

## 영업비밀 보호센터 자가 진단 항목의 활용

고시 <별표 7>의 비밀관리성 항목 작성 시 “영업비밀 보호센터 자가 진단 항목”을 활용할 수 있으며, 참고적으로, 고시 <별표 7> 비밀 관리성과 관련 있다고 판단되는 “영업비밀 보호센터 자가 진단” 항목에는 아래 고시에 기재된 ‘표시자’를 윗첨자로 표기하였습니다.

※고용노동부고시 <별표 7> 영업비밀에 해당함을 입증하는 자료 및 대체 필요성에 대한 판단기준	
1. 영업비밀에 해당함을 입증하는 자료	표시자
1) 비공개 신청 화학물질 제조·수입업체가 신청 정보의 비밀성을 보호하기 위한 조치의 종류 및 정도(정보에 대한 접근제한 조치, 내부직원에 대한 비밀유지의무 부여 및 비밀유지 고용계약 체결, 물리적 보안조치 여부, 보안시스템이 구비된 전산환경 마련 등 포함)	1-1)
2) 비공개 신청 정보에 대한 타인의 접근 및 획득 용이성 정도 ○ 해당 화학물질 제조·수입업체 이외의 자 또는 다른 화학물질 취급업체가 관련 정보를 획득 또는 접근할 수 있는 난이도 ○ 관련 정보의 비공지성 여부 및 공지된 정도	1-2)
2. 대체 필요성에 대한 판단기준	표시자
1) 해당 정보를 알 수 있는 인원(부서)의 제한범위를 구체적으로 명시하였는지	2-1)
2) 정보접근성을 제한하기 위해 취하는 노력을 구체적으로 명시하였는지 ○ 해당 정보를 모르는 자(공급자, 운반자, 그 외 인원 등)가 해당 물질을 취급함에 있어 비밀 관리를 어떤 방법*으로 하고 있으며, 이를 주기적으로 확인·점검하는지 ○ 해당 정보를 알고 있는 자를 대상으로 비밀관리를 어떤 방법*으로 하고 있으며, 이를 주기적으로 확인·점검하는지	2-2)

## 영업비밀 보호센터 자가 진단 항목

### 가) 정책 관리<sup>1-1), 2-2)</sup>

#### 1.1 영업비밀 접근 권한 제한

- 모든 영업비밀 대상에 대해 접근 권한 통제 기준을 가지고 통제하며 권한 변경 및 조정 시 접근 권한을 회수한다.
- 일부 중요 영업비밀에 대해 접근 권한을 통제하고 있다.
- 영업비밀에 대한 접근 통제 정책을 가지고 있지 않다.

#### 1.2. 영업비밀 교육

- 자체 및 외부 강사를 초빙하여 매년 1회 이상 주기적으로 전체 종업원들에게 영업비밀 교육을 실시한다.
- 서약서 징구 시 등 비정기적으로 주지 교육을 실시한다.
- 종업원에 대한 영업비밀 교육을 실시한 적이 없다.

#### 1.3. 최고 경영자 태도

- 최고 경영자가 회의나, 교육 등 수시(분기 1회 이상)로 영업비밀을 중요성을 강조하고 실행을 확인하는 등 적극적인 태도를 보인다.
- 영업비밀 보호를 위한 감시 설비·보안 솔루션 확충·교육 파견 등 영업비밀 보호 관련 예산을 당해년도에 책정되어 있거나, 최근 1년간 영업비밀 보호에 비용을 지불한 실적이 있다.
- 최고 경영자가 관심 없거나, 말로는 영업비밀의 중요성을 강조하지만 상기 내용을 실행하지 않는다.

#### 1.4. 영업비밀 관리 규정 제정/준수/감사 활동

- 영업비밀 관리 규정 준수 여부에 대하여 매년 감사 활동을 하고 있다.
- 영업비밀 관리 규정이 사규에 포함되어 있으며, 배포, 게시, 회의, 교육 등의 방법으로 수시로 임직원들에게 그것의 이행을 공지하고 있다.
- 영업비밀 관리 규정이 없거나, 있어도 사문화되어 준수하지 않고 있다.

#### 1.5. 관리 조직 및 운영

- 사내 전체 또는 부서별 영업비밀 관리 책임자가 지정되어 있다.
- 영업비밀 관리 책임자가 지정되어 있지 않다.

#### 1.6. 홍보물 통제 정책<sup>1-2)</sup>

- 회사의 공식 배포자료(홍보물/팜플렛/출판물/홈페이지 게시물 등), 논문 발표 자료에 영업비밀이 포함되어 있는지를 영업비밀 관리 책임자가 통제한다.
- 회사의 공식 대외 배포 자료나 논문의 공개를 영업비밀 관리 차원에서 당해 업무 담당자가 자율 검토하도록 의무화되어 있고, 그렇게 실행한다(본인 또는 입회자가 관련 서류에 확인 서명하고 그 서명 자료를 보관함).
- 종업원들이 자료를 대외로 배포하는 데 아무런 제한이 없다.

### 나) 취급 관리<sup>1-1), 2-2)</sup>

#### 2.1. 영업비밀의 등록

- 회사의 중요 정보나 자료 등을 관리대장에 영업비밀로 등록한다.
- 영업비밀로 등록하지 않는다.

## 2.2. 비밀 표시

- 등록된 영업비밀 문서의 표지나 전자 문서 폴더 등에 비밀임을 표시한다.
- 비밀임을 표시하지 않는다.

## 2.3. 보관 형태

- 영업비밀과 그 기록 매체는 다른 문서와 구별하여 보관함에 보관하거나 접근제한 조치된 정보 시스템에 보관한다.
- 일반 문서와 구별하여 보관하지만 시건 장치 없는 서랍에 보관하는 등 보관 상태가 취약하다.
- 사내 일반 문서와 함께 보관하고 있다.

## 2.4. 영업비밀의 생성 취득 과정<sup>2-1)</sup>

- 영업비밀은 생성 작업 착수 단계부터 영업비밀로 관리대장에 등록하여 관리한다.
- 영업비밀로 등록하지는 않지만, 영업비밀로 예상되는 작업 중인 정보나 자료를 통제 구역, 접근 제한된(전체 및 폴더별 비밀번호 설정) 전자 문서 형태 등으로 보관하고, 작업 완료 후 개인 컴퓨터에 보관 중인 정보를 소거하는 등 영업비밀에 준하여 관리한다.
- 영업비밀 생성 과정에 대한 규정이나 통제가 없다.

## 2.5. 비밀 취급 기록<sup>2-1)</sup>

- 영업비밀의 등록, 배부, 열람, 복제·인쇄, 열람, 사외 반출, 보관 등 전반적 관리 현황을 전자 정보 시스템으로 기록 관리한다.
- 영업비밀 전반적 관리 현황을 관리대장 등에 기록 관리한다.
- 영업비밀 관리대장에 기록하거나 그에 준하는 관리가 이루어지지 않는다.

## 2.6. 열람/사용<sup>2-1)</sup>

- 영업비밀에 접근 권한이 없는 자는 관리 책임자의 허락을 받아 열람·사용하며, 그 사실을 열람 기록표 등에 기록한다.

## 2.7. 복제/인쇄<sup>2-1)</sup>

- 영업비밀의 복제·인쇄를 원칙적으로 금하거나 특별한 제한이 가해진다.
- 영업비밀의 복제·인쇄에 제한이 없다.

## 2.8. 비밀 사외 반출 절차(USB, PC, 금형, 시제품 등)<sup>2-1)</sup>

- USB, PC, 금형, 시제품 등 영업비밀의 사외 반출 및 회수에 대한 허가 절차를 구비하고, 그대로 준수하고 있다.
- 사외 반출 절차 없이 담당자의 단독 결정으로 사외 반출할 수 있다.

## 2.9. 폐기<sup>2-1)</sup>

- 영업비밀의 폐기 방법이 규정되어 있고 그 방법대로 실행한다.
- 폐기 방법에 대한 규정이 없어 담당자가 임의로 처리한다.

## 다) 인적 관리<sup>1-1), 2-2)</sup>

### 3.1. 서약서 징구·보관<sup>2-1)</sup>

- 주기적(3년 이내) 또는 연봉 협상 시 또는 프로젝트 참여 시, 퇴직 시에 영업비밀 보호 서약서를 징구하여 보관한다.
- 입사 시 징구는 하지만 주기적으로 갱신하지 않는다.
- 징구도 보관하지도 않는다.

### 3.2. 협력업체 관리<sup>1-2), 2-1)</sup>

- 외부자(협력업체, 컨설팅, 계약자 등 거래자 등)에 대한 영업비밀 공개/열람 필요시 비밀 유지 계약 체결 또는 서약서를 징구한다.
- 외부자와 비밀 유지 계약 체결하지 않고 서약서도 징구하지 않는다.

### 3.3. 영업비밀 보호 의무 부과<sup>2-1)</sup>

- 모든 종업원에 대한 영업비밀 보호 의무를 사규로 규정하고 있다.
- 중요 직급 등 일부만 의무화되어 있다.
- 전혀 고려하고 있지 않다.

### 3.4. 퇴직자 관리

- 퇴직 징후 포착 및 퇴직 후까지 일정 기간 계속 관리한다.
- 퇴직 이후부터 대체적인 동향을 파악하고 있다.
- 전혀 파악하지 않는다.

### 3.5. 징계 절차

- 영업비밀 관리 규정 위반 시 징계 규정을 구비하고 있으며, 실제 징계 실적도 있다.
- 영업비밀 관리 규정에 징계 규정을 구비하고 있지만 아직 징계 사례는 없다.
- 영업비밀 관리 규정에 징계 규정이 없거나, 징계 규정이 있는데도 위반 시 징계하지 않은 사례가 있다.

## 라) 물리적 관리<sup>1-1), 2-2)</sup>

### 4.1. 통제 구역 보호

- 중요 시설을 통제 구역으로 지정하여 시건 장치 등으로 출입을 통제한다.
- 통제 구역 지정 등 중요 시설을 관리하지 않는다.

### 4.2. 협력업체 등 출입 절차<sup>1-2)</sup>

- 외주 업체, 아웃소싱 업체, 계약자 등 협력업체 종업원들의 출입 통제 절차가 확립되어 있다.
- 특별한 제한 없이 출입 가능하다.

### 4.3. 감시 장치(CCTV 등)

- 통제 구역 등 모든 중요 시설에 감시 장치가 설치되어 있다.
- 일부 지역에만 감시 장비가 설치되어 있다.
- 감시 장비가 설치되어 있지 않다.

### 4.4. 카메라 등 장비 반입 통제 여부<sup>1-2)</sup>

- 카메라, 모바일 부착 카메라, 카메라 부착 제조 장비, 컴퓨터 USB·전자 기록 매체 등 영업비밀 절취 장비의 반입이 통제된다.
- 특별한 반입 통제 절차가 없다.

## 마) 기술적 관리<sup>1-1), 2-2)</sup>

### 5.1. 서버 및 DB 보안 점검

- 보안 설정 여부를 주기적(반기 이상)으로 점검하고 조치한다.
- 보안 설정 점검을 시행하지 않는다.

## 5.2. 외부 침입자 솔루션 도입

- 외부 컨설팅 결과에 따라 보안 솔루션을 도입하여 운용한다.
- 일부 알려진 보안 솔루션을 구입하여 사용한다.
- 아무런 대책 없다.

## 5.3. 전자 기록 매체 관리 절차

- 개인 휴대용 PC 및 전자 기록 매체의 사용·관리 절차가 정해지고, 비밀용으로 등록된 메모리만 사용한다.
- 영업비밀 저장 전자 기록 매체는 관리번호가 부여되며, 문서화된 영업비밀 관리와 동등하게 취급된다.
- 상기 관리 절차 및 취급이 이루어지지 않는다.

## 5.4. 전자 문서 발송 제한

- 모든 메일은 문서 통제 대책(DRM)을 활용하여 발송한다.
- 영업비밀은 보안 조치 없이 이메일로 발송하지 못하도록 사규로 정하고 발송 용량을 제한한다.
- 발송 통제가 없다.

## 5.5. 비밀번호 관리

- 비밀번호는 3개월 기준으로 변경하며, 이를 점검한다.
- 주기적으로 비밀번호 변경을 권고한다.
- 사용자 재량에 맡겨진다.

## 5.6. 이식 시 IT 기기 보호(화면 보호기 등)

- 화면 보호기에 비밀번호가 설정되어 있으며, 이식 시 자동으로 작동된다.
- 화면 보호기는 작동하나 비밀번호 설정은 없다.
- 화면 보호기 설정이 없다.

## 5.7. 영업비밀 보관 서버와 외부 통신망 분리 운영

- 내부 영업비밀 보관 서버는 외부 인터넷 통신망과 차단된다.
- 내부 영업비밀 보관 서버와 외부망이 구분되어 있고, 외부서 내부망 접근 시 인증이 필요하다.
- 내부 서버 접근 시 인증 없이 접속 가능하다.

## 5.8. 로그 기록 유지

- 로그를 기록하고 영업비밀 정보를 보관한다.
- 전혀 기록하지 않는다.