13_영업비밀 보안의 첫 번째 스텝! 영업비밀을 특정하라

#1
이번 시간에는 영업비밀 보안을 위한 관리 방안을 알아보겠습니다.
영업비밀은 성립 요건을 만족시켜야만 법적으로 보호를 받을 수 있습니다. 그러므로 실무에서는 영업비밀의 성립 요건을 만족시키기 위해 다양한 방법으로 보안을 유지해야 합니다. 이러한 노력들이 영업비밀의 보완을 유지하는 데 기여하고, 영업비밀이 유출되는 불상사가 발생할 시 법적인 측면에서 유리하게 작용할 수 있기 때문입니다. 먼저, 영업비밀을 관리하기 위한 일반적인 절차를 살펴보겠습니다.

#2
※ 영업비밀 관리 프로세스
1. 영업비밀 보호 대상 특정: 회사는 영업비밀로 분류되는 정보를 식별하고 정리합니다.
2. 영업비밀 등급 분류: 영업비밀을 중요도에 따라 등급을 분류하여 각각의 보안 수준을 결정합니다.
3. 영업비밀 보안규정 제정: 회사는 영업비밀 보호를 위한 규정을 마련하고 문서화합니다.
4. 영업비밀 보안 조치 및 접근 권한 설정: 보안규정에 따라 영업비밀에 대한 접근 권한을 설정하고, 보안 조치를 시행합니다.
5. 내부 직원 비밀유지서약서(입사 및 퇴사 시): 영업비밀에 접근하는 직원들은 비밀유지서약서를 작성하여 영업비밀의 비밀을 지키도록 요구받습니다. 이 서약서는 입사 시에 작성되며, 퇴사 시에도 유효하게 유지됩니다.

#3
※ 영업비밀 관리 프로세스
6. 외부 비밀유지계약서: 외부 제3자에게 영업비밀을 공개할 경우, 비밀유지계약서(NDA) 등을 체결하여 영업비밀의 비밀을 보호합니다.
7. 영업비밀 시스템 관리: 영업비밀을 보호하기 위한 시스템을 운영하고 관리합니다. 이는 접근 제어, 암호화 등의 기술적인 조치를 포함합니다.
8. 영업비밀 보안 교육 실시: 회사는 직원들에게 영업비밀 보안 교육을 수시로 실시하여 영업비밀의 중요성과 보안 관행에 대한 이해를 높이고 지속적인 보안 의식을 유지합니다.

#4
※ 영업비밀 특정
우선 회사에서 보호하고자 하는 영업비밀을 특정해야 합니다. 회사 대표의 입장에서는 회사에서 다루는 모든 자료, 문서, 정보 등을 전부 영업비밀로 간주하고 보호하고자 할 수 있지만, 영업비밀로 관리되는 경우 직원이나 제3자가 해당 정보를 엄격하게 관리하고 사용해야 합니다. 때로는 영업비밀 유지를 위해 퇴사 후 이직이 제한되는 경우도 있습니다.

따라서 회사 내에서 다루는 정보 중 어떤 것이 영업비밀인지 특정해야 합니다. 이를 위해서는 회사는 영업비밀의 범위와 내용을 명확히 정의하고, 직원들에게 영업비밀의 중요성과 유지에 대한 교육을 제공하여 인식을 공유해야 합니다. 또한, 영업비밀을 보호하기 위한 적절한 보안 시스템과 절차를 마련하여 정보 유출과 무단 사용을 예방해야 합니다.

#5
※ 영업비밀의 대상 분류
영업비밀로 보호할 수 있는 대상이 정해지면 그 다음 단계로는 분류를 진행해야 합니다. 영업비밀은 모두 동일한 수준으로 간주되는 것이 아니라, 1급, 2급, 3급 등급으로 분류될 수 있습니다. 이렇게 등급이 분류되면 각 등급에 맞는 접근 권한을 설정하고, 해당 등급에 맞는 보안 조치를 취할 수 있습니다.

영업비밀 등급 분류를 통해 중요도와 민감도에 따라 정보에 접근하는 권한을 조절할 수 있습니다. 높은 등급의 영업비밀은 민감한 정보로 간주되므로 접근 권한을 제한하고, 추가적인 보안 조치를 강화할 수 있습니다. 이를 통해 영업비밀의 보안성을 높이고 정보 유출 및 무단 사용을 방지할 수 있습니다.

영업비밀 등급 분류는 회사의 내부 정책에 따라 결정되며, 등급 분류는 정보의 중요도, 경쟁 우위, 기술적 차별성 등을 고려하여 진행되어야 합니다. 이를 위해서는 회사는 명확한 등급 분류 기준을 마련하고, 직원들에게 해당 등급에 따른 보안 조치 및 접근 권한에 대한 교육을 제공해야 합니다.

#6
※ 영업비밀 보안규정 제정

영업비밀을 체계적으로 보호하기 위해서는 '영업비밀 보안규정'을 별도로 작성하고 운영하는 것이 중요합니다. 취업규칙에 보안규정이 포함되는 경우도 있지만, 영업비밀을 정확하게 보호하고 관리하기 위해서는 별도의 '영업비밀 보안규정'을 작성하는 것을 추천해드립니다.

'영업비밀 보안규정'은 회사 내에서 영업비밀의 보안에 관한 규칙과 절차를 명확히 정의한 문서입니다. 이 규정은 영업비밀의 정의, 등급 분류, 접근 제한, 보안 조치, 정보 유출 방지 등을 상세하게 기술해야 합니다. 또한, 규정에는 직원들의 의무와 책임, 제재 사항 등에 대한 내용도 포함되어야 합니다.

영업비밀 보안규정을 작성할 때에는 회사의 특성과 운영 환경을 고려하여 구체적인 내용을 결정해야 합니다. 이를 위해 보안 전문가나 법률 전문가의 도움을 받는 것이 좋습니다. 또한, 작성된 규정은 회사 내 모든 직원들에게 충분히 알려지고 이행되도록 해야 합니다. 규정의 이행 상황은 정기적으로 점검하고 개선해 나가야 합니다.

#7
※ 영업비밀 보안 조치 및 접근 권한 설정
영업비밀 보안 규정이 마련되었다면, 해당 규정에 따라 접근 권한을 설정하고 각 영업비밀에 맞는 보안 조치를 적용합니다. 또한, 설정된 보안 규정과 시스템을 운영하기 위해 영업비밀에 접근하는 직원들에 대해 비밀유지서약서를 작성할 수 있습니다. 이를 통해 직원들에게 영업비밀의 비밀을 지키도록 요구할 수 있습니다. 더 나아가, 외부 제3자에게도 영업비밀의 비밀을 유지하도록 요청하기 위해 비밀유지계약(NDA) 등을 별도로 체결할 수도 있습니다. 이러한 조치들을 통해 영업비밀의 보안성을 강화할 수 있습니다.

#8
※ 내부 직원 비밀유지서약서
- 입사 시: 직원이 영업비밀을 관리하고 사용하는 방법에 대한 내용을 중심으로 작성되어야 합니다. 이는 영업비밀의 보안 유지와 악용 방지를 강조합니다. 직원은 영업비밀을 제3자에게 유출하거나 무단으로 사용하지 않아야 하며, 보안 조치에 따라 올바르게 처리해야 합니다.
- 퇴사 시: 비밀유지서약서를 다시 한번 작성하는 것이 좋습니다. 이 경우에는 개인적인 이익을 위해 영업비밀을 활용하지 않도록 강조하고, 제3자에게 노출

되지 않도록 유의해야 합니다. 또한, 필요한 경우에는 동종업종의 업무나 이직을 제한하는 전직금지약정 등을 추가로 설정할 수도 있습니다. 이는 퇴사 후에도 영업비밀의 보안을 유지하기 위한 조치입니다.

#9
※ 외부 비밀유지계약서
외부 비밀유지계약서는 한 측이나 양측이 상대방에게 해당 영업비밀을 제공할 때 이를 보호하기 위해 체결하는 법적 문서입니다.

- "비밀 정보"의 정의: 계약서는 무엇이 비밀 정보로 간주되는지 명확하게 정의합니다. 이는 특정 기술, 제품 디자인, 비즈니스 전략, 고객 리스트 등이 될 수 있습니다.
- 비밀 정보의 사용 및 공개 제한: 계약서는 수신자가 비밀 정보를 어떻게 사용하고, 어떤 상황에서 공개할 수 있는지에 대한 제한을 설정합니다. 일반적으로, 수신자는 비밀 정보를 제공하는 목적 외의 용도로 사용하거나 제3자에게 공개하는 것을 금지합니다.
- 비밀 정보의 보호: 계약서는 수신자가 비밀 정보를 적절하게 보호하고, 침해를 방지하기 위해 어떤 조치를 취해야 하는지를 명시합니다.
- 계약 기간과 종료 후 처리: 계약서는 비밀 정보의 보호를 위한 기간을 설정하며, 이 기간이 끝나면 수신자가 비밀 정보를 어떻게 처리해야 하는지를 정합니다.

#10
※ 영업비밀 시스템 관리 방법
'영업비밀 시스템 관리'는 영업비밀을 안전하게 보호하고 관리하기 위한 기술적, 관리적 조치를 총괄하는 단계입니다. 이 과정에서는 정보 보안 시스템을 통해 영업비밀 정보에 대한 접근 제어를 설정하고, 암호화 등의 기술을 활용해 정보를 안전하게 보호합니다. 또한, 시스템 사용 로그를 관리하고, 이상 징후가 발견될 경우 즉시 대응하는 등의 보안 관리 활동을 수행합니다. 이렇게 해서 영업비밀이 효과적으로 보호되고, 침해 위험을 최소화하는 것이 목표입니다.

#11
※ 관리와 교육 실시

영업비밀에 접근하는 경로나 이용자를 기록 및 관리하는 것은 보안을 강화하기 위해 중요한 단계입니다. 회사는 영업비밀에 접근하는 모든 경로와 이용자에 대한 기록을 정확하게 관리해야 합니다. 이를 통해 누가 언제 영업비밀에 접근했는지 추적할 수 있으며, 필요한 경우에는 이를 확인할 수 있습니다.

또한, 회사는 직원들에게 영업비밀 보안 교육을 수시로 진행함으로써 보안을 지속적으로 강조해야 합니다. 이러한 교육을 통해 직원들은 영업비밀의 중요성과 보안 조치에 대한 이해를 높일 수 있으며, 올바른 보안 관행을 따를 수 있도록 돕습니다. 영업비밀 보안 교육은 회사 내에서 보안 의식을 고취시키고 지속적인 보안 문화를 형성하는 데에 큰 역할을 합니다.

#12
영업비밀의 등급을 분류하는 것은 영업비밀 보호의 중요한 부분입니다. 모든 정보나 자료를 영업비밀로 취급하는 것은 효율적이지 않을 수 있습니다. 영업비밀은 중요도에 따라 등급을 분류하여 적절한 보호 수준을 결정하는 것이 필요합니다. 이어서 영업비밀 등급 분류 시 어떤 요소를 고려해야 하는지 살펴보겠습니다.

#13
※ 투여 비용 고려
비용과 시간에 대한 고려는 중요합니다. 정보 보호에 대한 고려사항 중 첫 번째로 고려해야 할 요소는 획득 또는 개발 비용입니다. 영업비밀로서의 가치가 있는 정보는 주로 기술적이나 경영적인 정보입니다. 이러한 정보를 얻거나 개발하는 데 큰 비용과 시간이 들어갔다면, 당연히 이를 보호해야 할 가치가 높아집니다. 즉, 회사가 해당 정보를 확보하기 위해 투자한 비용이 많을수록 이를 실제로 보호해야 할 가치가 높아집니다. 이러한 정보를 얻는 데 소요된 시간과 비용을 대략적으로 계산할 수 있기 때문에 이러한 측면을 수치적으로 평가하여 고려해야 합니다.

#14
※ 수익의 영향력 고려
회사의 수익에 영향을 미치는 관련 영업비밀의 중요성을 고려해야 합니다. 영업비밀은 회사의 경쟁력을 향상시키거나 경제적 가치를 제공하는 역할을 합니다. 따라서, 기술정보를 수집하는 데 많은 시간과 노력을 투자했음에도 불구하

고, 이미 존재하거나 사용 가능한 시기를 놓쳤다면 해당 기술정보의 가치는 상당히 떨어질 수 있습니다. 이에 따라, 관련 영업비밀이 회사의 수익에 어떤 영향을 미치는지 그 영향력을 신중하게 고려해야 합니다.

#15
※ 유출 시 입게 될 손실의 가능성 고려
경쟁업체에 영업비밀이 유출될 경우 발생할 수 있는 손실 가능성을 평가하는 것입니다. 영업비밀은 경쟁업체로부터 비밀로 유지되어야 하는 이유로 회사의 경쟁력을 보장하기 위한 것입니다. 따라서, 영업비밀이 경쟁업체에 유출될 경우 해당 기업의 경쟁력이 저하되고, 이에 따라 영업적인 손실이 발생할 수 있습니다. 따라서, 해당 영업비밀의 중요성을 평가하기 위해서는 유출될 경우 경쟁력에 미치는 손실의 크기를 신중하게 고려해야 합니다.

#16
※ 영업비밀 등급을 분류하는 방법
- 첫 번째 방법은 각 요소에 가중치를 할당하여 종합적으로 점수를 계산하는 종합 점수 방법입니다. 이 방법은 모든 요소를 고려하여 전체적으로 등급을 평가하는 방식입니다.
- 두 번째 방법은 각 평가 요소를 개별적으로 판단하여, 특정 요소에 대해 예외적으로 높은 등급을 부여하는 개별 점수 방법입니다. 이 방법은 영업비밀 등급을 높게 주어야 할 이유가 있는 경우에 해당합니다. 이렇게 두 가지 방법을 활용하여 분류 기준을 정할 수 있습니다.

#17
※ 분류된 영업비밀 관리 방법
먼저, 분류된 각 영업비밀에 대해 표시 방법을 지정하고, 접근 권한을 설정합니다. 이는 무단 접근을 방지하고, 영업비밀의 안전성을 유지하기 위해 중요한 단계입니다. 또한, 보관 방법을 분류하여 각 등급의 영업비밀을 적절히 보호합니다. 이렇게 영업비밀을 분류하고 관리하기 위해 대략적인 범위와 등급을 확정한 후, 이를 바탕으로 본격적인 영업비밀 관리 규정을 작성할 수 있습니다. 이 규정은 영업비밀의 보호와 관리에 필요한 절차와 규칙을 명시하여 조직 내에서 일관된 관리를 할 수 있도록 도와줍니다.