정보보호 담당자	정보보호 책임자	최고 경영자

정보보호 정책서

문서번호 : SPC-PO-001
개정번호 : 1.1

문서번호 :SPC-PO-001	제 목	정보보호 정책서	문서등급	대외비
	버 전	Ver.1.1	제정일	2018. 03. 13

제·개정이력표

개정 번호	개 정 내 용 요 약	제·개정일자	주관부서	담당자	서명
1	제정	2018.03.13	총무팀	박상훈	
2	일부 개정 (제 3 조, 제 13 조 본문)	2023.3.14	인사총무팀	박상훈	

문서번호 :SPC-PO-001	제 목	정보보호 정책서	문서등급	대외비
	버 전	Ver.1.1	제정일	2018. 03. 13

목 차

제 1 장 총칙 1
제 1 조 (목적) 1
제 2 조 (범위) 1
제 3 조 (용어의 정의) 1
제 4 조 (책임사항) 3
제 2 장 정보보호관리체계 3
제 5 조 (정보보호정책의 수립) 3
제 6 조 (범위설정) 3
제 7 조 (경영진의 책임과 역할) 3
제 8 조 (정보보호조직구성) 4
제 9 조 (위험관리) 4
제 10 조 (정보보호대책구현) 4
제 11 조 (내부감사) 5
제 3 장 정보보호정책 5
제 12 조 (정보보호정책의 승인 및 관리) 5
제 13 조 (정보보호조직) 5
제 14 조 (외부자 보안) 6
제 15 조 (정보자산분류) 6
제 16 조 (정보보호교육) 6
제 17 조 (인적보안) 6
제 18 조 (물리적보안) 7
부칙 8
제 1 조 (시행일) 8
제 2 조 (준용) 8
제 3 조 (예외적용) 8

문서번호 :SPC-PO-001	제 목	정보보호 정책서	문서등급	대외비
	버 전	Ver.1.1	제정일	2018. 03. 13

정보보호 선언문(전문)

정보시스템과 정보는 에스피씨삼립(이하 “회사”라 함)의 주요한 자산이며, 이의 신뢰 있는 제공 없이는 직무를 효율적으로 수행하기 어렵다. 그러므로 회사의 경영진은 회사의 정보시스템과 정보를 보호· 향상시킬 의무가 있으며, 이는 정보시스템과 정보가 오류, 파괴, 테러, 개인정보 유출, 서비스 중단, 자연재해 등과 같은 여러 종류의 위협으로부터 보호되도록 적절한 조치를 반드시 취하여 한다는 것을 의미한다.

회사는 앞으로의 정보시스템 구축 및 향후 운영 또는 관리 시 예상되는 다양한 보안상의 문제들을 유념하고 이에 대비하여야 한다. 이는 회사의 정보시스템에 대한 해킹, 불법적인 정보유출 및 접근, 빠르고 광범위한 악성 컴퓨터 바이러스 감염, 그리고 그 외 각종 운영, 실행, 관리상의 문제들이 예상되기 때문이다. 따라서 이로 인한 중요 정보의 손실과 그에 따른 업무의 지연 및 저하, 그리고 그 외 이로 인한 각종 법적, 사회적, 윤리적인 여파를 철저히 고려하여 이에 따른 적절한 대비책을 마련해야 될 필요성이 날로 증대하고 있다.

그러므로 회사의 정보는 민감성, 가치, 심각도에 준하여 반드시 보호되어야 하며, 정보가 저장되는 매체, 처리되는 시스템, 전송수단에 모두 보안 대책이 적용되어야 한다. 이러한 보호는 직무 수행에 반드시 필요한 정보로의 접근만 허용하는 것을 포함한다. 관리자는 정보가 적절히 보호되기 위한 충분한 시간과 자원을 지원하여야 하며 정보시스템과 정보에 대한 보안 대책이 불충분하다고 판명될 경우에는 신속히 보완 대책을 강구·시행하여 정보의 노출을 최소화하여야 한다.

회사의 정보보호를 달성하기 위해서는 회사 구성원 모두의 참여와 협조가 요구되며 이를 뒷받침 할 충분한 교육과 참고자료가 제공되어야 한다. 회사의 정보시스템 보호를 수행하는데 필요한 지침과 절차서의 수립 및 제정을 포함한 모든 활동은 정보보호를 담당하는 부서를 중심으로 이루어져야 한다. 끝으로 정보시스템 보안 감사가 주기적으로 전사적으로 행하여져 정보보호가 제대로 이루어지는가를 확인하여야 한다.

2017 년 9 월

문서번호 :SPC-PO-001	제 목	정보보호 정책서	문서등급	대외비
	버 전	Ver.1.1	제정일	2018. 03. 13

정보보호 강령

정보통신 기술의 발달에 따라 새롭게 파생되고 있는 각종 위협들은 에스피씨삼립(이하 “회사”라 함)의 중요 자산인 정보시스템과 정보에 심각한 영향을 미칠 수 있게 되었으며 정보보호 활동은 전자상거래의 활성화 및 나아가서는 회사의 생존을 위해 필수 불가결한 요소가 되었다. 따라서 전 임직원은 다음에 제시하는 정보보호방침을 기초로 정보자산의 보호를 위해 최선을 다하여야 한다.

첫째, 임직원은 정보를 보호해야 할 중요한 자산으로 인식하고 취급해야 한다. 중요 정보 자산에 대한 접근 시 사용자 식별 및 인증 절차를 거쳐야 하고, 사용자는 불법적인 접근을 시도하거나, 패스워드 등을 다른 사람과 공유해서는 안되며, 부서장의 승인 없이 외부에 유출 또는 공개해서는 안 된다.

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 정보보호조직에 의해 일관성 있게 추진되어야 한다.

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

다섯째, 회사의 모든 정보자산은 인가된 인원에 한하여 접근 가능하도록 적절한 조치가 취해져야 하며 중요 정보자산을 운영·관리 하는 지역은 비인가자의 접근, 정전, 화재, 수해 등 각종 재난과 사고로부터 보호되어야 한다.

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

일곱째, 회사 정보시스템의 운영은 업무의 특성을 고려하여 적절히 분배되어야 하며 사전에 정의된 절차에 따라 수행되어야 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 관리되어야 한다.

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

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

전 임직원은 성공적인 정보보호가 세계적인 기업 경쟁력을 갖추기 위한 지름길임을 다시 한번 인식하고 정보보호를 위해 최선을 다해야 할 것이다.

문서번호 :SPC-PO-001	제 목	정보보호 정책서	문서등급	대외비
	버 전	Ver.1.1	제정일	2018. 03. 13

제 1 장 총칙

제 1 조 (목적)

본 정책은 에스피씨삼립(이하 “회사”라 함)의 자산에 대한 내·외부로부터의 훼손, 변조, 도난, 유출 등의 다양한 형태의 위협으로부터 효과적으로 보호하기 위한 정보보호 상위 정책과 임직원이 준수하여야 할 정보보호 규정을 정함을 목적으로 한다.

제 2 조 (범위)

본 정책은 회사에 근무하는 전 임직원을 대상으로 적용되며, 계약관계에 의하여 회사의 자산에 접근하는 모든 제3자에게도 적용된다.

제 3 조 (용어의 정의)

본 정책에서 사용하는 용어의 뜻은 다음과 같다.

① 개인정보 : 살아 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다. <신설 2023.3.14>

② 처리 : 정보(개인정보를 포함한다)의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다. <신설 2023.3.14>

③ 정보시스템 : 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

④ 임직원 : 회사 인사규정에 따라 채용되어 회사에 소속된 내부직원을 말한다. <신설 2023.3.14>

⑤ 제3자 : 방문객, 피교육자, 일용근로자와 같이 임직원이 아닌 외부인 또는 회사와 계약관계에 있는 타 회사(조직) 및 이에 속하는 직원을 말한다.

⑥ 정보보호 : 정보의 기밀성, 무결성, 가용성을 보장하기 위한 관리적, 기술적, 물리적 수단 또는 그러한 수단으로 이루어지는 행위를 말한다.

⑦ 정보보호책임자 : 관련 법령에서 정한 “정보보호최고책임자” 및 “개인정보보호책임자”

를 의미하며, 회사 보안부서(업무)를 총괄하며, 개인정보 관련 이용자의 고충처리를 담당하는 임원을 말한다.

⑧ 정보보호담당부서(자) : 정보보호계획 수립 및 실행, 보안사고 대응 등 회사 정보보호 체계를 수립하고 수행하는 부서 또는 임직원을 말한다. <개정 2023.3.14>

⑨ 개인정보 유출 : 개인정보의 분실·도난·유출(이하 유출 등이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우, 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우, 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우, 기타 권한이 없는 자에게 개인정보가 전달된 경우 그리고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다. <개정 2024.1.4>

⑩ 개인정보 노출 : 개인정보의 노출이란 공중이 해킹 등 특별한 방법을 사용하지 않고도 개인정보를 손쉽게 확인·조회하거나 취득할 수 있도록 개인정보가 공개 또는 방치되어 있는 상태를 말한다. <개정 2024.1.4>

⑪ 침해사고 : 권한이 없는 사용자가 비합법적인 방법으로 시스템에 접근하여 시스템의 서비스를 지연시키거나 시스템을 파괴, 데이터를 변조, 삭제하는 등의 행위를 통칭한다.

⑫ 위험관리 : 자산별 위험평가에 따라 파악된 위험을 관리하기 위한 방법을 말한다. 위험관리의 방법에는 회피, 전이, 감소, 수용하는 방법이 있다.

⑬ 정보자산 : 회사가 소유하고 있는 정보 및 정보시스템을 통칭하며, 서버시스템, 네트워크, 보안시스템, 응용시스템, 전자정보, 문서, 단말기, 소프트웨어, 물리적자산을 말한다.

⑭ 접근통제 : 정보시스템의 자원에 대한 접근을 제한하고 통제하는 프로세스로 비인가된 진입이나 사용으로부터 보호하기 위하여 설계된 논리적이거나 물리적인 통제를 말한다.

⑮ 정보보호관리체계 : 회사의 중요 정보자산(개인정보를 포함한다)를 보호하기 위하여 수립한 정보보호정책, 관리절차, 정보보호조직 및 관리적, 물리적, 기술적 통제수단 등의 보호체계와 정보보호 목표를 지속적으로 관리하고 운영하기 위한 종합적인 체계를 말한

다.

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 지침서의 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 정보보호책임자에게 보고되어야 하며, 정보보호책임자는 이를 면밀히 조사해야 한다.

⑤ 정보보호책임자는 정책의 유지관리 및 이행을 위한 충고 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 직원/고용인 각자의 책임이다.

제 2 장 정보보호관리체계

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 사전 보안성 검토

⑦ 중요 정보의 암호화 및 보안서버 적합성 검토

⑧ 그 밖에 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

제 8 조 (정보보호조직구성)

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

정보보호 최고책임자는 대표이사의 임무를 위임 받아 정보보호 관리체계가 지속적으로 운영이 가능하도록 한다.

제 9 조 (위험관리)

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

제 10 조 (정보보호대책구현)

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)

회사는 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사 기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다.

회사는 그 외에도 정보보호를 위하여 필요하다고 생각할 경우 정보보호실무조직의 장의 결정 하에 수시로 감사를 실시할 수 있다.

제 3 장 정보보호정책

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.

제 13 조 (정보보호조직)

회사는 정보자산의 보호와 관리를 위하여 다음과 같이 정보보호조직을 구성한다.

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

② 개인정보 보호책임자(CPO) : 개인정보를 처리하는 실무조직의 장으로 조직 내에서 개인정보 보호와 관련된 정보보호정책의 실행, 법적 의무사항 준수, 위험 관리 등을 총괄 관리한다. <신설 2023.3.14>

③ 정보보호 담당자 : 정보보호 최고책임자의 역할을 지원하고 회사의 정보보호활동을 체계적으로 이행할 정보기술부문과 정보보호부문 담당자(부서)로 구성한다.

④ 정보보호 실행조직 : 개인정보를 처리하는 실무조직으로 개인정보 보호와 관련된 정보보호정책과 절차, 지침의 시행, 법적 의무사항을 준수하고 개인정보 유출 또는 노출을 인지한 즉시 개인정보 보호책임자, 정보보호 최고책임자 및 정보보호 실무조직에 유출

사실, 시점, 원인, 규모 등을 신속하게 파악하여 보고한다. 개인정보 보호책임자의 지시에 따라 사고 대응팀에 참여하고 유출 경로 확인, 시스템 로그 분석 등 기술적 조사에 협조하며 유출된 정보의 삭제 또는 접근 차단 조치를 수행한다. <신설 2023. 3.14>

⑤ 정보보호위원회 : 정보보호 자원 할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 한다.

제 14 조 (외부자 보안)

회사의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 외부 서비스를 이용할 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다. 명시된 외부자의 보안요구사항의 이행여부는 주기적인 점검 또는 감사를 수행하여야 한다.

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.

제 16 조 (정보보호교육)

① 연간 정보보호교육 계획을 수립하여야 한다.

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

③ 연 1회 이상 임직원 및 외부자를 대상으로 기본 정보보호 교육을 수행하여야 하며, 만일 관련법령에서 이보다 엄격한 교육의무를 정한 경우 이에 따라 교육을 수행하여야 한다.

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 비밀유지서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.

제 18 조 (물리적보안)

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

② 보호구역별 내·외부자 출입통제 및 보호구역 내 장비, 문서, 매체등의반출입 통제를 마련하고 관리하여야 한다.

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

부칙

제 1 조 (시행일)

본 정책은 정보보호 최고책임자의 승인 시점일로부터 시행한다.

제 2 조 (준용)

회사의 정보보호 업무는 본 정책에 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 정보보호 최고책임자의 승인을 받아 예외 취급할 수 있다. 단 관련법령에 근거하여 반드시 준수해야 하는 규정은 그러하지 아니하다.

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