SeAH 세아제강

최종 승인일	2025. 11. 6.
작성부서	DX 팀

정보보호처리방침

(Information Security Policy)

Rev. 0

제 1 장. 총칙

제 1 조. 목적

본 정책은 ㈜세아제강(이하 '회사')의 정보자산을 보호하고 보안업무를 수행하는데 필요한 제반 사항을 정의하고 이를 업무에 적용함으로써 정보자산의 기밀성, 무결성, 가용성을 확보하는 것을 목적으로 합니다.

제 2 조. 적용 범위

① 본 규정은 회사가 보유하고 있는 모든 정보자산을 대상으로 하며, 전 임직원 및 회사의 업무에 종사하는 외부회사 임직원 등을 포함하여 적용합니다.

② 단, 이 규정에 정한 범위 내에서 특수성과 실정에 따라 회사의 외부 출입자 및 기타 회사와 계약관계가 있는 특수인에게도 적용할 수 있습니다.

③ 회사에서 보유하고 있는 유·무형의 자산(이하 "자산") 및 영업비밀 등 모든 정보자산(이하 "정보자산", 이하 자산과 정보자산을 통칭하여 "회사자산")을 대상으로 합니다.

제 3 조. 승인 및 효력

본 규정은 정보보호책임자의 검토 및 승인 절차를 거친 후 회사 전반에 걸쳐 효력을 가집니다.

제 4 조. 정보보호 역할 및 책임

① 회사의 모든 임직원은 정보보호를 준수하고 유지할 책임이 있습니다.

② 정보자산을 사용하는 임직원은 관련 규정을 준수하며, 정보보호 사고 발생 시 즉시 보고하여야 합니다.

③ 정보자산을 관리하거나 타 사용자에게 제공하는 직원은 해당 정보자산의 기밀성, 무결성, 가용성을 보장할 책임이 있습니다.

④ 정보보호책임자는 회사의 정보보호에 대한 최종 관리 책임을 가집니다.

⑤ 회사의 정보자산을 이용하는 외부 개인 또는 조직은 회사가 정한 보안 규정을 준수하고 정보자산을 보호할 의무가 있습니다.

제 5 조. 위반 시의 처벌

임직원, 외부 인력(아웃소싱 및 계약직 포함)이 본 규정을 위반하여 회사의 보안 수준에 부정적 영향을 미친 경우, 관련 사규에 따른 징계 또는 계약상 제재를 받을 수 있으며, 필요 시 법적 조치가 병행될 수 있습니다.

제 2 장. 정보보호관리체계

회사는 정보보호관리체계를 운영하여 정보보호 조직을 구성하고 정보보호 활동의 기반을 마련합니다.

제 6 조. 정보보호 조직의 책임 및 역할

정보보호 조직의 책임 및 역할은 다음과 같습니다.

구분	책임 및 역할
정보보호책임자	- 정보보호에 대한 관리 총괄 - 정보보호 조직을 구성 - 정보보호 정책의 구현 및 검토 - 정보보호 방향 설정 및 지원 제공 - 정보보호 통제 구현에 관한 제안, 협의, 조정
정보보호관리자	- 정보자산 보호와 정보보호 정책서 및 지침에 기재된 보안 프로세스 수행관련 권한과 책임의 규정 - 보안과 관련한 자문의 획득 및 결과의 공지 - 외부 보안 관련 기관과의 연락체계 관리 - 위험분석 및 내부감사 결과 검토
정보보호담당자	- 정보보호관리자의 업무 지원 - 정보보호 관련 업무 정책 및 지침에 대한 준수 사항 점검 - 기술적 보호 구현에 대한 기록 및 검토 - 정보시스템에 대한 위험평가 및 점검 수행

제 7 조. 정보보호 조직체계

① 회사는 정보보호 업무를 총괄하는 정보보호책임자를 지정하며, 필요 시 이를 지원하기 위한 관리·담당 조직을 둘 수 있습니다.

② 각 구성원은 책임과 역할에 대한 명확한 인지를 하여야 합니다.

제 3 장. 정보자산의 보안 관리

회사는 정보자산의 중요도와 특성에 따라 적정한 보호 수준을 정하고, 훼손·변조·도난·유출 등 위험으로부터 안전하게 관리하기 위한 기준을 수립·운영합니다.

제 8 조. 정보자산 분류 및 관리

① 회사의 모든 정보자산은 식별되고, 식별된 정보자산에 대해서 목록을 작성하여 관리합니다.

② 회사의 정보자산에 대한 중요도를 평가하여 등급별로 분류하고 정기적으로 적정성을 검토하여야 합니다.

③ 중요 정보자산은 주기적으로 점검·분석하고, 발견된 취약점은 개선 대책을 마련하여야 합니다.

④ 중요 데이터 및 문서의 폐기 시에는 복구가 불가능한 방법으로 처리합니다.

제 9 조. 정보자산의 위험관리

① 회사는 정보자산의 중요도, 취약성, 위협 정도를 고려하여 위험을 평가하고, 이에 따른 관리 방안을 수립합니다.

② 회사는 관리 방안 수립 시에는 위험의 긴급성, 필요한 자원, 구현 가능성 등을 종합 고려하여 우선순위를 정합니다.

③ 위험 관리 절차는 회사의 보안 관리체계에 따라 정기적으로 검토·개선합니다.

제 4 장. 정보기기 보안 관리

회사의 PC 등 정보기기의 사용, 반출·입에 대해 발생할 수 있는 정보보호 취약점을 사전에 예방함으로써, PC 등 정보기기 사용의 안전성과 신뢰성을 높이는데 그 목적이 있습니다.

제 10 조. 정보기기 보안 관리

① 회사에서 지급한 업무용 PC는 회사의 정보보호정책을 준수하여 사용 및 관리하여야

합니다.

② 업무용 PC는 본래 사용 목적 외의 용도로 사용하지 않아야 하며, 업무용 PC의 관리 부주의에 따른 보안 사고가 발생하지 않도록 보호 대책을 수립하여 관리하여야 합니다.

③ 업무용 PC에 응용프로그램을 설치, 운영할 경우 사용허가 및 등록 절차에 의해 허가된 응용프로그램만 사용할 수 있습니다.

④ 업무용으로 개인 보조저장매체를 사용하지 않아야 하며, 부득이하게 사용해야 할 경우 사용허가 및 등록 절차에 의해 허가된 매체만 사용할 수 있도록 합니다.

⑤ 보조저장매체의 반출·입 절차를 수립하여 보조저장매체의 보유현황을 파악해야 합니다.

⑥ 보조저장매체의 폐기 및 재사용, 분실 등으로 인한 정보유출에 대하여 대책을 마련하여야 하며, 정보유출을 방지할 대책을 강구할 수 없는 경우에는 해당 보조저장매체의 반출 전에 저장된 모든 데이터를 복구가 불가능한 방법으로 파기해야 합니다.

제 5 장. 정보시스템 보안 관리

회사의 정보시스템 보안에 필요한 사항을 정하고, 이를 적용하여 운영, 관리하도록 함으로써 회사의 정보자산을 안전하고 효율적으로 보존 관리합니다.

제 11 조. 사용자 인증 및 식별

① 구성원, 외부인력 등의 사용자를 대상으로 어플리케이션, 서버, 네트워크 장비, DB 등의 정보시스템 접속 시 인증을 통해 필요한 최소의 권한만을 부여받도록 함으로써 인가되지 않은 사용자의 접근 및 정보의 사용을 통제하여야 합니다.

② 정보시스템의 인증 구현 시 사용자 및 업무의 중요도, 접근 과정에 따른 위험, 자원의 중요성 등을 고려하여 인증 방식을 차등 적용하여야 합니다.

제 12 조. 계정 및 권한 관리

① 정보시스템 계정(ID)의 등록, 변경, 삭제 등에 대한 관리 기준을 수립하고 유지해야 하며, 변경 이력을 일정 기간 보관하여야 합니다.

② 주요 정보시스템의 권한 부여 시 취급 정보, 사용자, 직무에 따른 역할을 기반으로 최소한의 권한만을 부여해야 하며, 정기적으로 검토를 수행하여야 합니다.

③ 1인 1계정 사용을 원칙으로 하고, 공용계정 사용을 금지합니다. 다만 내부 사정 등으로 인하여 공용 계정의 사용이 불가피한 경우 정보보호 조직의 승인을 받아야 하며, 승인 받은 목적 내에서만 제한적으로 사용할 수 있습니다.

제 13 조. 패스워드 관리

① 패스워드는 대문자, 소문자, 숫자, 특수문자를 포함한 10자리 이상으로 설정하며, 타인에게 노출되지 않도록 관리하여야 합니다.

② 다만, 자체 시스템 보안 정책에 따라 별도의 패스워드 기준을 적용할 수 있으며, 정보보호 조직의 사전 승인 하에 운영할 수 있습니다.

제 14 조. 서버 보안 관리

① 서버를 도입할 경우에는 보안성에 대한 검토를 실시하여야 하고, 적절한 보안설정을 적용하여야 합니다.

② 서버의 보안성 확보를 위해 OS 및 소프트웨어의 주요한 패치를 지속적으로 적용하며, 패치는 반드시 사전 테스트를 통해 보안패치의 안전성과 기존 시스템과의 호환성을 검증 후 적용하여야 합니다.

제 15 조. 네트워크 보안 관리

① 업무의 특성 및 중요도에 따라 네트워크 영역을 분리하고, 분리된 네트워크 영역 간에는 접근통제를 수행하여야 합니다.

② 네트워크 이용에 대한 접근 규칙 및 보안성 검토 등을 통한 점검 및 보호대책을 수립하고 적용해야 합니다.

③ 정보보호 조직의 승인 없이 무선 AP(Access Point) 장비를 내부 네트워크에 연결하여 무선 네트워크를 구축을 금지합니다.

제 16 조. 데이터베이스 보안 관리

① 데이터베이스는 무결성 확보를 위하여 사용자가 직접 접근할 수 없도록 통제하여야 합니다.

② 데이터베이스의 접근권한은 사용자의 직무별로 구분하여 부여하고, 특정 명령(Update, Delete 등)은 권한이 부여된 자만이 사용 가능 하도록 통제하여야 합니다.

제 17 조. 정보보호시스템 보안 관리

① 네트워크를 통한 침입을 방지하기 위한 기술적 수단으로써 방화벽, 침입차단시스템, 가상사설망 등의 정보보호시스템을 설치·운영하여야 합니다.

② 정보보호시스템의 보안정책이 변경되어야 하는 경우 반드시 정보보호 조직의 승인을 득한 후 수행해야 하며, 관련 내역을 반드시 기록·관리하여야 합니다.

제 6 장. 응용프로그램 보안 관리

회사의 응용프로그램을 개발, 운영, 사용하는데 있어 정보보호 사항을 정의하고 응용프로그램 및 데이터의 안전성을 보장하는데 그 목적이 있습니다.

제 18 조. 응용프로그램 보안 관리

① 신규 개발 또는 변경되는 응용프로그램은 보안 요구사항을 반영하여 설계·개발되어야 하며, 운영 전 보안성 검토를 거쳐야 합니다.

② 개발 프로젝트는 분석, 설계, 개발, 테스트, 운영이관 등 전 단계에서 보안성을 고려하고, 세부 기준은 별도의 개발 보안 지침에 따릅니다.

제 19 조. 응용프로그램 개발 보안 관리

① 시스템 개발 및 테스트 환경은 운영 환경과 분리하는 것을 원칙으로 하여야 합니다.

② 운영 응용프로그램의 주요 변경을 통제하기 위한 절차를 수립하고, 변경내역은 사고 및 장애 발생 시 원인 규명을 위해 기록, 관리하여야 합니다.

③ 응용프로그램 테스트 시 운영 데이터의 유·노출을 방지하기 위해 임의의 테스트 데이터를 생성하여 활용하거나 운영 데이터를 가공하여 사용하도록 하며 실제 운영 데이터의 사용을 금합니다.

④ 응용프로그램을 운영 단계로 이관 시, 다음 각 호의 보안 사항을 준수하여야 합니다.

1) 개발자 이외의 이관 담당자 지정

2) 테스트 후 이관

3) 보안 점검 후 이관

4) 이관 시 문제에 대한 대응방안 마련

제 7 장. 물리 보안 관리

구성원, 외부인력 또는 방문자 등을 대상으로 시설 또는 정보자산의 중요도에 따른 물리적인 보호대책을 수립 및 운영함으로써 회사자산을 보호하는데 그 목적이 있습니다.

제 20 조. 보호구역 분류 기준

① 정보자산의 중요도를 고려하여 정보를 보호해야 할 필요가 있는 사무실 등 물리적인 장소를 보호구역으로 선정하고 일반구역, 제한구역, 통제구역으로 구분하여 운영하여야 합니다.

② 일반구역은 중요 회사자산이 보관되지 않아 외부인의 출입이 허용되는 구역으로서 접견실, 안내실 등을 말합니다.

③ 제한구역은 일부 중요 회사자산이 보관되어 있는 장소로서 외부인력의 출입이 제한적으로 허용되는 구역으로서 사무실, 회의실, 문서고, 상황실 등을 말합니다.

④ 통제구역은 외부인력의 출입이 엄격히 금지되고, 임직원은 업무적 필요에 따라 최소한의 인원만이 출입이 가능한 구역입니다. 전산실, NW장비실, 서버실 등이 통제구역에 해당합니다.

제 21 조. 보호구역 출입 및 감시

① 보호구역에 대한 임직원 및 외부인력의 출입내역을 기록·보관하고, 주요 제한구역 및 통제구역의 출입기록에 대해서는 주기적으로 적정성을 검토하여야 합니다.

② 통제구역 내에 정보자산의 불법 유출을 방지하기 위해 회사자산의 반출·입 시에는 정보보호 조직의 승인을 득하도록 통제 절차를 수립하여야 합니다.

제 22 조. 시설 보호

① 환경적, 자연적 위협으로부터 건물 및 시설을 보호하기 위해 방재, 방화, 항온·항습, 케이블 보호, 랙 실장도 관리, 비상전원 설비 등을 갖추어 최적의 상태를 유지하여야 합니다.

제 8 장. 침해사고 대응

침해사고 발생을 사전에 예방하고 사고 발생 시 체계적인 대응을 위한 방법과 절차를 제시함으로써 효과적인 대응과 피해를 최소화하는데 그 목적이 있습니다.

제 23 조. 침해사고 대응 계획

① 회사는 침해사고에 대한 신속하고 체계적인 대응을 위해 침해사고 대응체계를 마련하여야 합니다.

② 침해사고를 예방하기 위해 사전 모니터링 및 탐지·대응 체계를 구축하여 운영하고, 불법적인 정보유출과 보안 침해 시도에 대응하여야 합니다.

③ 침해사고가 발생한 경우, 신속하게 대응하여 피해를 최소화하고 사고 경위 및 원인 등을 분석하여 필요한 조치를 하여야 합니다.

제 24 조. 침해사고 대응 절차

① 침해사고 발생 시, 정보보호조직은 관련 부서와 협력하여 원인과 영향을 신속히 조사·분석하고 피해 확산을 최소화하기 위한 대응 및 복구를 수행합니다.

② 침해사고 대응 완료 후 관련 기록을 분석하여 재발방지 대책을 수립하고, 필요 시 별도의 교육 또는 훈련을 실시할 수 있습니다.

제 9 장. 재해복구 관리

재해복구 측면에서 체계적인 대응을 위한 방법 및 절차를 수립하여 효과적인 대응과 피해를 최소화하는 데 목적이 있습니다.

제 25 조. 재해복구 계획 수립

① 재해, 사고, 장애 발생 시 핵심 업무를 지속하기 위한 비상 대응 방안으로 위험 영향도에 따른 우선순위, 처리시간에 따른 긴급도를 정의하여 재해복구 계획을 수립하여야 합니다.

② 주요 서비스 및 IT 자산의 복구목표시간과 복구목표시점을 달성할 수 있도록 비용을 고려하여 효과적인 복구전략 및 계획을 수립하여야 합니다.

제 26 조. 재해복구 계획의 가동

① 재해복구 계획에 따라 위기상황 발생 시 위기 상황의 발생원인, 발생 범위 등 관련 정보를 수집하고 분석하여야 합니다.

② 업무영향분석에 따라 핵심업무 복구 우선순위, 업무복구 목표정의를 기준으로 재해복구계획을 따라 대응하여야 합니다.

③ 위기상황이 종료된 후에는 대응 결과를 분석하여 복구 계획의 미흡점을 개선하여야 합니다.

부칙

본 정책은 2025. 11. 6. 부로 제정하여 시행한다.