

제 1 장. 총칙

제 1 조 (목적)

본 정책은 현대하이텍·글로벌하이텍전자(이하 '회사'라 한다)의 정보보호 활동을 위해 필요한 사항을 규정하 여 회사의 정보자산을 보호함을 목적으로 하며, 모든 구성원은 본 정보보호 정책을 준수하여야 한다.

제 2 조 (적용범위)

본 정책은 회사에 근무하는 전 구성원과 외부인력, 출입자 등을 대상으로 적용되며, 본 정책에서 정한 범위 내에서 직·간접적인 관계에 있는 회사 및 계약관계에 있는 모든 인력에게 적용된다. 또 한, 정보보호의 적용범위는 회사의 정보자산으로 한다.

제 3 조 (정의)

- ① "정보"란 재무정보, 경영정보, 개인정보, 영업정보, 기술정보 등 회사와 관련된 모든 정보를 말한다.
- ② "정보자산"이란 제1호에서 정의한 "정보"의 가치를 지닌 자료, 문서, 소프트웨어, 하드웨어 및 "정보" 그 자체를 나타내는 유·무형의 모든 자산을 말한다.
- ③ "정보보호"란 정보의 수집, 가공, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하고 수행하는 것을 말한다.
- ④ "정보보호 최고책임자"란 회사의 정보보호를 위한 관리적·기술적 수단의 마련 및 활동 수행을 총괄 관리할 수 있는 임원을 말한다.
- ⑤ "개인정보"란 주민등록번호 등 특정 개인을 식별할 수 있는 정보와 서비스이용 기록, 구매 내역 등 서비스를 이용하는 과정에서 생성되는 정보, 그리고 다른 정보와 용이하게 결합하여 개인 식별이 가능한 정보 등 특정 개인과 관련된 모든 정보를 말한다.
- ⑥ "개인정보 보호책임자"란 회사 내에서 개인정보를 취급하는 특정 사업을 주관하는 임원이나 개인정보와 관련된 이용자의 고충처리를 담당하는 부서의 장을 말한다.
- ⑦ "개인정보 취급자"란 개인정보처리시스템의 접근/접속 권한을 보유하고 있거나, 업무상 또는 서비스 제공을 위해 개인정보를 취급(수집, 보관, 이용, 처리, 제공, 관리, 파기 등)하는 회사 및 외부업체 직원을 말한다.
- ⑧ "패스워드"란 이용자 및 개인정보 취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
- ⑨ "보조저장매체"란 외장HDD, USB메모리, 플래쉬메모리, CD/DVD, PMP, MP3 등 휴대가 용이

하고 정보의 저장이 가능한 모든 매체를 말한다.

- ⑩ "외부업체"란 회사와 계약을 통해 업무의 일부를 위탁 받거나 회사에 용역을 제공하는 법인으로서, 업무상 회사 정보시스템에 접속하거나 회사의 정보 및 개인정보 취급하는 법인을 말한다.
- ⑪ "외부인력"이란 회사와 계약 또는 제휴를 맺은 외부업체 소속 직원과 외부업체와 계약에 의해 위탁 또는 제휴 업무를 수행하는 모든 인력을 말한다.
- ⑫ "정보시스템"이란 정보를 처리, 저장, 전달할 목적으로 회사가 사용 또는 관리하는 모든 PC, 서버, 네트워크, 보안장비 등 하드웨어와 그 하드웨어에 포함된 데이터베이스, 어플리케이션 등 소프트웨어를 말한다.
- ⑬ "침해사고"란 회사가 제공하는 모든 서비스가 해킹 또는 악성코드 등에 의해 지연·파괴되거나, 회사의 기업비밀 및 개인정보가 무단 노출/유출되는 것을 말한다.
- ⑭ "업무용 PC"란 원활한 업무 수행을 위해 회사가 임직원에게 지급한 PC를 말한다.

제 4 조 (정보보호 정책의 수립 및 운용)

- ① 정보보호 최고책임자는 회사의 보안을 위한 전반적인 사항을 포함하여 보안관리 정책을 수립, 관리하며, 정책 수립 시 관련 부서 및 이해관계자들에게 배포하여야 한다.
- ② 정보보호 최고책임자는 보안관리 정책 수립 시 국내·외 유관 법령을 토대로 업무 환경에 부합하는 보안관리 정책을 수립·운영해야 하며, 실무에 적용 가능하도록 절차 등을 마련해야 한다.
- ③ 보안관리 정책의 효율적인 업무 적용을 위하여 관련 분야별 세부 지침을 수립할 수 있다.
- ④ 정보보호 최고책임자는 보안관리 정책에서 요구하는 정보보호 수준유지를 위해 연간 정보보호 업무계획을 수립·시행하고 그 추진 결과를 심사·분석·평가하여 최신의 상태가 유지되도록 관리하여야 한다.
- ⑤ 정보보호 최고책임자는 정보보호정책, 정보보호 관련 지침의 타당성을 주기적으로 검토하도록 관리 감독하여야 한다.
- ⑥ 보안관리 정책 및 세부 지침은 제·개정 시 공식 정책으로써 대표이사과 정보보호 최고책임자의 승인을 득한 후 공표하며, 공표한 날로부터 시행한다.
- ⑦ 개정 및 승인된 보안관리 정책은 구성원이 언제든지 열람할 수 있는 방법으로 공표 및 게시하여야 한다.

제 2 장. 정보보호 조직의 운영

회사는 정보보호 조직을 구성하고 정보보호 활동의 기반을 마련하는 것에 그 목적이 있다.

제 5 조 (정보보호 조직 구성 기준)

- ① 정보보호 활동의 계획, 관리 및 이행을 위한 정보보호 조직을 구성 및 운영하며, 각 구성원의 책임과 역할을 명문화하여 원활한 정보보호 업무 운영 및 추진이 가능하도록 해야 한다.
- ② 회사의 정보보호 및 개인정보 조직은 다음과 같이 구성한다.
 1. [정보보호 조직]
 - 정보보호 최고책임자
 - 정보보호 관리자
 - 정보보호 담당자
 2. [개인정보 조직]
 - 개인정보 보호책임자
 - 개인정보 보호관리자
 - 개인정보 보호담당자
- ③ 회사의 정보보호 조직은 인사발령에 의하며, 각 구성원의 책임과 역할은 직무기술서를 통해 명문화하여야 한다.

제 6 조 (정보보호위원회 운영)

- ① 회사의 전반에 걸친 중요한 정보보호 관련사항에 대해 검토 및 의사결정을 할 수 있는 정보보호위원회를 구성하여야 한다.
- ② 정보보호위원회의 위원은 정보보호 최고책임자로 하며, 관련사업 부문, 본부의 간부급으로 구성한다.
- ③ 정보보호위원회는 조직 전체의 정보보호 목표, 목적 및 우선순위 등을 고려하여, 연 1회 이상 회사의 정보보호 주요 현안을 검토하고 이에 대한 의사결정을 수행한다.

제 3 장. 인력 보안 관리

회사의 임직원 및 계약직원(계약직, 임시직, 아르바이트 등)이 입·퇴사 및 직무 이동 등을 통해 발생 가능한 정보의 유출, 변조, 오·남용, 삭제 등 각종 보안 위험을 최소화하는데 그 목적이 있다.

제 7 조 (구성원 정보보호 서약 및 갱신)

- ① 구성원은 입사 및 퇴사 시 회사의 정보보호 정책을 이해하고, 이를 준수하겠다는 내용의 동의 및 서약을 징구 하며, 별도의 기준을 마련하여 주기적으로 갱신하여야 한다.
- ② 정보보호 서약서에는 다음의 내용이 포함되어야 한다.
 1. 회사 정보보호 정책의 준수
 2. 영업비밀 및 개인정보보호법에 준하는 개인정보의 보호
 3. 기타 회사와 관련된 법규 및 요건에 대한 준수
 4. 정보보호 관련 법령에 대한 준수
 5. 위반시의 책임 감수
- ③ 신규로 입사하는 모든 구성원은 본 정책을 숙지하고, 정보보호 서약서를 작성하여 제출한다.
- ④ 신규 입사자에 대하여 회사의 정보보호 정책 및 하위 지침에 대한 교육을 실시한다. 단, 전사적으로 입사자 교육을 실시한 경우에는 예외로 한다.
- ⑤ 구성원의 퇴사 시 정보보호 서약서를 징구하고, 보유중인 회사의 모든 정보자산 및 정보 시스템 사용권한, 사원증 등을 회수하여 개인 물품 이외의 반출이 불가하도록 하여야 한다.

제 8 조 (구성원 정보보호 교육)

- ① 정보보호 교육은 교육대상, 교육자원(인력, 예산 등, 교육방법 및 주기) 등을 고려하여 계획하여야 한다.
- ② 신규 입사자에 대해 부서 배치 전 회사의 정보보호 정책 및 업무상 필요한 정보보호 활동을 주지시키기 위해 정보보호 교육을 실시할 수 있다.
- ③ 회사의 구성원 등을 대상으로 정보보호 정책 및 업무 상 필요한 정보보호 활동을 교육하고 홍보함으로써, 구성원의 정보보호 인식을 제고하는데 그 목적이 있다.
- ④ 정보보호 주관부서는 교육 대상, 교육방법 및 내용, 교육 일정, 횟수 등을 포함하여 연간 정보보호 교육 및 훈련 계획을 수립하여야 한다.
- ⑤ 정보보호 교육 및 훈련은 전 구성원을 대상으로 연 1회 이상 정기적으로 실시하여야 한다.
- ⑥ 개인정보 취급자(외부인력 포함)에 대해서는 연 1회 이상 정기적으로 교육을 실시하여야 한다.
- ⑦ 정보보호 교육은 구성원 등이 회사의 정보보호 활동을 이해하고 수행할 수 있도록 업무 및 수준 등을 고려하여 이행하여야 한다.
- ⑧ 정보보호 교육을 수행하는데 있어 내부 교육, 외부 위탁교육 등 다양한 방법을 활용할 수

있다.

- ⑨ 정보보호 교육 이행 후 평가를 실시하여 교육의 효과 및 문제점을 분석하고, 추후 정보보호 교육 계획에 반영해야 한다.

제 4 장. 외부인력 보안 관리

회사의 정보자산을 관리, 운영, 활용하는 구성원 이외의 외부인력(용역직원, 위탁 업무직원, 협력 업체 직원 등) 및 계약 업체를 대상으로 회사의 정보자산 보호에 관한 의무와 책임을 명확히 하는데 그 목적이 있다.

제 9 조 (외부인력 계약 시 보안 요구사항)

- ① 외부인력 또는 외부업체와 계약을 할 경우, 비밀유지, 정보보호 준수 의무, 정보보호 문제 발생 시의 손해배상 책임 등 정보보호 요건을 정의하여 계약서 상에 반드시 반영해야 하며, 필요 시 별도의 정보보호 약정서를 징구 할 수 있다.
- ② 계약서 및 정보보호 약정서에 명시된 보안 요구사항의 이행여부를 관리·감독하여야 한다.

제 10 조 (외부인력 업무 수행 시 보안 요구사항)

- ① 외부인력의 업무 수행 시 회사의 보안 정책 및 업무상 필요한 정보보호 활동에 대해 교육 후 보안 정책의 준수와 비밀유지에 대한 정보보호 서약서를 징구 하여야 한다.
- ② 외부인력의 보안 요구사항 이행 점검 시 발견된 결함은 조치 계획을 수립하여 반영하고, 유사한 문제가 재발하지 않도록 추가적인 보호 대책을 수립·이행하여야 한다.
- ③ 외부인력의 보안 관리 정책 위반 시 그 결과를 해당 업체에 경고 조치하고, 계약에 따른 해지, 손해배상 등의 필요 조치를 수행하여야 한다.

제 11 조 (외부인력 계약 종료 시 보안 요구사항)

외부인력의 계약 종료 시 정보보호 약정서를 징구 하며 보유 중인 회사의 모든 정보 자산 및 정보 시스템 사용 권한, 출입 권한 등을 회수 및 파기하여 개인 물품 이외의 반출이 불가하도록 하여야 한다.

제 5 장. 정보자산의 보안 관리

회사의 정보자산에 대해 식별 및 분류 기준을 정의하고, 정보자산의 훼손, 변조, 도난, 유출

등 다양한 형태의 위험을 관리하기 위한 기준을 정립하는데 그 목적이 있다.

제 12 조 (정보자산 등급 분류 및 관리)

- ① 회사의 정보자산에 대한 중요도를 평가하여 보안 등급 별로 분류기준을 수립하고 정기적으로 적정성을 검토하여야 한다.
- ② 정보자산은 보안 등급에 따라 취급절차(생성, 저장, 이용, 파기 등)수립 및 사용자를 지정하고 비 인가자의 접근을 차단하여야 한다.
- ③ 중요 정보자산에 대해서는 주기적으로 보안 점검 및 분석을 수행하고 발견된 취약점에 대해서는 보호 대책을 수립하여야 한다.
- ④ 중요 데이터 및 문서 등의 폐기 시에는 해당 내용을 복구할 수 없도록 파기 또는 완전 삭제 등을 시행하여야 한다.

제 13 조 (정보자산의 위험관리)

- ① 정보자산의 중요도, 취약 정도, 위협 정도를 기반으로 위험도를 평가하고 위험 관리 계획을 수립하여 관리하여야 한다.
- ② 위험 관리 계획에 따른 보호 대책을 수립할 경우에는 긴급성(위험 수준), 소요되는 자원(예산, 인력), 구현 가능성(기대 효과) 등을 고려하여 우선순위를 결정한다.

제 6 장. 개인정보보호

회사에서 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등을 방지하는데 그 목적이 있다.

제 14 조 (내부관리 계획의 수립 및 공표)

- ① 개인정보 보호와 관련한 법령 및 정책 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부관리 계획을 수립하고 관련 법령의 제·개정 사항 등을 반영하기 위하여 연 1회 이상 내부관리 지침의 타당성과 개정 필요성을 검토하여야 개정하여야 한다.
- ② 개인정보 보호책임자는 연 1회 이상으로 내부관리 지침의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.
- ③ 개인정보 보호책임자는 승인된 개인정보 내부관리 지침을 모든 구성원 및 관련자에게 알림으로써 이를 준수하도록 하고 구성원이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제 15 조 (개인정보 보호조직 역할 및 책임)

- ① 회사는 개인정보 보호책임자를 지정하고, 다음의 업무를 총괄하여 지휘·감독한다.
 1. 개인정보 보호 내부관리 지침의 수립 및 시행
 2. 개인정보 처리실태 및 관행의 정기적인 조사 및 개선
 3. 개인정보 처리와 관련한 불만의 처리 및 피해구제
 4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
 5. 개인정보 보호 교육 계획의 수립 및 시행
 6. 개인정보 파일의 보호 및 관리감독 실태 점검
 7. 개인정보 보호법에 따른 개인정보 처리방침의 수립·변경 및 시행
 8. 개인정보 보호 관련 규정 및 자료의 관리
 9. 처리 목적이 달성되거나 보유기간이 만료된 개인정보의 파기
 10. 기타 개인정보보호 법령상 규정하는 업무
- ② 개인정보 보호관리자는 회사의 개인정보 주관부서의 관리자로서 개인정보보호 관련 각종 계획 수립 및 개인정보보호 업무에 대한 조정, 통제, 필요한 업무를 관리·감독하며, 개인정보 보호책임자를 보좌하여 개인정보보호 관련 업무를 수행한다.
- ③ 개인정보 보호담당자는 개인정보보호 조직 구성원이며 회사 내 개인정보보호 계획에 따른 활동을 수행하여야 한다.
- ④ 개인정보 취급자는 개인정보를 처리하는 업무를 담당하는 자(구성원, 파견근로자, 시간제 근로자 포함)로 개인정보를 처리함에 있어 동 계획은 물론, 개인정보 보호와 관련한 법령 및 정책 등을 준수하여야 한다.

제 16 조 (개인정보보호 교육)

회사는 개인정보의 적절한 취급을 보장하기 위하여 연 1회 이상 개인정보 보호책임자 및 취급자를 대상으로 개인정보보호 교육 계획을 수립하고 실시하여야 한다.

제 17 조 (개인정보의 생명주기 및 권리보장)

- ① 회사는 개인정보의 수집, 이용, 저장, 제공, 파기의 생명주기에 따라 적절한 보호조치를 하고, 정보주체의 권리보장을 위한 방법을 제공하여야 한다.
- ② 개인정보는 동의 받은 이용 목적 내에서만 이용하여야 한다.

제 18 조 (개인정보의 기술적·관리적·물리적 보호조치)

- ① 회사는 개인정보처리시스템에 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당

자에게 차등 부여하며, 내·외부자의 불법적인 접근 및 정보보안사고 방지를 위해 고유식별 정보, 비밀번호 등 암호화, 접근통제, 악성프로그램 등 방지를 위한 보호조치를 하여야 한다.

- ② 회사는 개인정보의 안전한 처리를 위하여 개인정보 보호책임자 지정, 개인정보 유출사고 대응체계 수립, 개인정보의 위험도 분석 및 대응, 개인정보의 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독 등의 보호조치를 하여야 한다.
- ③ 회사는 전산실, 자료보관실, 문서고 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우 출입통제 절차 수립·운영 등 보호조치를 하여야 한다.

제 7 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 있다.

제 19 조 (정보기기 보안 관리)

- ① 회사에서 지급한 업무용 PC는 회사의 보안정책을 준수하여 사용 및 관리하여야 한다.
- ② 업무용 PC는 본래 사용 목적 외의 용도로 사용하지 않아야 하며, 업무용 PC의 관리 부주의에 따른 보안 사고가 발생하지 않도록 보호 대책을 수립하여 관리하여야 한다.
- ③ 업무용으로 개인 보조저장매체를 사용하지 않아야 하며, 부득이하게 사용해야 할 경우 사용허가 및 등록 절차에 의해 허가된 매체만 사용할 수 있도록 한다.
- ④ 보조저장매체의 반출·입 절차를 수립하여 보조저장매체의 보유현황을 파악해야 한다.
- ⑤ 보조저장매체의 폐기 및 재사용, 분실 등으로 인한 정보유출에 대하여 대책을 마련하여야 한다.

제 8 장. 정보시스템 보안 관리

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

제 20 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 부여 받도록 함으로써 인가되지

많은 사용자의 접근 및 정보의 사용을 통제 하는데 그 목적이 있다.

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

제 21 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 한다.
- ② 주요 정보시스템의 권한 부여 시 취급 정보, 사용자, 직무에 따른 역할을 기반으로 최소한의 권한만을 부여해야 하며, 정기적으로 검토를 수행하여야 한다.
- ③ 1인 1계정 사용을 원칙으로 하고, 공용계정 사용을 금지한다. 다만 내부 사정 등으로 인하여 공용 계정의 사용이 불가피한 경우 정보시스템 관리자의 승인을 받아야 하며, 승인받은 목적 내에서만 제한적으로 사용할 수 있다.

제 22 조 (패스워드 관리)

패스워드는 대문자, 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 사용하며, 타인에게 노출되지 않도록 관리하여야 한다.

제 23 조 (서버 보안 관리)

- ① 서버를 도입할 경우에는 보안성에 대한 검토를 실시하여야 하고, 적절한 보안설정을 적용하여야 한다.
- ② 서버의 보안성 확보를 위해 OS 및 소프트웨어의 주요한 패치를 지속적으로 적용한다. 패치는 반드시 사전 테스트를 통해 보안패치의 안전성을 검증 후 적용하여야 한다.
- ③ 그 밖에 서버의 보안 관리를 위한 세부적인 사항은 『서버보안 지침』에서 정한 바에 따른다.

제 24 조 (네트워크 보안 관리)

- ① 업무의 특성 및 중요도에 따라 네트워크 영역을 분리하고, 분리된 네트워크 영역 간에는 접근통제를 수행하여야 한다.
- ② 네트워크 이용에 대한 접근 규칙 및 보안성 검토 등을 통한 점검 및 보호대책을 수립하고 적용해야 한다.
- ③ 정보시스템 관리자의 승인 없이 무선 AP(Access Point) 장비를 내부 네트워크에 연결하여

무선 네트워크를 구축을 금지한다.

- ④ 그 밖에 네트워크 보안 관리를 위한 세부적인 사항은 『네트워크 보안 지침』에서 정한 바에 따른다.

제 25 조 (데이터베이스 보안 관리)

- ① 데이터베이스는 무결성 확보를 위하여 사용자가 직접 접근할 수 없도록 통제하여야 한다.
- ② 데이터베이스의 접근권한은 사용자의 직무별로 구분하여 부여하고, 특정 명령(Update, Delete 등)은 권한이 부여된 자만이 사용 가능 하도록 통제하여야 한다.
- ③ 그 밖에 데이터베이스 보안 관리를 위한 세부적인 사항은 『데이터베이스 보안 지침』에서 정한 바에 따른다.

제 26 조 (정보보호시스템 보안 관리)

- ① 네트워크를 통한 침입을 방지하기 위한 기술적 수단으로써 방화벽, 침입차단시스템, 가상 사설망 등의 정보보호시스템을 설치·운영하여야 한다.
- ② 정보보호시스템의 보안정책이 변경되어야 하는 경우 반드시 정보시스템 관리자의 승인을 득한 후 수행해야 하며, 관련 내역을 반드시 기록·관리하여야 한다.
- ③ 그 밖에 정보보호시스템 보안 관리를 위한 세부적인 사항은 『정보보호시스템 보안 지침』에서 정한 바에 따른다.

제 9 장. 응용프로그램 보안 관리

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

제 27 조 (응용프로그램 보안 관리)

- ① 응용프로그램 신규 개발 및 변경 시 다음 각 호와 같은 보안 통제 요구사항을 명확히 정의하여야 한다.
 - 1. 사용자 인증
 - 2. 접근권한 및 통제
 - 3. 입력 데이터 검증, 내부처리, 출력 데이터 검증
 - 4. 로그관리
 - 5. 암호화

6. 기타 개발, 운영 시 정보보호 통제

- ② 개발 프로젝트 수행 시 응용프로그램의 보안성 확보를 위해 분석, 설계, 개발, 테스트, 운영이관 등 진행 단계별로 보안성 적용을 수행하고 완료이전에 프로젝트 보안성 검토를 마쳐야 한다.

제 28 조 (응용프로그램 개발 보안 관리)

- ① 시스템 개발 및 테스트 환경은 운영 환경과 분리하는 것을 원칙으로 하여야 한다.
- ② 운영 응용프로그램의 주요 변경을 통제하기 위한 절차를 수립하고, 변경내역은 사고 및 장애 발생 시 원인 규명을 위해 기록, 관리하여야 한다.
- ③ 응용프로그램 테스트 시 운영 데이터의 유·노출을 방지하기 위해 임의의 테스트 데이터를 생성하여 활용하거나 운영 데이터를 가공하여 사용하도록 하며 실제 운영 데이터의 사용을 금한다.
- ④ 응용프로그램을 운영 단계로 이관 시, 다음 각 호의 보안 사항을 준수하여야 한다.
 - 1. 개발자 이외의 이관 담당자 지정
 - 2. 테스트 후 이관
 - 3. 보안 점검 후 이관
 - 4. 이관 시 문제에 대한 대응방안 마련
- ⑤ 그 밖에 응용프로그램 보안 관리를 위한 세부적인 사항은 『응용프로그램 보안 지침』에서 정한 바에 따른다.

제 10 장. 물리 보안 관리

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

제 29 조 (보호구역 지정 및 통제)

사업장 외곽 및 진입 통로를 비롯하여 각 부서가 입주하고 있는 건물 및 시설에 대해 보호구역을 지정하여 인가되지 않은 직원의 출입을 엄격히 통제하여야 한다.

제 30 조 (보호구역 분류 기준)

- ① 보호해야 할 필요가 있는 곳을 보호구역으로 선정하고 일반구역, 제한구역, 통제구역으로 구분하여 운영하여야 한다.

- ② 일반구역은 중요자산이 보관되지 않아 외부인의 출입이 허용되는 구역으로서 접견실, 안내실 등을 말한다.
- ③ 제한구역은 일부 중요자산이 보관되어 있는 장소로서 외부인력의 출입이 제한적으로 허용되는 구역으로서 사무실, 회의실, 문서고, 상황실 등을 말한다.
- ④ 통제구역은 외부인력의 출입이 엄격히 금지되고, 임직원은 업무적 필요에 따라 최소한의 인원만이 출입이 가능한 구역이다. 전산실, NW장비실, 서버실 등이 통제구역에 해당한다.

제 31 조 (보호구역 출입 및 감시)

- ① 물리보안 관리자는 보호구역에 대한 임직원 및 외부인력의 출입내역을 기록·보관하고, 주요 제한구역 및 통제구역의 출입기록에 대해서는 주기적으로 적정성을 검토하여야 한다.
- ② 통제구역 내에 정보자산의 불법 유출을 방지하기 위해 자산의 반출·입 시에는 정보시스템 관리자의 승인을 득하도록 통제 절차를 수립하여야 한다.

제 32 조 (시설 보호)

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

제 11 장. 정보보안 점검 및 감사

회사의 정보보호 점검, 취약점 점검, 물리 보안 등 보안관리 규정에서 정의하는 관리 대상에 대한 정보보호 이행 점검의 세부 사항을 정하는데 그 목적이 있다.

제 33 조 (정보보안 점검 영역)

정보보안 점검은 다음 각 호에 대한 이행 여부를 점검한다.

- 1. 정보보호 관리체계 자체 점검
- 2. 정보보호의 날 운영
- 3. 생활보안 및 퇴직자 보안점검
- 4. 정보시스템 취약점 점검
- 5. 기타 정보보호 및 개인정보보호 컴플라이언스 준수 여부 등

제 34 조 (정보보안 감사 수행 및 사후 관리)

- ① 정보보안 감사는 연 1회 이상 전사적으로 실시하여야 하며, 인력/비용/기타 현실적인 제약

으로 인하여 전사적 감사가 불가능한 경우에는 사전에 대상을 선정하여 제한적으로 실시할 수 있다.

- ② 보안감사는 객관성 확보를 위해 제3자 수행을 원칙으로 하며 전문적인 감사를 위하여 외부전문가를 보안감사 수행조직에 포함시킬 수 있다.
- ③ 정보보안 감사 결과 도출된 지적 사항에 대해 시정 및 조치 여부를 점검하고 향후 보안감사 계획에 반영한다.

제 12 장. 암호 관리

회사의 데이터 보호 및 암호화 관리에 필요한 사항을 규정하는데 그 목적이 있다.

제 35 조 (암호화)

- ① 회사가 처리하는 개인정보를 보호하기 위하여 암호화 적용 기준을 수립하여야 한다.
- ② 암호화 적용 기준에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반영하여야 한다.

제 36 조 (암호키 관리)

- ① 암호키를 사용할 경우 생성에서 파기까지의 관리절차를 수립하여야 한다.
- ② 중요 정보를 취급(생성, 저장, 전송 등)하는 어플리케이션의 경우 중요 정보에 대한 암호화를 적용하여야 하며, 암호화 키 관리 등에 대한 담당자를 지정 및 관리 대책을 수립하여야 한다.

제 13 장. 침해사고 대응

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

제 37 조 (침해사고 대응 계획)

- ① 회사는 침해사고에 대한 신속하고 체계적인 대응을 위해 침해사고대응체계를 마련하여야 한다.
- ② 침해사고를 예방하기 위해 사전 모니터링 및 탐지·대응 체계를 구축하여 운영하고, 불법적인 정보유출과 보안 침해 시도에 대응하여야 한다.

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

제 38 조 (침해사고 대응 절차)

- ① 침해사고는 다음과 같이 4가지 유형으로 구분하며, 각각의 대응 절차에 따라 대응 조직을 구성하고 사고 대응 및 복구를 수행한다.
 - 1. 서비스(시스템) 중단
 - 2. 서비스(시스템) 변조 및 수정
 - 3. 악성코드 감염
 - 4. 중요정보 유출
- ② 침해사고의 원인 및 현황 조사, 분석하여 피해확산을 최소화하기 위한 대응방안을 수립하여야 한다.
- ③ 침해사고 대응 완료 후 관련 기록을 분석하여 재발방지 대책을 수립하여야 하며, 필요시 별도의 교육 또는 훈련을 실시할 수 있다.

제 14 장. 재해복구 관리

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

제 39 조 (재해복구 계획 수립)

- ① 재해, 사고, 장애 발생 시 핵심 업무를 지속하기 위한 비상 대응 방안으로 위험영향도에 따른 우선순위, 처리시간에 따른 긴급도를 정의하여 재해복구 계획을 수립하여야 한다.
- ② 주요 서비스 및 IT 자산의 복구목표시간과 복구목표시점을 달성할 수 있도록 비용을 고려하여 효과적인 복구전략 및 계획을 수립하여야 한다.

제 40 조 (재해복구 계획의 가동)

- ① 재해복구 계획에 따라 위기상황 발생 시 위기대응팀을 소집하고 위기 상황의 발생원인, 발생 범위 등 관련 정보를 수집하고 분석하여야 한다.
- ② 위기대응팀은 업무영향분석에 따라 핵심업무 복구 우선순위, 업무복구 목표정의를 기준으로 재해복구계획을 따라 대응하여야 한다.
- ③ 위기상황이 종료된 후에는 대응 결과를 분석해 재해복구 계획의 미흡점을 개선하여야 한다.

다.

- ④ 재해복구계획의 실효성을 확보하기위해 모의훈련 또는 교육을 연 1회 이상 실시하고, 재해복구계획을 주기적으로 검토, 개선하여야 한다.