[기술유출분쟁대응] 기술유출 분쟁대응에 관한 실무적 포인트

1. 기술유출 대응팀 구성방안

5

- 보안담당자, 법무담당자, 인사담당자, 기술담당자, IT 담당자 등으로 TFT 구성
- 대응팀 내부 정보보안도 중요함. 팀원에게 비밀준수 의무 부과
- 증거 확보 및 대응 방안이 수립까지 엄격한 보안 필수적
- 기술유출 혐의자도 통상 전현직 직원이므로 동료직원 등 기술유출 혐의자와 직접 연결된 내부 관계자 있음 유의!
- 기술유출 관련 외부 전문가 조력 필요함. 객관적 입장에서 진행

2. 신속한 증거 확보 방안 필요

6

- 대상자의 PC, 메일, 문서 등 확인
- 증거수집 자체가 위법하지 않도록 유의. 법률 전문가 조력 필요
- 위법수집 증거의 경우 추후 법적 절차에서 적법한 증거로 사용할 수 없음 유의
- 수집된 증거의 핵심을 신속하게 분석하여 그 결과를 종합
- 기술유출 행위, 규모 등 분석 및 평가
- 대응방안 수립 및 회사 의사 결정

3. 법적 조치

7

형사상 구제 방안

- 검찰/경찰 고소장 또는 진정서 제출
- 일정기간 내사 필요한 경우 적절한 수사기관 선택 + 진정서 제출
- 통상 형사고소/진정을 먼저 하여 증거 수집하는데 주력
- 민사소송의 경우 기술유출 혐의자에게 소장 송달 + 주장 및 증거에 대한 검토 및 대응 기회 제공함
- 증거수집을 위한 압수/수색 중요 + 충분한 사전 준비 필요

민사상 구제 방안

- 통상 침해금지/전직금지 등 가처분신청을 먼저 제기
- 침해금지 본안 소송
- 손해배상 청구 소송

4. 압수·수색 관련 실무적 포인트

8

▣ 기술유출 수사는 압수·수색 중요

- 압수·수색은 필연적으로 혐의 대상 회사 및 개인의 권리침해 우려
- 혐의 유무에 대한 정확한 판단으로 수사 개시해야 함
- 압수 · 수색으로 증거확보 여부가 승패 좌우하는 경우 많음

▣ 압수·수색상 애로점

- 정확한 압수 · 수색 장소 선정
- 압수 · 수색 대상자 선정
- 현장 압수 · 수색시 어려움: 시스템, 개인장비, 소형 메모리 등

▣ 압수·수색 직후 중요 관련자 조사 필요

- 초기 단계에 관련 진술을 확보해 둘 필요 있음
- 추후 진술 번복에 대비

5. 영업비밀 보호정책 시행

9

1. 회사정보 중 비밀로 관리할 대상 정보를 분류한다.
2. 비밀정보 문서, 파일 등에 "대외비" 표시 및 비밀등급을 표시한다.
3. 비밀정보를 개방되지 않은 곳에 보관하고 접근을 제한한다.
4. 비밀정보 관리대장을 만들고 관리자를 지정한다.
5. 비밀정보의 등급별 접근권한을 정한다.
6. 사규 또는 입사규정으로 전 사원으로부터 회사비밀정보를 외부에 누설하거나 사적으로 이용하지 않겠다는 비밀유지 서약서를 받는다.
7. 사원을 대상으로 영업비밀보호에 관한 교육을 정기적으로 실시한다
8. 퇴사자에게도 비밀유지 서약서를 받는다.
9. 현장 상황을 정기적으로 점검하여 실천한다.
10. 관리규정만 만들고 현장에서 시행하지 않거나 사용자가 실시 여부를 점검하지 않는 경우 오히려 역효과 우려 있음.

영업비밀, 기술유출, 경업금지, 전직금지, 민형사소송, 다수사건 A~Z 수행경력

T. 02-591-0657 E. kkh@kasanlaw.com H. www.kasanlaw.com