명시하지 않고 회사 내부적으로 대비하는 것도 가능합니다. 이는 반드시 포함되어야 하는 조항은 아니며, 회사의 상황에 따라 생략할 수도 있습니다.

#12

※ 영업비밀 생성과 취득 조항 관리 규정 포함 시 고려 사항

「특허법」의 성격과 영업비밀의 성격을 고려해야 합니다. 특허법에 따라 특허권은 발명자 혹은 승계인이 특허를 받을 수 있기 때문에 회사 내 직원이 발명했다면 원칙적으로 특허출원의 원칙은 직원에게 발생합니다. 회사는 직원으로부

터 권리를 승계해야 출원이 가능하고, 정당한 대가로 보상금을 지급하도록 직무발명제도가 존재하기도 합니다. 또, 영업비밀은 범위가 애매하고 오히려 회사와 직원들 간 분쟁을 야기시킬 요소가 크기 때문에 법률에서는 영업비밀에 대하여 직원이 권리를 주장할 수 있다는 요건을 두고 있지 않습니다.

#13

※ 영업비밀의 사용과 양도

※ 영업비밀의 사용

① 회사의 영업비밀은 제10조에 따라 영업비밀 취급 자격이 인정되는 영업비밀 관리책임자의 승인을 얻어 사용할 수 있다.

② (생략)

※ 영업비밀의 양도

① 영업비밀을 양도할 때에는 관련 부서와 협의를 하고 영업비밀 관리책임자, 보안관리책임자 및 대표이사의 승인을 얻어야 한다.

② 영업비밀 관리책임자는 영업비밀을 양도한 후에도 필요에 따라 관계기록을 폐기하지 않고 영업비밀유지·관리를 수행해야 한다.

#14

영업비밀의 비밀성을 판단할 때, 실제로 어떻게 표시되었는지도 중요한 요소입니다. 판례에서도 영업비밀 등급을 명시적으로 구분하지 않은 경우, 전체적으로 해당 정보를 '영업비밀'로 인정하지 않았다는 사례가 있습니다. 때문에 적절한 방식으로 영업비밀에 대해 반드시 표시할 필요가 있습니다. 그렇다면 영업비밀의 비밀성을 인정받기 위해서 어떻게 표시할 수 있을까요?

#15

※ 워터마크

가장 일반적인 방법 중 하나는 영업비밀임이 지워지지 않도록 워터마크로 표시하는 것입니다. 문서에 워터마크를 삽입한 후에는 비밀번호를 설정하여 영업비밀로의 지속적인 유지를 보장할 수 있습니다.

※ 표지, 머리글 또는 꼬리글에 기재

또 다른 방법은 가장 눈에 띄는 표지에 영업비밀임을 명시하거나, 머리글 또는 꼬리글에 기재하는 것입니다. 이러한 표시 방법에 대한 기준을 정하고 회사 내의 모든 임직원이 동일하게 작성하는 것이 중요합니다.

#16
※ 서류 관리 방법
영업비밀에 해당하는 문서나 물건이 있는 경우, 권한이 없는 자가 접근하지 못하도록 금고나 보관함을 설치하고 명확한 잠금장치를 사용하는 것이 필요합니다.

특히 설계도면이나 제작도면과 같은 자료의 경우, 대부분 서류로 보관됩니다. 이러한 도면이나 자료는 꼭 잠금장치를 사용하고, 접근 권한이 있는 사람만이 비밀번호 등을 통해 확인할 수 있도록 제한적으로 설정하는 것이 필요합니다.

#17
※ 소프트웨어 프로그램과 파일의 관리 방법
현재 시대에는 대부분의 작업이 컴퓨터를 통해 디지털 파일로 진행되며 정보를 얻거나 생성하는 경우가 많습니다. 이러한 자료는 회사 내 별도의 서버나 웹하드를 통해 보관됩니다. 그러므로 이러한 디지털 파일이나 소프트웨어 프로그램 등에 대한 영업비밀 보호를 위해 비밀등급을 표시하고, 비밀번호 등을 설정하여 접근 권한을 차등으로 관리해야 합니다.