최종 수정일	2025.07
문서 관리자	정보보호팀

현대엔지니어링 정보보안 정책

목 차

1. 개요

가. 제정목적

본 규정은 현대엔지니어링 주식회사(이하 '회사' 또는 '당사'라 한다)의 유·무형의 모든 자산을 내·외부 위협으로부터 안전하게 보호하여 회사 경쟁력을 유지·강화하고, 정보자산을 건전하고 안전하게 활용할 수 있는 환경을 조성하여 회사발전과 대외 신뢰도 향상에 기여하는 것을 목적으로 한다.

나. 적용범위

본 규정은 회사의 모든 임직원, 협력사 등 계약관계에 있는 제3자 및 출입자와 정보자산이 기록, 저장, 활용되는 모든 매체, 전산장비 및 관련시설을 포함한 모든 정보자산에 적용한다. 당사의 임직원 등 회사와 계약관계에 있는 모든 사람은 신의와 성실의 원칙으로 본 규정과 이를 기반으로 한 지침을 준수한다.

다. 일반사항

1. 회사의 영업비밀 등 중요한 자산의 유출 및 파괴를 예방하고, 정보시스템의 안정적인 운영을 통해 신뢰성 있는 업무연속성을 보증하며, 보안사고에 따른 업무상의 손실을 최소화하기 위해 노력한다. 또한, 급변하는 사이버 환경에 대응하기 위해 정보보안 관리체계를 정기적으로 점검하고 최신 기술 및 대응 체계를 반영하여 지속적으로 개선한다.
2. 수립한 정보보안 정책의 실현을 위하여 다음과 같은 목표를 달성한다.

(1) 각종 위협으로부터 조직 내 정보자산에 대한 보호
(2) 정보보호업무 수행을 위한 인적 구성 및 시설과 제도 등 운영방안 마련
(3) 정보자산에는 인가된 사람만이 접근하도록 통제 대책 운영
(4) 정보자산에 대한 관리적·물리적·기술적 정보보호 대책 강구
(5) 정보자산에 대한 관리 등 정보보호 교육의 실시
(6) 각종 침해사고 및 재난에 대비하는 침해사고 대응 계획의 수립 및 운영
(7) 서비스 및 업무가 중단되지 않도록 업무연속성의 보장
(8) 유관 법률의 준수 및 준거성 확보에 대한 사항
(9) 기타 회사가 별도로 정하는 사항 등

2. 보안책임 및 조직

가. 책임사항

본 책임 사항은 정보보안 총괄 책임 사항을 위주로 하며, 임직원의 정보보안 관련 책임을 명시한다.

1. 회사보안대표는 대표이사로 하며, 회사의 보안업무 총괄에 대한 책임과 권한이 있다. 보안대표는 각 본부의 보안업무를 본부/센터/실 보안책임자에게 위임하고, 보안경영활동 총괄 업무를 정보보호최고책임자에게 위임한다.
2. 정보보호최고책임자(CISO)는 보안총괄책임자로서 보안에 관련한 모든 정책을 결정한다. 전사 정보보호 계획 수립, 시행 및 개선, 정보보호 실태 감사, 개선 지시 및 관리, 정보호호 위험의 식별 및 평가 정보보호 대책 마련, 정보보호 교육과 모의 훈련 계획 수립하고 실시한다.
3. 개인정보보호책임자(CPO)는 개인정보보호 업무의 기획, 시행, 관리 및 감독을 담당한다.
4. 당사의 임직원은 보안관련 회사표준(규정 지침 등)을 숙지하고 준수할 의무를 가지고 있으며, 보안 교육 참석 및 자체 점검 등 회사 보안 활동에 적극 참여해야 한다. 보안 관련 회사표준 위반 등 보안 사고 위험성 인식 시 지체없이, 팀/현장 보안 책임자, 전사보안담당자에게 신고하여야 한다.

나. 정보보안 문화 형성 및 조직운영

1. 전사보안 담당자는 연간 보안교육계획을 수립하고 정보보호최고책임자의 검토·승인을·받는다
2. 전사보안담당자는 연간 보안 교육 계획에 따라 연1회 이상 정기적으로 교육을 시행하고, 관련 법규 및 규정의 중대한 변경 시 이에 대한 추가 교육을 시행할 수 있다.
3. 전사보안담당자는 임직원 및 외부인에게 회사의 보안 준수사항, 보안 위반 행위로 인한 피해 사례를 포함한 교육 관련 자료를 제공할 수 있다.
4. 전사보안담당자는 보안 관련 전문성을 강화하기 위해 주기적으로 사내·외 전문 교육 과정을 이수하여야 한다.
5. 임직원은 보안 교육을 연 1회 이상 수강해야 한다.
6. 전사보안담당자는 보안 교육 시행 후 교육에 대한 효과성을 측정(예: 설문지, 시험 등)하여 개선 사항을 차년도 보안 교육 계획에 반영한다.
7. 팀/현장 보안책임자는 내/외부 보안사고 발생 등 보안상 필요하다고 판단되는 경우 팀원에 대한 보안교육을 실시할 수 있다.
8. 사내 규정 변경 등 전달사항이 있는 경우 팀/현장 보안담당자가 팀 내 전달교육을 시행하도록 한다.

3. 보안위협 및 사고대응

가. 위험식별

1. 전사보안담당자는 이슈 및 요구사항(Context) 기반의 이슈위험분석을 연 1회 이상 실시하며 그 결과를 정보보호최고책임자에게 보고한다.
2. 회사의 위험관리 절차는 ISO31000 및 ISO27005의 위험관리 프레임워크를 준용한다.
3. 위험관리 방법은 현실적으로 목표를 달성할 수 있는 수준으로 결정한다.
4. 정보보호최고책임자는 회사의 보안관리체계를 구성하는 환경의 중대한 변화가 발생되었을 경우 등 위험분석의 재실시가 필요하다고 판단된 때에는 주기와 상관없이 위험분석을 실시할 수 있다.

나. 사고대응 및 보고 절차

1. 회사는 보안사고의 효과적 대응을 위해 대응체계를 구축·운영하고 불법적인 유출, 침해 시도 발생 시 구성원의 행동 요령을 포함하는 대응지침을 수립하여야 한다.
2. 모든 임직원은 보안사고의 징후가 인지되면 가능한 빠른 시간 내에 전사보안담당자에 보고한다.
3. 외부에서 침입한 흔적이 의심되는 경우 전사보안담당자는 보안진단 도구나 체크리스트를 이용하여 점검해야 하며, 데이터의 변조나 불법 접근이 있는 경우 해당 서비스를 중지시킨다.
4. 침해사고에 의한 정보시스템의 장애 시 신속히 복구되어야 하며, 장애 복구에 대한 모의 훈련이 년 1회 이상 주기적으로 실시되어야 한다.
5. 공개가 허용된 침해사고는 임직원에게 공지 또는 교육해야 한다.
6. 보안사고 발생시 피해를 최소화하기 위하여 정해진 대응절차에 따라 신속히 대응한다.

4. 부칙

본 정책은 현대엔지니어링의 정보보호 규정을 외부 이해관계자에게 투명하게 전달하고, 기업의 지속가능경영 및 책임경영 원칙을 공유하기 위해 작성된 **공시용 기준 문서**입니다.