HS 효성첨단소재㈜

# 정보 보안 정책

보안책임강화 TFT

2026 년 03 월 03 일

# 목차

# 01. 총칙

### 01) 목적

본 정책은 HS 효성첨단소재(이하 '당사'라 한다)의 기밀 정보, 지적 재산, 고객 개인정보 등 중요 정보의 유출을 방지하고, 정보보안 사고로부터 자산 손실 위험을 최소화하여 안전한 경영활동을 지원함을 목적으로 한다.

### 02) 적용 범위

본 정책은 당사의 임직원, 협력사 임직원을 포함한 모든 외부자, 당사의 정보통신망 및 시설을 이용하는 모든 인원을 대상으로 하며 당사가 소유, 관리하거나 업무상 취득한 모든 정보자산(제 3 자 제공정보 포함)에 적용한다.

# 02. 정보 보안 관리 체계

### 01) 정보 보안 거버넌스

① 당사는 정보보안 관리 시스템을 지속적으로 점검하고 개선할 책임을 가지며, 국내외 정보보호 관련 법령 및 요구사항의 변화를 지속적으로 모니터링하고 이를 정보보안 규정에 반영한다.

② 정보보호 최고책임자(CISO)를 임명하여 전사 정보보안 활동을 총괄하도록 한다.

③ CISO 는 사내 정보보안 활동 전반과 정보 유출 사고에 대한 모니터링 책임을 가지며, 유관 조직과 함께 '보안책임 강화 TFT'를 구성하여 정보보안 정책 운영 및 기존 정책의 효과성 · 이행 실적을 정기적으로 점검한다.

④ 전사적 보안 책임 강화를 위해 모든 부서장을 '부서 보안 책임자'로 지정하여, 정보 유출로 인한 자산 손실 위험을 최소화한다.

### 02) 임직원 보안 책임

① 모든 임직원은 당사의 보안 정책을 숙지하고 신의성실의 원칙에 따라 정책을 준수하여야 한다.

② 업무상 취득한 당사 또는 제 3 자 소유의 정보를 업무 목적 이외의 용도로 사용하거나 당사의 보안 정책에 따라 접근이 허용된 인원 외의 임직원 및 외부자에게 승인 없이 공개, 누설해서는 안 된다.

③ 보안 관련 규정, 지침, 절차에 따라 모든 정보보안 업무를 처리하며 이에 명시되지 않은 사항은 관련 법령 및 사규가 정하는 바에 따라야 한다.

# 03. 외부 협업 보안

### 01) 계약 및 서약

① 당사와 업무 협업을 진행하는 경우 사전에 외부자를 대상으로 비밀유지를 위한 보안계약서 및 서약서를 징구하여야 한다.

② 외부자와 업무상 협업을 위한 계약을 체결하는 경우에는 당사 정보자산 보호에 필요한 사항을 검토하여 외부자가 준수해야 하는 사항을 계약서에 명시하여야 한다.

③ 계약 업무 수행 상 당사의 보안문서를 취급, 열람하는 외부업체의 인원 범위는 필요한 최소인원으로 한정해야 한다.

### 02) 외부 협업 보안 관리

외부업체 직원은 당사에서 허가한 지역에 제한적으로 출입할 수 있고 업무 협업을 위해 전산장비를 반입하는 경우 당사의 전산장비 반출입절차를 준수하여야 한다.

# 04. 정보 보안 사고 예방 및 대응

### 01) 정보 보안 사고 예방

① 당사는 보안사고 발생 시 신속하고 효과적으로 대응하기 위해 즉시 지원 가능한 전문기관과의 협력 체계를 유지하고, 비상 연락망을 관리한다.

② 정보 자산 유출 위험을 체계적으로 관리하기 위해 정기적인 정보보안 위험성 평가를 실시한다.

③ 정보 자산의 식별 및 중요도 분류, 위험 수준 측정, 대응 전략 수립을 통해 리스크를 관리하며, 정기적인 재평가와 모의 훈련을 통해 관리 체계의 실효성을 지속적으로 강화한다.

④ 임직원의 정보보안 인식 강화를 위해 정기적으로 모의 훈련을 실시하며 사이버 위협 대응 역량을 높인다.

### 02) 정보 보안 사고 인지 및 대응 절차

① 모든 임직원은 비인가된 활동을 인지하거나 이상징후를 발견하는 경우 내부 신고처, 사업장 부문 보안관리자, 부서보안책임자에게 신고하여야 한다.

② 보안담당자는 시스템에 비인가된 활동이나 이상징후가 보이면, 확인 및 점검 후 정보보안사고로 판단될 시 전사보안책임자에게 보고하여야 한다.

③ 침해사고 대응 및 원인분석, 사고조사를 수행하여 전사보안책임자에게 보고하여야 한다.

### 03) 복구 절차 및 사후 조치

① 시스템 담당자는 중요 파일을 백업하고 관련 시스템의 계정 정보를 변경하며, 시스템 복구 시 백업 이미지의 훼손/침해 여부를 검증하여야 한다.

② 복구된 시스템은 침해사고 취약점 제거 여부를 확인하고, 사고 발생 관련 최신 보안 패치 적용을 지원하여야 한다.

③ 보안 담당자는 피해 사실과 원인, 재발 방지 대책 등을 포함한 보고서를 작성하여 전사보안책임자에게 보고한다.

④ 사후조치로 사고 재발 방지를 위한 대응책을 마련한다.

## 05. 데이터 무결성 및 보호

### 01) 정보 자산 보안 관리

① '정보자산'은 당사가 보유하거나 당사에서 생성된 출력물, 전자문서 등을 포함한 모든 유·무형의 정보를 의미한다.

② 정보자산 보안 관리 프로세스:

- 생성: 보안 등급 및 보관 기간에 따라 분류하여 관리
- 보관: 전자 정보 자산은 중앙 시스템에 등록하며, 실물 정보 자산은 보안 등급에 따라 관리
- 반출: 정보 자산은 사전 승인 없이 반출 금지되며, 승인 후에도 모든 전송 내역을 저장해 정보유출 사고에 대비

### 02) 데이터 보호 조치

① 정보 자산 유출 방지와 침해 사고에 신속히 대응하기 위해 보안 솔루션을 적용하여 운영한다.

② 당사는 데이터의 데이터 무결성 확보를 위하여 사용자가 직접 접근할 수 없도록 통제하여야 한다.

③ 정상적인 인증방법 외의 방법을 통한 데이터 수정을 금지하며, 수정 필요시, 운영 담당자의 승인하에 인가된 인원에 한하여 수정이 가능하다.

④ 데이터베이스간 또는 데이터파일 공유는 원칙적으로 금지하며, 반드시 필요한 경우 보안성 검토 등 적절한 보안대책을 적용하여야 한다.

### 03) 보안시스템 로그 관리

① 당사는 보안시스템 로그가 위·변조되지 않도록 관리적, 기술적 보호 조치를 취하여야 한다.

② 중요 로그는 제 3 의 장소에 백업하고 안전하게 관리하여야 한다.