정보보호 정책

2024. 01. 10. 제정

(주)조강기업

정보보호 강령

정보통신 기술의 발달에 따라 새롭게 파생되고 있는 각종 위협들은 ㈜조강기업의 중 요 자산인 정보시스템과 정보에 심각한 영향을 미칠 수 있게 되었으며, 정보보호 활동은 통신서비스의 활성화뿐 아니라 나아가 ㈜조강기업의 생존을 위한 필수 불가결한 요소 가 되었다. 따라서 ㈜조강기업의 구성원들은 다음에 제시하는 정보보호 정책을 기초로 정보자산의 보호를 위해 최선을 다하여야 한다.

첫째, 임직원은 정보를 보호해야 할 중요한 자산으로 인식하고 처리해야 한다. 중요 정보 자산에 대한 접근시 사용자 식별 및 인증 절차를 거쳐야 하고, 사용자는 불법적인 접근을 시도하거나, 패스워드 등을 다른 사람과 공유해서는 안되며, 부서장의 승인없이 외부에 유출 또는 공개해서는 안된다.

둘째, 전 임직원은 정보보호의 중요성을 인식하고 정보보호 능력을 배양할 수 있도록 각자의 직무와 부합하는 적절한 수준의 정보보호 교육을 받아야 한다. 또한 정보보호 활동과 관련 포상 및 처벌 기준을 공정하게 수립하여 시행함으로써 정보보호 활동에 대한 동기를 부여하여야 한다.

셋째, 정보보호와 관련된 모든 방침 및 지침은 자산에 대한 기밀성·무결성·가용성을 확보할 수 있도록 수립, 검토, 시행되어야 하며, 이러한 일련의 활동들은 정보보호 담당조직에 의해 일관성 있게 추진하여야 한다.

넷째, ㈜조강기업의 모든 자산은 그 가치와 중요도에 따라 등급을 분류하여 각 등급별로 적절한 절차에 의거 관리되어야 하며 주기적으로 자산의 가치를 재평가하여 정보보호 정책 및 지침에 반영하여야 한다.

다섯째, ㈜조강기업의 모든 정보자산은 인가된 인원에 한하여 접근 가능하도록 적절 한 조치를 취해야 하며 중요 정보자산을 운영·관리 하는 지역은 비인가자의 접근, 정전, 화재, 수해 등 각종 재난과 사고로부터 보호하여야 한다.

여섯째, ㈜조강기업의 정보 자산이 침해사고 및 내·외부인력의 고의적이거나 우발적인 침입에 의해 손상을 입었을 경우에도 회사는 사업을 지속할 수 있어야 하며 신속히 정보 자산을 복구하여 피해를 최소화하도록 침해사고 대응계획이 수립되어 관리하여야 한다.

일곱째, ㈜조강기업 정보시스템의 운영은 업무의 특성을 고려하여 적절히 분배되어 야 하며 사전에 정의된 절차에 따라 수행하여야 한다. 또한 정보시스템 운영에 관한 기록을 유지·관리함으로써 향후 정보시스템의 운영 계획의 수립 및 침해사고 발생시 그 기록이 반영 되도록 하여야 한다. 이는 정보 자산의 관리 책임은 자신에게 있음을 의미하는 것으로, 중요 정보 자산에 대해서는 작성자, 작성일자, 사용자가 명확히 지정되어야 하고, 사용시에는 사용 실적의 추적이 가능하도록 관리하여야 한다.

여덟째, 유해한 소프트웨어로부터 ㈜조강기업의 정보시스템을 보호할 수 있도록 조치를 취하여야 하며 업무와 관련이 없는 정보시스템 사용으로 인하여 정보자산이 외부로 유출되거나 정보시스템의 성능이 저하되지 않도록 하여야 한다.

아홉째, ㈜조강기업의 모든 정보보호 활동은 상급기관의 관련 지침, 지적재산권 및 개인정보보호에 관한 법률 등을 준수해야 하며 정보보호 활동이 지침과 절차에 의해 올바르게 수행되고 있는지 주기적으로 점검하여야 한다.

㈜조강기업의 구성원은 성공적인 정보보호가 세계적인 기업 경쟁력을 갖추기 위한 지름길임을 다시 한번 인식하고 정보보호를 위해 최선을 다해야 할 것이다.

㈜조강기업

목 차

제 1 장 총 칙

제 1 조 (목적)

본 규정은 ㈜조강기업(이하 "회사"라 함)의 자산에 대한 내·외부로부터의 훼손, 변조, 도난, 유출 등의 다양한 형태의 위협으로부터 효과적으로 보호하기 위하여 임직원이 준수하여야 할 정보보호 상위 정책의 규정을 목적으로 한다.

제 2 조 (범위)

본 규정은 회사에 근무하는 전 임직원을 대상으로 적용되며, 계약관계에 의하여 회사의 자산에 접근하는 모든 제 3 자에게도 적용된다.

제 3 조 (용어의 정의)

본 규정에서 사용되는 용어는 정보보호관리지침에서 규정된 '용어의 정의'를 사용한다.

제 4 조 (책임사항)

회사의 정보보호에 대한 책임은 전 임직원에게 있으며 이를 위하여 정보보호 관련 사규를 모든 임직원이 숙지하여 준수하여야 한다.

① 모든 임직원이 본 정책서의 내용을 숙지하여 생활화하기 위해서 적절한 교육이 시행되어야 하며, 정보보호담당부서는 이에 대한 책임이 있다.

② 법적, 규범적, 해당 감독기관의 요구사항이 만족되어야 한다.

③ 정보보호 훈련이 모든 직원에게 적용되어야 한다.

④ 정보보호에 대한 위반은, 실제적이거나 의심스러운 경우 모두 정보보호최고책임자에게 보고되어야 하며, 정보보호최고책임자는 이를 면밀히 조사해야 한다.

⑤ 정보보호최고책임자는 정책의 유지관리 및 이행을 위한 제제 및 지침 제공의 직접적인 책임을 가진다.

⑥ 모든 관리자들은 그들의 업무 범주 내에서 지침의 이행에 대한 직접적인 책임을 가진다.

⑦ 이 방침을 지키는 것은 모든 임직원 각자의 책임이다.

제 2 장 정보보호 관리체계

제 5 조 (정보보호정책의 수립)

회사가 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립한다. 동 정책은 국가나 관련산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.

제 6 조 (범위설정)

회사에 미치는 영향을 고려하여 주요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호관리체계 범위를 설정한다. 범위 내 모든 자산을 식별하여 문서화하여야 한다.

제 7 조 (경영진의 책임과 역할)

회사가 수행하는 정보보호 활동 전반에 경영진이 참여하여 의사결정을 할 수 있도록 경영진의 책임과 역할을 다음과 같이 정의한다.

① 정보보호 관리체계의 구축 및 관리·운영

② 정보보호 취약점 분석·평가 및 개선

③ 침해사고의 예방 및 대응

④ 사전 정보보호대책 마련

⑤ 보안조치 설계·구현 등

⑥ 정보보호 보안성 검토

⑦ 중요 정보의 암호화 및 보안서버 적합성 검토

⑧ 그 밖에 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

제 8 조 (정보보호조직 구성)

최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호최고책임자, 실무조직 등 정보보호조직을 구성하여야 한다. 또한 정보보호 관리체계 운영 활동을 수행하는 데 필요한 자원(예산 및 인력)을 확보하여야 한다.

정보보호최고책임자는 최고경영자의 임무를 위임 받아 정보보호 관리체계가 지속적으로 운영이 가능하도록 한다.

제 9 조 (위험관리)

① 회사는 정보보호 전 영역에 대하여 다음과 같은 단계로 위험관리를 하여야 한다.

1. 위험관리 방법 및 계획 수립
2. 위험 식별 및 평가
3. 정보보호대책 선정 및 이행계획 수립

② 위험관리에 대한 세부사항은 '위험관리지침'을 따른다

제 10 조 (정보보호대책 구현)

정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.

구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.

제 11 조 (내부감사)

① 회사는 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 점검하기 위하여 연 1 회 이상 내부감사를 수행하여야 한다.

② 내부감사에 대한 세부사항은 '내부감사지침'을 따른다.

제 3 장 정보보호 정책

제 12 조 (정보보호정책의 승인 및 관리)

① 정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.

② 정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.

③ 정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하여야 한다.

④ 정보보호정책 승인 및 관리에 관한 세부 사항은 '정보보호관리지침'을 따른다.

제 13 조 (정보보호조직)

회사는 정보자산의 보호와 관리를 위하여 다음과 같은 조직을 구성한다.

① 정보보호최고책임자(CISO): 최고경영자가 임원급으로 지정하며 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리한다.

② 정보보호실무조직: 정보보호최고책임자의 역할을 지원하고 회사의 정보보호활동을 체계적으로 이행한다.

③ 정보보호위원회: 정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련 사항에 대한 검토 및 의사결정을 한다.

④ 정보보호 조직 구성에 관한 세부 사항은 '정보보호관리지침'을 따른다.

제 14 조 (외부자보안)

① 회사의 정보처리 업무를 제 3 자 또는 외부자(이하 "외부인력"이라 함)에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 외부 서비스를 이용할 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다. 명시된 외부인력의 보안요구사항의 이행여부는 주기적인 점검 또는 감사를 수행하여야 한다.

② 외부인력보안에 관한 세부사항은 '외부인력보안지침'을 따른다.

제 15 조 (정보자산분류)

① 회사의 정보자산 분류기준을 수립하고 모든 정보자산을 식별하고 목록으로 관리하여야 한다.

② 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 회사에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다.

③ 정보자산 관리에 관한 세부사항은 '정보자산관리지침'을 따른다.

제 16 조 (정보보호교육)

① 연간 정보보호교육 계획을 수립하여야 한다.

② 교육대상으로 정보보호 관리체계 범위 내 임직원 및 외부인력을 모두 포함하여야 한다.

③ 연 1 회 이상 전 임직원 및 외부인력을 대상으로 기본 정보보호 교육을 수행하여야 한다.

④ 정보보호 교육 실시에 관한 세부사항은 '정보보호관리지침'을 따른다.

제 17 조 (인적보안)

① 회사 내 중요 정보자산을 취급하는 임직원을 주요 직무자로 지정하고 관리하여야 한다.

② 정보보호 관련 주요 직무 분리 기준을 수립하고 적용하여야 한다.

③ 임직원으로부터 '정보보호서약서'를 받아야 하고 임시직원이나 외부인력에게 정보시스템에 대한 접근권한을 부여할 경우에도 정보보호서약서를 받아야 한다.

④ 인적 보안에 관한 세부사항은 '인적보안지침'을 따른다.

제 18 조 (물리적보안)

① 물리적 보호구역을 구분·지정하고 각 구역별 보호대책을 수립·이행하여야 한다.

② 보호구역별 내·외부인력 출입통제 및 보호구역 내 장비, 문서, 매체 등의 반출·입 통제를 마련하고 관리하여야 한다.

③ 사무실 내 개인업무 및 공용업무 환경보안을 위한 보호대책을 수립하여야 한다.

④ 물리적 보안에 관한 세부사항은 '물리적보안지침'을 따른다.

제 19 조 (시스템개발보안)

① 분석 및 설계 단계에서는 보안 요구사항 정의, 인증 및 암호화 기능, 보안로그 기능, 접근권한 기능 등이 반영 되어야 한다.

② 구현 및 이관 단계에서는 코딩 표준, 기술적 보안취약점 점검, 개발과 운영 환경 분리, 시험데이터 및 소스프로그램 보안 등이 고려되어야 한다.

③ 외주 개발 시 분석에서 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

④ 시스템 개발 보안에 관한 세부사항은 '응용프로그램보안지침'을 따른다.

제 20 조 (암호통제)

① 암호화 대상, 암호 강도(복잡도), 키 관리, 암호사용에 대한 정책을 수립하고 이행하여야 한다.

② 개인정보 저장 및 전송시 암호화 적용 등 암호화 관련 법적 요구사항을 반영하여야 한다.

③ 암호 키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하여야 한다.

④ 암호통제에 관한 세부사항은 '암호화지침'을 따른다.

제 21 조 (접근통제)

① 정보시스템 영역별(네트워크장비, 서버, 응용프로그램, DB, 정보보호시스템, 모바일기기, 인터넷 등)로 접근통제 규칙, 방법, 절차 등을 수립하여야 한다.

② 접근권한 관리를 위해서는 사용자 등록 및 권한부여, 관리자 및 특수 권한 관리, 접근권한 검토, 사용자 인증 및 식별, 사용자/이용자 패스워드 관리 등이 고려되어야 한다.

③ 접근통제에 관한 세부사항은 '네트워크보안지침', '서버보안지침', '데이터베이스보안지침', '정보보호시스템보안지침', '응용프로그램보안지침'을 따른다.

제 22 조 (운영보안)

① 운영 절차 및 변경 관리: 각종 정보시스템의 운영 및 변경을 위한 절차(또는 매뉴얼)를 수립하여야 한다. 운영 절차 및 변경관리에 관한 세부사항은 '네트워크보안지침', '서버보안지침', '데이터베이스보안지침', '정보보호시스템보안지침', '응용프로그램보안지침'을 따른다.

② 시스템 및 서비스 운영 보안: 정보시스템 인수, 보안시스템 운영, 성능 및 용량관

리, 장애관리, 원격운영관리, 스마트워크 보안, 무선네트워크 보안, 공개서버 보안, 백업관리, 취약점 점검 등을 고려하여야 한다. 시스템 및 서비스 운영보안에 관 한 세부사항은 '네트워크보안지침', '서버보안지침', '데이터베이스보안지침', '정보보 호시스템보안지침', '응용프로그램보안지침'을 따른다.

③ 정보 전송 보안: 업무상 조직 간에 중요정보(개인정보, 기밀정보 등)를 상호 교환 하는 경우 안전한 전송을 위한 협약 체결 등 보호대책을 수립·이행하여야 한다. 정보 전송 보안에 관한 세부사항은 '정보보호관리지침'을 따른다.

④ 매체보안: 정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 저장매체 처리 (폐기, 재사용)절차를 수립·이행하여야 하며, 휴대용 저장매체(외장하드, USB, CD 등)의 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하여야 한 다. 매체 보안에 관한 세부사항은 '정보보호관리지침'을 따른다.

⑤ 악성코드관리: 악성코드로부터 정보시스템을 보호하기 위하여 보호대책을 수립· 이행하여야 하며, 운영체계 및 소프트웨어 패치관리 정책 및 절차를 수립·이행하 여야 한다. 악성코드 관리에 관한 세부사항은 '서버보안지침', '물리적보안지침'을 따른다.

⑥ 로그관리 및 모니터링: 주요 정보시스템에 대한 로그관리 절차를 수립하고 이에 따라 로깅하여야 하며, 사용자 접속 기록 및 외부침해시도에 대한 검토(모니터링) 을 하여야 한다. 로그관리 및 모니터링에 관한 세부사항은 '네트워크보안지침', '서 버보안지침', '데이터베이스보안지침', '정보보호시스템보안지침', '응용프로그램보안 지침'을 따른다.

제 23 조 (침해사고관리)

① 침해사고 유형별 중요도 분류, 유형별 보고 대응, 복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.

② 침해사고 대응절차에 관한 세부사항은 '침해사고대응지침'을 따른다.

제 24 조 (IT 재해복구)

① IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직,

비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다.

② IT 재해복구 체계 구축에 관한 세부사항은 1 재해복구관리지침 1 을 따른다

부칙

제 1 조 (시행일)

본 규정은 최고경영자의 승인 시점일로부터 시행한다.

제 2 조 (준용)

회사의 정보보호 업무는 본 규정에 따라 수행하며, 이에 명시되지 않은 사항은 사규 및 관련 법령이 정하는 바에 따른다.

제 3 조 (예외적용)

다음 각 호에 해당하는 경우에는 본 규정에서 명시한 내용이라도 최고경영자의 승인을 받아 예외 취급할 수 있다.

① 기술 환경의 변화로 적용이 불가능할 경우

② 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급할 사유가 있을 경우

③ 기타 재해 등 불가항력적인 상황일 경우