삼립

정보보호 및 개인정보보호 정책

1. 목적

㈜삼립(이하 "회사"라 한다)은 "개인정보보호법", "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 등 관련 법령을 준수하고, 회사가 보유한 정보자산 및 개인정보를 훼손·변조·도난·유출·오남용 등 제반 위협으로부터 효과적으로 보호하기 위하여 본 정책을 수립합니다. 본 정책은 회사의 정보보호 및 개인정보보호에 관한 최상위 정책으로서 전 임직원이 준수해야 할 기본 방침과 관리 원칙을 규정하는 것을 목적으로 합니다.

2. 적용 범위

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

3. 경영진의 책임과 역할

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

1) 정보보호 관리체계의 구축 및 운영

2) 정보보호 취약점 분석 평가 및 개선

3) 침해 사고의 예방 및 대응

4) 사전 정보보호대책 마련

5) 보안조치의 설계 및 구현

6) 정보보호 사전 보안성 검토

7) 중요 정보의 암호화 및 보안서버 적합성 검토

8) 그 밖에 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

4. 조직의 구성

대표이사는 조직의 규모, 업무 중요도 분석을 통해 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 조직을 구성하여야 합니다. 또한 관리체계 운영 활동을 수행하는 데 필요한 자원(예산 및 인력)을 확보하여야 합니다. 정보보호 최고책임자는 대표이사의 권한과 책임을 위임받아 관리체계가 지속적으로 운영될 수

있도록 합니다. 개인정보 보호책임자는 개인정보 보호계획의 수립·시행 및 그 결과를 대표이사, 정보보호 최고책임자 또는 이사회에 직접 보고할 수 있는 독립적인 보고 체계를 갖추어야 하며, 개인정보 처리와 관련된 정보에 대한 접근이 보장되어야 합니다.

5. 정보보호

1) 임직원은 정보를 보호해야 할 중요한 자산으로 인식하고 취급해야 합니다. 중요 정보자산에 대한 접근 시 사용자 식별 및 인증 절차를 거쳐야 하고, 사용자는 불법적인 접근을 시도하거나, 패스워드 등을 다른 사람과 공유해서는 안 되며, 부서장의 승인 없이 외부에 유출 또는 공개해서는 안 됩니다.

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

3) 정보보호와 관련된 모든 방침 및 지침은 자산에 대한 기밀성·무결성·가용성을 확보할 수 있도록 수립, 검토, 시행되어야 하며, 이러한 일련의 활동들은 정보보호조직(정보보호 최고책임자, 개인정보 보호책임자, 정보보호 담당자, 정보보호 실행조직을 말하며, 이하 같다)에 의해 일관성 있게 추진되어야 합니다.

4) 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 합니다.

5) 회사의 모든 정보자산은 인가된 인원에 한하여 접근할 수 있도록 적절한 조치가 취해져야 하며 중요 정보자산을 운영·관리하는 지역은 비인가자의 접근, 정전, 화재, 수해 등 각종 재난과 사고로부터 보호되어야 합니다.

6) 회사의 정보자산이 침해사고 및 내·외부자의 고의적이거나 우발적인 침입에 의해 손상을 입었을 경우에도 회사는 사업을 지속할 수 있어야 하며 신속히 정보자산을 복구하여 피해를 최소화하도록 침해사고 대응계획을 수립하고 관리하여야 합니다.

7) 회사 정보시스템의 운영은 업무의 특성을 고려하여 적절히 분배되어야 하며 사전에 정의된 절차에 따라 수행되어야 합니다. 또한 정보시스템 운영에 관한 기록을 유지·관리함으로써 향후 정보시스템의 운영 계획의 수립 및 침해사고 발생 시 그 기록이 반영되도록 하여야 합니다. 이는 정보자산의 관리 책임이 각 사용자에게 있음을 의미하며, 중요 정보자산에 대해서는 작성자, 작성일자, 사용자가 명확히 지정되어야 하고, 사용

시에는 사용 이력의 추적이 가능하도록 관리되어야 합니다.

8) 정보통신망법 제48조의3 및 같은 법 시행령 제58조의2 제1항에 따라 정보통신망법이 규정하는 침해사고 발생 시, 정보통신서비스 제공자는 침해사고의 발생을 알게된 때로부터 24시간 이내에 과학기술정보통신부장관이나 한국인터넷진흥원에 신고할 의무가 있습니다.

6. 개인정보보호

1) 모든 임직원이 본 정책의 내용을 숙지하여 생활화하기 위해서 적절한 교육이 시행되어야 하며, 정보보호조직은 이에 대한 책임이 있습니다.

2) "개인정보보호법", 동법 시행령·시행규칙 및 관련 법령, 감독기관의 요구사항을 준수하여야 합니다.

3) 모든 임직원에게 관련 정보보호 정책 및 지침을 배포하거나 내부 정보통신망에 게시하고 관련 교육을 실시합니다.

4) 개인정보보호 훈련은 모든 임직원에게 적용되어야 합니다.

5) 개인정보보호 위반이 발생하였거나 그 위반이 의심되는 경우에는 모두 개인정보 보호책임자에게 보고되어야 하며, 개인정보 보호책임자는 이를 면밀히 조사해야 합니다.

6) 개인정보 보호책임자는 정책 및 지침의 유지관리 및 이행을 위한 자문 및 지침 제공에 대한 직접적인 책임을 갖습니다.

7) 개인정보 보호책임자 및 개인정보취급자는 "개인정보보호법" 제31조 및 제28조에서 정하는 각자의 업무 범위 내에서 본 정책의 이행에 대한 직접적인 책임을 갖습니다.

8) 개인정보 보호책임자 주재 회의 시 개인정보보호 관련 사항이 논의되어야 합니다.

9) 개인정보 보호책임자는 정보보안 교육 실시, 불시점검 등 정보보안 강화에 필요한 사항을 지시합니다.

10) 모든 임직원들은 본 정책 및 개인정보 및 정보보호와 관련한 법령을 준수할 책임을 부담합니다.

11) 개인정보가 분실·도난·유출된 사실을 알게 된 경우, 회사는 지체 없이(72시간 이내) 해당 정보주체에게 유출 사실, 유출 항목, 유출 시점 및 경위, 피해 최소화 방법 등을 통지하여야 합니다. 또한 일정 규모 이상의 유출이 발생한 경우에는 "개인정보보호법" 제32조 및 동법 시행령 제40조에 따라 개인정보보호위원회 또는 한국인터넷진흥원에 72시간 이내에 신고하여야 합니다.

7. 부칙

제 1 조 (시행일)
본 정책은 정보보호 최고책임자 및 개인정보 보호책임자의 승인 시점일로부터 시행합니다.

제 2 조 (준용)
회사의 정보보호 업무는 본 정책에 따라 수행하며, 이에 명시되지 않은 사항은 사규 및 관련 법령이 정하는 바에 따릅니다.

제 3 조 (예외 적용)
다음 각 호에 해당하는 경우에는 본 규정에서 명시한 내용이라도 정보보호 최고책임자 및 개인정보 보호책임자의 승인을 받아 예외 취급할 수 있습니다. 다만, 관련법령에 따라 반드시 준수하여야 하는 사항은 예외로 적용할 수 없습니다.
① 기술 환경의 변화로 적용이 불가능할 경우
② 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우
③ 기타 재해 등 불가항력적인 상황일 경우