한화첨단소재

문서관리번호	HAMC-I02-4
최초 제정일	2025.07.22
최신 개정일	2025.07.22
문서 관리자	경영혁신팀

정보보호 정책

(Information Security Policy)

2025.7

<정보보호정책>
1. 임직원은 회사 정보보호 정책을 성실히 준수하며, 정보보호 관련 법규 및 내부 규정이 있을 경우 이를 우선적으로 따른다.
2. 정보자산은 승인된 목적에만 사용하며, 무단 접근이나 유출을 금지한다.
3. 보안 사고 발생 시 관련부서와 정부기관에 보고하고 즉시 대응한다.
4. 각 국가별 개인정보보호법 등 보안관련 법률을 성실히 준수한다.

1. 정보보호 정책 개요

1.1 정보보호 침해 예방 교육

1) 모든 직원이 정보보호 규정을 숙지하고 실천할 수 있도록 정기적으로 정보보호 교육(온라인 or 오프라인)을 실시한다.

2) 신규 입사자에게는 보안 정책 가이드를 제공하여 교육한다.

1.2 정보보호 정기 점검

- 정보보호 위반을 방지하고 보호 정책 준수를 확립하기 위해 정기적인 내부 점검을 실시한다.

1.3 정보보호 리스크 평가 수행

- 정기적으로 정보보호 리스크 평가를 수행하여 잠재적인 보호 위협을 사전에 식별하고 대응 방안을 마련한다.

1.4 고객 및 제3자 데이터 보호

- 고객 및 제3자의 데이터를 보호하기 위해, 승인되지 않은 접근이나 공개를 방지하는 보호 조치를 마련한다.

1.5 이해 관계자의 동의 정책

1) 기밀 정보의 처리, 공유 및 보관에 대한 명확한 절차로 운영한다.

2) 관련하여 임직원, 협력사 등 이해관계자에게 사전 동의를 받는다.

1.6 개인정보보호 정책

1) 개인정보와 관련된 정보는 각 국가별 법적 사항을 준수하여 처리한다.

2) 정보주체의 동의 없이 개인정보를 처리하거나 공유하지 않는다.

2. 이행 방안

2.1 정보보호 위반 처리 절차 운영

1) 임직원 및 이해관계자는 내부 정보 유출 등 정보보호 위반 사고를 신속하고 안전하게 처리할 수 있는 내부고발 채널과 절차를 마련한다.

2) 신고 접수 즉시, 주관 부서에서 위반에 대한 해결방안을 논의하고 신속히 조치한다.

3) 신고인의 인적사항이나 정보를 다른 사람에게 공개하지 않으며 관련된 모든 내용은 비밀로 취급하여 신고인의 불이익 없도록 조치한다.

<정보보호 신고 채널>

담당자: 경영혁신팀 보안담당자

한화첨단소재 홈페이지 내 제보하기 채널:

https://www.hwam.co.kr/kr/sustainability/report.do

2.2 정보보호 사고 대응 절차

1) 정보보호 사고 발생 즉시, 회사 경영에 피해를 최소화하기 위하여 네트워크망을 원천 차단 조치하고 아래 신고 기준에 따라 신고한다.

- 사고 유형별 신고 기준

. 경미한 사고(랜섬웨어 초기 감염 등): 각 법인 자체 조치

. 중대 피해(랜섬웨어 확산, 네트워크 마비 등): 본사 주관부서 신고

※ 각 국가별 법률에 따라 정보보호 관련 정부기관 및 경찰에 신고

2) 정보보호 사고 원인을 파악하고 추가 피해가 발생하지 않도록 신속히

조치하며, 정보 유출 중요도를 즉시 파악한다.

3. 부칙

1) 본 정보보호 정책은 2025.07.22부로 제정하여 시행한다.