문서 관리번호	H123000192 71-20260602-010830
최초 제정일	2026년 6월
문서 관리부서	정보보안운영팀

현대제철㈜ 정보보안 정책

제·개정이력	차수	제·개정일	주요 내용
	0	2026년 6월	초도 제정

[담당]	[승인]
정보보안운영팀	경영지원본부장

제1조 총칙

① 제정 목적

본 정책은 현대제철 주식회사(이하 ' 회사 ' 또는 ' 당사 ' 라 한다)의 유무형 자산, 영업비밀 및 경영 활동에 필요한 체계를 정의하고, 지속적인 보호활동을 통해 보안사고를 예방하며 회사의 안정적인 발전에 기여함을 목적으로 한다.

② 적용 범위

본 정책은 회사 임직원 및 상주 협력사 인원, 기타 회사를 출입하거나 회사의 정보자산을 취급하는 모든 제 3자에게 적용되며, 회사의 모든 문서, 시설, 정보시스템 및 정보처리 장비에 적용된다.

③ 지속적 개선

회사는 보안 환경의 변화와 신규 위협에 대응하기 위해 정보보안 경영체계를 주기적으로 검토하고 지속적으로 개선한다.

제2조 정보보안 조직 및 책임

① 조직의 구성

1. 정보보안 관리활동을 체계적으로 이행하기 위하여 전사 정보보안 최고책임자(CISO), 전사 정보보안 총괄부서, 부서 정보보안 책임자/담당자, 전사 보안위원회 등으로 구성한다.
2. 전사 정보보안 총괄부서는 보안 위협을 실시간 모니터링하고, 이상 징후 발견 시 즉각 대응할 수 있는 관제 체계를 운영한다

② 정보보안 책임과 의무

1. 임직원은 회사 및 제 3자의 정보를 업무 목적 외로 사용하거나 승인 없이 외부에 공개 · 누설해서는 안되며, 회사의 보안규정에서 정한 책임과 역할을 준수해야 한다.

   또한 회사에 손실을 초래할 수 있는 보안위반 사항을 인지한 경우, 이를 즉시 보안 주관 부서에 보고 할 의무가 있다
2. 외주사(공급사)는 계약 또는 협력 범위 내에서 회사가 정한 정보보안 요구사항을 준수할 의무가 있다. 회사는 필요 시 외주사(공급사)의 정보보안 준수 여부를 점검할 수 있으며, 위반시 계약상의 조치를 취할 수 있다.

제3조 정보자산 관리 및 보호 원칙

① 정보자산 식별 및 분류

회사는 보유한 모든 정보자산을 식별 · 분류하여 중요도에 따라 적절한 보호조치를 적용하며, 임직원은 분류된 등급에 따라 자산을 취급하고 보호조치를 준수해야 한다.

② 정보자산 취급 및 보호 기준

정보자산은 등급, 유형 및 활용 목적에 따라 정해진 보호 기준에 따라 취급되어야 하며, 임직원은 자산의 무단 접근, 유출 및 무단 변경(무결성 훼손)을 방지하기 위해 해당 기준을 준수해야 한다.

③ 정보자산의 사용 및 반출 통제

1. 정보자산은 업무 수행에 필요한 범위에서만 사용되어야 하며, 불필요한 접근 · 활용은 금지한다.
2. 정보자산을 외부로 반출할 경우에는 사전에 정해진 승인 절차를 준수해야 하며, 자산의 중요도에 따라 적절한 보호조치를 적용해야 한다.

제4조 개인정보보호

① 개인정보보호 관리

1. 회사는 임직원 및 고객의 개인정보를 보호하기 위해 개인정보보호 관리체계를 운영하고, 내부 규정과 책임자 지정을 통해 체계적인 보호 활동을 수행한다.
2. 개인정보 라이프사이클에 따라 동의서 관리, 처리방침 수립, 파기 등 관리적 조치와 함께 암호화, 접근통제, 악성코드 방지 등 기술적 보호조치를 실시한다.

② 개인정보보호 원칙

1. 회사는 개인정보 처리 목적을 명확히 하고, 그 목적에 필요한 최소한의 개인정보만을 적법하고 정당하게 수집 · 이용한다.
2. 개인정보의 정확성과 최신성을 유지하고, 처리 과정에서 부당하게 변경 · 훼손되지 않도록 적절한 관리적 · 기술적 · 물리적 보호조치를 적용한다.
3. 필요한 경우 개인정보는 익명 또는 가명으로 처리하여 위험을 줄이며, 모든 처리 과정에서 관계 법령에 따른 책임과 의무를 준수하여 정보주체의 신뢰를 확보한다.

제5조 보안사고 대응 및 조치

① 보안사고 예방

1. 회사는 시스템 도입 및 변경 시 보안성 검토를 수행하고, 정기적인 취약점 점검과 긴급 보안조치를 통해 잠재적 위험을 사전에 제거한다.
2. 불필요한 계정 관리, 최신 해킹 기법 대비, 기술 · 관리적 조치를 통해 보안 취약요인을 지속적으로 최소화한다.

② 보안사고 대응 및 사고처리

1. 보안사고 발생 시 원인판단, 백업 실시, 침입 흔적 수집, 서비스 보호 조치를 우선으로 하며 필요한 경우 네트워크 차단 등 즉각적인 대응을 수행한다.
2. 사고 처리 과정에서 로그 분석, 악성코드 및 백도어 확인, 계정 무결성 검증 등을 통해 침입 여부와 피해 범위를 정확히 파악한다.
3. 사고 원인 제거 및 복구 조치를 완료한 후 취약점 점검을 수행하여 안전성이 확인된 경우에만 서비스를 재개한다.

③ 보안사고 사후조치

1. 임시 조치된 문제의 근본 원인을 제거하고 재발방지 대책을 마련하며, 필요 시 임직원 공지 · 교육을 실시한다.
2. 사고 기록 · 증거를 보존하고 법적 대응을 위해 안전하게 관리하며, 내부자 위반 시 사규에 따른 조치를 시행하고 승인되지 않은 정보 유출을 금지한다.