정보보호 정책서

2024. 04. 22

문서 이력

No.	버전	작성일	이력사항	작성자	승인자
1	1.0	2024.04.22	신규 제정	이윤재	대표이사
2					
3					
4					
5					
6					
7					
8					
9					

목차

제 1 장 총칙

제1조 (목적)

본 정책은 ㈜넥스트칩(이하 '회사'라 함)의 정보보안 최상위 정책서로서, 보안 업무에 필요한 사항을 규정함을 목적으로 한다.

제2조 (적용범위)

1. 본 정책은 회사 및 협력회사의 임직원과 내방객 등 회사를 출입하는 모든 사람에게 적용되며, 회사가 보유하고 있는 유・무형의 자산 및 영업비밀 등 모든 정보자산을 대상으로 한다.
2. 본 정책의 내용은 다음과 같다.
   2.1 회사의 정보보안에 대한 정의
   2.2 회사 정보보안관리체계의 범위
   2.3 회사 보안의 원칙과 목표를 뒷받침하는 회사의 보안관리 방향성 제시
   2.4 회사의 중요 정책과 절차에 대한 요약
   2.5 보안 관리에 대한 책임 정의
   2.6 기타 정책을 뒷받침하기 위한 문서화된 참고 자료

제3조 (용어 정의)

1. "정책"이라 함은 회사의 정보보안 전체에 대한 정의와 방향성을 명시한다.
2. "지침"이라 함은 정책의 필요에 대한 구체 설명과 구현 방법을 설명한다.
3. "정보보안"라 함은 일반보안 행위를 포함하고, 정보시스템 및 정보통신망을 통해 수집・가공・저장・검색・송신 또는 수신되는 정보의 유출・위조・변조 및 훼손 등을 방지하기 위하여 관리적・물리적 또는 기술적 수단을 강구하는 모든 행위를 말한다.
4. "개인정보"라 함은 생존하고 있는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향, 영상 및 생체특성 등에 관한 정보를 말한다.(당해 정보만으로 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다) [정보통신망이용촉진 및 정보보호에 관한 법률 2조]
5. "보안관리실태"라 함은 PC, 사무기기, 사무공간 보안 등 부서(팀/그룹/실)단위의 보안 유지 상태를 말한다.
6. "정보시스템"이라 함은 정보의 수집, 가공, 저장, 검색, 송신・수신 및 그 활용과 관련되는 하드웨어와 소프트웨어의 조직화된 체계를 말한다.
7. "보조저장매체"라 함은 이동형 하드디스크(HDD), USB메모리, Flash메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 또는 IC칩 등에 정보를 저장할 수 있는 모든 것으로 정보통신망과 분리할 수 있는 기억장치를 말한다.

8. "보안시스템"이라 함은 정보의 수집, 저장, 검색, 송신 또는 수신할 경우에 정보의 유출, 위조, 변조 및 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다. 이 경우 시설 보호를 위한 CCTV, 출입통제시스템 등을 함께 포함한다.
9. "전산자료"라 함은 회사 업무와 관련하여 취급하는 것으로 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 문서 및 출력물을 말한다.
10. "자산"이라 함은 조직의 정책, 기술, 생산 및 서비스에 관련된 프로세스에서 보유하거나 취급되어지는 효용 가치가 있는 "정보"를 말하며, 서버, 네트워크장비, 보안시스템, 지원장비, PC, 소프트웨어, 저장매체, DB 등 데이터, 홈페이지, 문서파일(전자문서), 문서(종이문서) 등의 보안이 요구되는 모든 보호 대상을 말한다.
11. "서버실"이라 함은 서버·PC 등과 스위치·교환기·라우터 또는 보안시스템 등이 함께 설치 운용되는 출입 통제가 엄격히 요구되는 장소를 말한다.
12. "접근권한"이란 정보시스템에 접속하여 정보를 활용할 수 있는 권한과 정보를 생성·변경·열람 또는 삭제할 수 있는 권한을 말한다.
13. "보안사고"라 함은 내부직원 및 외부자에 의한 비밀정보의 유출, 노출이 발생한 사태를 말한다. 이 경우 해킹, 컴퓨터바이러스, 악성코드 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 포함한다.
14. "비밀정보"라 함은 상당한 노력에 의하여 회사 내에서도 그 취급이 극히 제한되고 권한 이외의 자에게 노출 또는 유출이 되는 경우 회사에 막대한 손해는 물론 민·형사상 책임이 우려되는 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 자산을 말한다. 이 경우 「부정경쟁방지 및 영업비밀 보호에 관한 법률」에서 정한 영업비밀, 「산업기술의 유출방지 및 보호에 관한 법률」에서 정한 국가핵심기술과 본 정책에서 정의하는 개인정보를 포함한다.
15. "주요 직무자"라 함은 임직원 중 집적된 비밀정보 접근이 가능한 권한을 지닌 인원으로서 인원식별 및 추가적인 보안 대책 적용이 요구되는 인원을 말한다. 이 경우 계약관계로 회사에서 근무하는 외부자도 그 대상이 될 수 있다.
16. "중요 자산(시스템)"이라 함은 보안 1등급 자산 중 법준거(예, 정보통신망법, 개인정보보호법, 산업기술의 유출방지 및 보호에 관한 법률)가 요구되는 자산을 말한다.
17. "취약성(Vulnerability)"이라 함은 자산이 잠재적으로 갖고 있는 약점을 말한다. 이 약점 자체가 직접적인 위험을 초래하지는 않지만, 위협에 의해 이용되어 위험을 발생시킬 환경을 제공한다.
18. "기밀성(Confidentiality)"이라 함은 정보가 비인가 된 개인, 개체 또는 처리(processes)들에게 누설되거나 공개되지 않는 특성을 말한다.
19. "무결성(Integrity)"이라 함은 정보가 의도적 또는 비의도적으로 변경되지 않아, 원래의 정보를 유지하는 특성을 말한다.
20. "가용성(Availability)"이라 함은 인가된 개체(entity)가 요구할 때 정보 자산에의 접근과 사용을 가능케 하는 특성을 말한다. 즉 특정 자산이 필요할 때 사용될 수 있어야 함을 의미한다.
21. "보안관리체계"라 함은 정보시스템의 안정성 및 신뢰성을 확보하기 위하여 관리적, 물리적, 기술적 보호조치를 포함하는 종합적인 보안 운영관리체계를 말한다. 이 경우 한국인터넷진흥원 또는

ISO27000계열(예: ISMS, ISO27000 등) 인증기관의 보안관리체계 인증제도에서 요구하는 기준을 포함한다.

22. "보안전담조직"이라 함은 보안 활동을 수행하기 위하여 책임, 권한, 관계가 정의된 조직, 인원 등을 말한다.
23. "정보보안담당자" 이라 함은 사내 정보시스템을 주도적으로 관리하는 인원을 말한다.

제4조 (책무)

1. 대표이사는 자산을 보호하기 위한 보안 대책을 마련하여야 하며 보안에 대한 총괄 책임을 진다.
2. 대표이사는 보안의 책무를 원활히 수행하기 위하여 보안 조직을 구성하고 운영하여야 한다.
3. 회사 소속의 모든 내부직원 및 관련 외부자는 이 정책을 충분히 숙지하고 준수해야 한다.
4. 회사 소속의 모든 내부직원 및 관련 외부자는 이 정책의 위반 시 징계 또는 민・형사상 고발 대상이 되며 그 행위가 회사 경영에 부정적인 영향을 줄 수 있음을 인식한다.
5. 회사 소속의 모든 내부직원은 인사, 복무, 징계 등의 정책에서 정하지 아니한 경우 이 정책에 따라야 한다.

제5조 (지침의 유지관리)

1. 대표이사는 다음 각 호의 상황을 고려하여 연 1회 이상의 정책 변경 여부를 검토하고 필요 시에 지침을 변경할 수 있다.
   1.1 사업상의 변경
   1.2 보안 목표 및 전략의 변경
   1.3 보안 관련 조직 구조 및 인력의 중대한 변경
   1.4 정보시스템의 주요 변경
   1.5 중대한 보안사고 및 새로운 위협・취약성이 발생한 경우
   1.6 보안 관련 법규 및 계약 관계 기업의 보안 정책 요구
   1.7 그 밖에 기타 사용자 부서로부터 검토 및 개정에 대한 요구가 있는 경우와 대표이사가 필요하다고 판단하는 경우
2. 이 지침은 보안위원회의 승인 및 대표이사의 결재를 득한 뒤 인쇄물 형태나 회사의 전자게시판 등을 통하여 전 직원에게 공표되어야 한다.
3. 이 지침의 원활한 시행을 위하여 각 부서 단위의 별도의 지침 또는 운영절차(매뉴얼, 가이드) 등을 수립할 수 있다. 다만 지침과의 일관성 유지를 위하여 지침에 대하여는 그 시행 전에 보안조직에 검토를 요청하여야 하고, 보안조직은 운영절차를 년 1회 목록으로 관리하여야 한다.

제2장 보안 조직

제6조 (보안 조직 구성 및 운영)

1. 회사의 보안을 위하여 대표이사로부터 정보보안책임자로 임명된 임원이 회사 보안을 총괄 관리, 감독하는 정보보안최고책임자로서 역할을 담당하고, 정보보안책임자의 지휘·감독 아래 보안조직이 제반 보안 관리를 담당한다. 이 경우 보안조직 구성 시 보안 관련 교육 이수, 자격 보유 등 보안 전문성을 고려하여 구성원을 임명할 수 있고, 조직 구성원의 활동을 평가할 수 있는 방안을 마련하여야 한다.
2. 보안조직은 보안위원회, 정보보안책임자, 개인정보보호책임자, 정보보안관리자, 정보보안담당자로 구성한다.
3. 보안위원회는 보안 관련 최상위 의사결정 기구로서 필요시 정보보안책임자가 요청하여 소집한다. 위원회는 정보보안책임자와 임원으로 구성한다.
4. 정보보안책임자는 회사의 대표이사 또는 권한을 위임 받은 부문담당 임원 또는 부서장 이상의 직원이 담당하고, 회사의 보안 활동에 대한 총괄 및 책임을 지며 보안조직을 운영하는 책임을 진다.
5. 정보보안관리자는 정보보안책임자로부터 권한을 위임 받은 부서(팀/그룹/실)장급 이상의 직원이 담당하고, 회사의 보안조직을 관리하는 책임을 진다.
6. 각 부서(팀/그룹/실) 정보보안담당자는 각 부서(팀/그룹/실)장이 선임하며 회사의 보안 정책, 지침에 의해 각 부서(팀/그룹/실)별 보안 업무를 수행한다.
7. 보안 업무를 수행하는 자는 수행한 보안활동의 증거가 되는 기록 및 산출물을 필요시 쉽게 확인할 수 있게 이를 유지, 관리한다.
8. 보안조직의 조직원 상세 역할과 책임 및 직무기술 세부사항은「인적보안 관리지침」에서 정한다.

제7조 (보안위원회의 운영)

1. 보안위원회는 CEO가 위원장, 정보보안책임자가 간사를 구성원으로 하여 보안 관련 최고 의사결정기구 역할을 한다. 이 경우, 경영회의 등 보안위원회 구성원과 동일한 경우 해당 회의로 대체할 수 있다.
   1.1 보안 활동의 계획 및 예산 심의
   1.2 보안 정책/지침/절차 등 정책의 검토 및 승인
   1.3 주요 보안 이슈에 대한 대책 결정
   1.4 보안관리체계 내부 이행점검 결과 및 위험분석·평가결과의 검토
   1.5 중대 보안 사고에 대한 검토 및 협의

제3장 인적보안

제8조 (보안에 대한 활동 평가)

정보보안책임자는 보안 전담조직 및 그 구성원에 대한 관리체계를 마련하여야 한다.

제9조 (비밀정보 취급자에 대한 적격심사)

1. 인사부서는 회사의 신규 직원 채용 시에 신원확인 절차 등을 통하여 적격여부에 대한 심사를 할 수 있다.
2. 비밀정보에 해당하는 주요/민감한 정보를 취급하고 정보시스템에 접근권한을 가지는 등 집적된 비밀에 접근할 수 있는 권한을 소유한 인원에 대하여는 채용 절차를 적용하여 적격심사를 할 수 있다.
3. 채용에 관한 일반적인 적격심사는 인사 관련 정책에 따르고 해당 정책에서 정하지 아니한 비밀정보 취급자에 대한 적격심사 세부사항은「인적보안 관리지침」에서 정한다.

제10조 (비밀유지 등 서약의 집행)

1. 인사부서는 회사의 중요 정보를 보호하기 위해 모든 임직원의 채용 시 보안서약서에 서명하도록 하고, 퇴직 시에는 보안서약서의 내용을 환기시켜야 한다. 만약 해당 임직원이 '국가핵심기술 취급자' 업무에 발령 시, 국가핵심기술 취급자용 별도의 보안서약서에 서명하여야 하며, 세부사항은「인적보안 관리지침」에서 정한다.
2. 직원의 채용 및 퇴직에 대한 일반적인 사항은 인사 관련 정책에 따르고 해당 정책에서 정하지 아니한 세부사항은「인적보안 관리지침」에서 정한다.

제11조 (용역사업 보안 등 외부자 보안관리)

1. 용역사업 계약 시 정보시스템, 네트워크, 인력 및 사무환경 등을 관리•통제하기 위한 보안요구사항을 계약서 상에 명시하여야 하며, 제3자에게 정보시스템 및 통제구역에 대한 접근을 허용하는 계약을 체결하는 경우에는 보안정책 준수 및 필수 보안요건을 포함하는 공식적인 계약을 하여야 한다.
2. 정보보안관리자는 회사의 전산자료에 접근이 우려되는 용역사업을 발주하는 경우에는 계약서에 회사의 자산 및 정보시스템을 보호하기 위한 보안요구사항을 반영하여 계약을 체결한다.
3. 용역사업에 대한 관리 책임이 있는 부서의 장은 용역사업의 보안을 위하여 참가인원 등 외부자에 대한 보안서약서를 징구하고 용역사업 산출물의 유출이 이루어지지 않도록 보호대책을 강구하여야 한다.
4. 용역사업에 대한 보안관리 및 외부자 보안에 대한 세부사항은「외부자 보안관리지침」내에서 정한다.

제12조 (보안 감사 및 내부조사)

1. 정보보안책임자는 관련 법률 및 정책 준수여부를 연 1회 이상 정책의 준수 사항을 정기적으로 감사하기 위하여 감사계획을 수립하고 대표이사에게 보고하여야 한다.
2. 감사의 범위는 다음 각 호의 사항 중 하나 이상을 포함할 수 있다.
   2.1 당해 연도 위험평가 결과에 대한 대책의 이행 여부 점검
   2.2 보안관리체계 전 영역에 대한 이행 여부 점검
   2.3 정책, 지침의 내용 중 일부 영역에 대한 이행 여부 점검
   2.4 감독기관 또는 계약관계 기업이 요구하는 보안점검 영역

3. 감사 대상이 되는 부서(팀/그룹/실) 및 직원은 감사조직에 협조하여야 하고 감사결과에 대한 개선요구에 따라야 한다. 다만 보안 전문영역에 대한 감사가 요구되는 경우는 감사의 전문성, 독립성, 객관성을 보장할 수 있는 감사조직을 구성하여야 한다.
4. 감사 및 내부조사에 대한 세부사항은「보안감사 지침」에서 정한다.

제13조 (보안교육)

1. 정보보안관리자는 교육의 시기, 기간, 대상, 내용, 방법 등이 명시된 연간 보안교육계획을 수립하고 정보보안책임자의 승인을 받는다.
2. 정보보안관리자는 모든 내부임직원을 대상으로 정기(연 1회 이상) 및 부정기(필요 시) 보안 정책 등의 준수사항(개인정보보호 포함)을 교육한다.
3. 보안교육의 일반적인 사항은 인사 관련 정책에 따르고 해당 정책에서 정하지 아니한 세부사항은「정보보안교육 지침」내에서 정한다.

제4장 개인정보보호

제14조 (개인정보보호 원칙)

1. 회사에서 수집, 이용, 보관, 폐기 등의 단계를 거쳐 관리가 요구되는 개인정보를 보호하기 위하여 보호원칙을 정의하고 이를 적용하여야 한다.
2. 회사에서 영상정보기기(CCTV)를 이용/사용 시 촬영, 수집, 보관 등의 단계를 거쳐 관리되는 영상정보 또한 개인정보이며, 이를 보호하기 위하여 보호원칙을 정의하고 이를 적용하여야 한다.
3. 개인정보 수집 시, 보유 및 이용 시, 제공 시, 파기 시 등에 보호조치들을 지침으로 규정한다.
4. 개인정보보호를 위하여 정보통신서비스를 통해 관리가 요구되는 경우「정보통신망이용촉진 및 보안 등에 관한 법률」을 따르고 이 외의 영역에서 보안통제가 필요하거나, 회사 비즈니스/업무 변화 따라서 필요 시 별도로「개인정보보호 관리지침」을 제정하여 이를 따른다.

제15조 (정보주체 권리 보장)

1. 회사는 정보주체(고객)가 자신의 개인정보에 대한 열람, 정정・삭제, 처리정지에 대한 요구에 대하여 별다른 사유가 없는 경우 이에 응하고 그 사실을 기록으로 유지한다.
2. 개인정보보호 관련 법률에서 정하는 일정 규모(회사 IT부문 매출, 이용자수) 이상인 경우 연 1회 이상 개인정보 수집·이용 등의 내역을 통지하여야 한다.
3. 개인정보 유출 발생 시 부득이한 경우를 제외하고는 지체 없이 유출 사실 등을 정보주체에게 통지하여야 한다.
4. 정보주체 권리 보장 및 기타 개인정보보호 관련 상세한 사항은「개인정보보호 내부관리계획 지침」에서 정하고, 회사 비즈니스/업무 변화 따라서 필요 시 별도로「개인정보보호 내부관리계획 지침」

과「개인정보보호 관리지침」을 제정하여 이를 따른다.

제5장 자산 및 위험관리

제16조 (자산의 책임)

각 자산의 보호 책임은 관리자, 사용자별로 지정된다.

1 자산의 관리자는 소유 자산을 보호하고 관리할 총괄 책임이 있다. 자산의 관리자에게 부여된 책임과 역할은 다음과 같다.

1.1 자산에 대한 평가/비밀등급 결정

1.2 자산에 대한 사용권한 및 접근권한에 대한 결정

1.3 자산에 공개/반출에 대한 결정 및 승인

1.4 자산을 보호하기 위한 보안사항 정의

2 자산의 사용자는 자산의 관리 및 보호 업무를 수행하며 자산 관리자가 정의한 보안사항을 분석하여, 적절한 보안대책을 구현하여야 한다.

3 자산의 사용자는 자산 관리자가 정의하고 구현한 자산 보안대책을 충실히 이행하여, 획득한 자산을 보호하여야 한다.

4 하드웨어, 소프트웨어 등 회사의 자산은 사용자 등이 임의적으로 교체, 변경, 제거할 수 없으며, 허가되지 않은 프로그램, 통신장치, 보조 저장장치 등을 설치 시 자산 관리자의 승인이 있어야 한다.

제17조 (자산의 분류)

1. 회사의 자산 목록은 정보보안담당자가 작성하여 자산 관리부서에서 취합 관리한다.
2. 자산 목록은 최소 년 1회 이상 갱신되어야 하며, 중대변경 사항 발생 시에는 발생 후 1개월 안에 변경되어야 한다.
3. 정보보안담당자는 자산별 기밀성, 무결성, 가용성의 보장수준을 고려하여 보안등급을 식별하고 보안등급에 따른 보호대책을 강구한다.
4. 자산의 분류 및 관리에 대한 세부사항은「정보자산보안 관리지침」에서 정한다.

제18조 (자산의 위험평가)

1. 정보보안관리자는 위험평가를 위하여 해당 자산의 명세와 책임자를 지정하고 정기적으로 연 1회 이상 재검토한다.
2. 정보보안관리자는 다음 각 호로 구분된 관리운영적, 법(개인보안법)적, 기술적 취약점 진단을 수행한다. 수행 방법론은 다음 각 호의 방법 중 하나 이상을 적용한다.

2.1 취약점 진단 대상 범위 내의 정보자산에 대한 운영 관리 상에서 우려사항(Concern / Issuue) 및 관리운영적 취약점 진단을 수행한다.

2.2 웹페이지 개인정보 법 준거 여부는 개인정보보호법 기반으로 웹에서의 진단이 가능한 항목은 '법 준거(개인정보보호법) 진단 기준에 대해 이행여부를 확인하여 미이행(N: no)에 해당하는 취약성을 위험으로 진단 수행한다. 그리고 어플리케이션 취약점에 대하여 진단을 수행한다.

2.3 취약점 진단 대상 범위 내의 자산 중 '자산 유형'이 '하드웨어'에 대한 관리 및 운영 등에 대한 기술적 취약점 진단을 수행한다.

3. 자산의 위험평가에 대한 세부사항은 「위험관리 지침」에서 정한다.

제6장 물리보안

제19조 (보호구역의 지정 및 관리)

1. 정보보안책임자는 회사 시설 내의 자산을 보호하기 위하여 다음 각 호의 등급에 따른 보호구역을 지정한다.
   1.1 비밀정보의 취급이 빈번하게 발생하는 시설은 통제구역으로 지정하고 외부자의 출입을 제한 적용한다.
   1.2 업무 외 외부인은 공용구역으로 지정된 장소에서만 접견하도록 한다.
2. 관리부서는 외부인이 사업장 내부로 무단 침입할 수 없도록 필요한 물리적 접근 통제 시설과 감시 장치 등을 구축해야 하며, 사업장 각 출입문은 출입이 허가되지 않은 비정상 출입자가 출입할 수 없도록 통제하고 관리 운영하여야 한다.
3. CCTV는 공개된 장소에 설치될 수 없으나, 법령에서 구체적으로 허용하고 있는 경우와 범죄예방 및 수사, 시설안전, 화재예방에 필요한 경우는 설치・운영할 수 있다.
4. 보호구역의 관리에 대한 세부사항은 「물리보안 관리지침」에서 정한다.

제20조 (출입관리)

1. 관리부서는 보호구역의 출입권한을 구분하고 출입자를 식별하기 위하여 지문인식 또는 출입카드 등의 소지기반 출입관리시스템을 적용하여야 한다.
2. 관리부서는 비정상 출입시도를 검토하기 위하여 정기적으로 지문 또는 출입카드 등록현황과 이용내역을 점검하는 등의 주기적인 모니터링과 관리를 한다.
3. 정보보안관리자는 서버실과 IDC(클라우드)의 출입에 대하여 사전 등록된 인원 이외의 자가 출입한 이력이 있는 지의 여부와 장비 반입 반출기록 등을 주기적으로 모니터링하고 관리한다.
4. 보호구역의 출입관리에 대한 세부사항은 「물리보안 관리지침」에서 정한다.

제21조 (통신 및 사무기기 보안)

1. 정보보안관리자는 회사 내의 유선 및 무선 전화를 통한 비밀정보의 유출・노출을 방지하기 위한 보호대책을 수립하여 이행하여야 한다.

2. 정보보안관리자는 인터넷 전화시스템의 도입 시에 정보시스템 운영 등의 업무를 위한 정보통신망 IP대역이 할당되지 않도록 하여야 한다.
3. 통신 및 사무기기 보안에 대한 세부사항은「물리보안 관리지침」에서 정한다.

제22조 (자산의 반입・반출관리)

1. 자산의 반출입 시에는 대상 자산의 비밀등급에 따른 절차에 따라야 한다. 이 경우 용역관계로 인한 외부자의 반입・반출에 대하여도 해당 부서(팀/그룹/실)의 내부직원 관리책임하에 동일하게 적용한다.
2. 자산의 반입・반출 시 전자결재 등의 수단으로 자산의 반출입 이력을 남기고, 작업 내역은 자산 등급에 따라 해당부서(팀/그룹/실) 및 보안조직의 최종 승인권자 확인을 획득한다.
3. 자산의 반입・반출에 대한 세부사항은「물리보안 관리지침」에서 정한다.
4. 자산의 분류 및 관리에 대한 세부사항은「정보자산보안 관리지침」에서 정한다.
5. 자산 분류 내에서 보조저장매체 및 문서에 대한 관리 세부사항은「문서 및 매체 보안 지침」에서 정한다.

제23조 (보조저장매체 보안관리)

1. 회사 내부직원은 보조기억매체를 통한 중요정보 유출 및 매체를 통한 악성코드 감염을 방지하기 위한 사내 정책을 준수하여야 한다.
2. 기타 세부사항은「정보시스템 및 서비스 보안관리 지침」,「문서 및 보조저장매체 관리지침」에서 정한다.

제7장 인증 및 접근권한관리

제24조 (접근권한 관리)

1. 정보보안관리자 또는 보안전담조직은 관리 책임이 있는 정보시스템에 대하여 반드시 사용자 인증과정을 거쳐 접근이 가능하도록 관리하며 다음 각 호의 보호대책을 적용한다.
   1.1 관리책임이 있는 대상 정보시스템에 대한 관리자 및 사용자 접근권한을 주기적으로 점검
   1.2 입사, 부서 이동, 퇴직 등의 변경사항이 발생하는 경우 해당 인원에 대한 접근권한은 즉시 변경, 삭제 등의 조치를 적용
2. 정보보안관리자는 중요정보가 집적된 시스템에 대한 관리자 접근권한에 대하여는 주기적인 패스워드 점검 및 변경, 권한의 오・남용 여부 확인 등 보다 엄격한 관리대책을 적용한다.
3. 정보보안관리자는 중요정보를 취급・운영하는 주요 직무자를 식별하고 인터넷 차단 등의 보호대책을 적용할 수 있다.
4. 기타 세부사항은「인증 및 접근통제 지침」에서 정한다.

제25조 (접근통제)

1. 정보보안관리자는 주요 정보시스템에 대한 보안을 위하여 침입차단시스템 또는 접근통제시스템 이상의 보안시스템을 도입・운영하고 다음 각 호의 보호대책을 적용한다.
   1.1 주요 정보시스템, 네트워크(무선네트워크 포함), 응용프로그램 및 데이터베이스 시스템등에는 인터넷의 연결 또는 원격접근 등을 위한 네트워크 접속은 사전 정의된 보호대책 및 접근규칙을 적용한 후 접속을 통제・허용하고, 의도하지 않은 접속은 불허하도록 관리한다.
   1.2 업무상 동일한 네트워크 대역이 필요한 경우를 제외하고는 IT서비스 업무영역, 대량의 고객정보 취급업무 영역, 일반 업무영역 등의 네트워크를 분리하여야 한다.
   1.3 게스트망 및 인터넷망을 별도로 두는 경우에는 내부 업무망과 단말 간의 자료 전송을 차단하는 조치를 적용하여야 한다.
2. 기타 세부사항은「인증 및 접근통제 지침」에서 정한다.

제8장 암호화 적용

제26조 (암호화 대상 관리)

1. 정보보안관리자는 정보시스템의 개발 및 운영 시 비밀정보와 개인정보 등에 대하여 암호화 적용을 대상으로 한다.
2. 자산은 그 중요성과 기밀성에 따라서 '비밀', '대외비', '일반'으로 비밀등급으로 분류하며, 이때 분류하는 상세방법은「자산 보안관리지침」에 따르며, '비밀', 등급에 해당하는 정보가 비밀정보에 해당한다.

제27조 (비밀정보의 관리)

1. 문서의 열람, 취급 및 배포는 문서의 보안등급에 따라 제한함을 원칙으로 한다.
2. 대외비 이상의 출력물, 복사물 등을 파기하여야 하는 경우에는 분쇄기를 이용하거나 소각, 용해 등 복구가 불가능한 방법을 사용하여야 하며, 비밀정보가 저장된 매체 폐기가 필요한 경우 복구 불가능한 수준으로 이루어져야 한다.
3. 기타 세부사항은「문서 및 보조저장매체 보안 지침」에서 정한다.

제28조 (암호 통제)

1 회사의 비밀정보 및 개인정보의 기밀성, 무결성, 인증 및 부인방지등을 보장하기 위한 암호화를 적용하는데 있어 필요한 사항을 규정하고,『개인정보보호법』,『정보통신망 이용촉진 및 정보보호 등에 관한 법률』의 개인정보의 보호, 정보통신망의 안전성 확보 등 관계법령의 규정을 토대로, 직원 및 개발인력을 통한 보안사고를 예방하기 위하여 지침을 정한다

2 문서의 암호화 기술 적용 시에는, 만족하는 암호화 기술 중 비밀정보/개인정보의 보안성, 성능, 호환

성 및 목적 등을 고려하여 선택 및 검토하여 적용한다. 시스템 관리 및 기술적 한계 등으로 적용이 불가능한 경우 정보보안관리자의 승인을 받아 예외로 할 수 있다.

3 암호화키의 길이는 전수조사공격(가능한 모든 경우의 수를 시행하여 키를 찾아내는 공격)에 의한 피해를 막기 위해 한국인터넷진흥원이 권고하는 기준에 따라 2030년까지 안전도가 보장되는 대칭키 암호알고리즘의 암호화키는 128비트 이상, 비대칭키 암호알고리즘의 암호화키는 2048비트 이상으로 정한다.

4 기타 세부사항은 회사 비즈니스/업무 변화 따라서 필요 시 별도로 「암호화 관리지침」을 제정하여 정한다.

제9장 정보시스템 보안관리

제29조 (정보시스템 도입 시 보안관리)

1. 모든 정보시스템을 소유, 관리하는 정보보안관리자 또는 보안전담조직은 정보시스템 도입 시 알려진 보안취약점을 제거한 후에 네트워크 연결을 하여야 한다.
2. 정보시스템 도입하는 경우 다음 각 호의 조치를 하여야 한다. 다만, 국내외 보안 인증을 획득한 정보보호시스템에 대하여는 적용하지 아니한다.
   2.1 정보보안담당자는 정보시스템의 신규 도입 시 계획을 수립하고 보안 관리자의 승인을 받는다.
   2.2 정보시스템 신규 도입 시 반드시 허가된 소프트웨어만 설치하여야 한다.
   2.3 정보시스템 도입 또는 개선하고자 하는 정보시스템에 대한 기본 보안설정 등이 반영된 인수 승인 기준을 수립한다.
   2.4 정보시스템 인수 전 인수기준 적합성 여부를 확인하기 위한 테스트를 수행하고 그 결과를 문서화하여 관리한다.

5 정보보안관리자는 조직 내 재택근무, 원격협업 이용한 업무 등 스마트워크 환경 도입 시 보안 우려사항을 사전 검토 후 관리, 물리, 기술적 보호조치를 적용하여야 한다.

6 정보보호관리자는 전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다. 이 경우 「전자상거래 등에서의 소비자 보호에 관한 법률」 등 관련 법규의 요구사항을 고려하여야 한다.

7 기타 세부사항은 「정보시스템 및 서비스 보안관리지침」에서 정한다.

제10장 정보시스템 및 서비스 운영보안관리

제30조 (로그인 접근 통제 기능 및 보안관리)

1. 정보보안관리자는 개발자가 정보시스템 로그인 시, 접근통제 기능에 대하여 정의하여야 한다.

2. 접근통제 기능 설계 시, IP를 통한 접근통제, 동시 접속, 우회 로그인, 자동 로그아웃, 접속정보 기록 등에 대한 보안관리 방안과 일반사용자가 응용프로그램을 통하지 않고 직접적으로 DB 및 중요 정보를 가진 파일에 접근할 수 없도록 설계하여야 한다.
3. 정보보안관리자는 정보시스템 서비스에 대한 성능관리를 위하여 성능 점검 항목을 정의하고, 이에 따라 점검 및 관리하여야 한다.
4. 정보보안관리자는 정보시스템 서비스에 장애가 발생하는 경우 장애유형, 장애 관련 로그 및 메시지를 분석하여 시스템 관리자와 그 내용을 공유하고, 정보보안책임자에게 보고하며, 보안사고로 인한 장애의 경우 보안전담조직과 공동 조치할 수 있도록 한다.
5. 정보보안관리자는 장애 발생에 대비하여 중요 정보시스템 서비스에 대한 백업 및 복구 계획을 수립하고, 장애 발생 시 신속한 복구를 위하여 백업 및 복구 계획에 따라 중요 정보시스템 및 데이터 등을 주기적으로 백업하여 관리하여야 한다.
6. 기타 세부사항은「정보시스템 및 서비스 운영관리 지침」에서 정한다.

제31조 (로그 관리)

1. 모든 사용자의 정보시스템 접근 및 사용 내역을 로그 파일에 기록하도록 설계하여야 하며, 사용자 접속 로그(사용자 계정, IP, 일시, 로그인 및 로그아웃 시간), 실패, 출력 내역 등이 기록되어야 한다.
2. 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 안전하게 보존 및 관리 하여야 한다.
3. 기타 세부사항은「정보시스템 및 서비스 운영관리 지침」에서 정한다.

제32조 (보안시스템의 관리)

1. 정보보안관리자는 정보통신망을 보호하기 위하여 보호대책을 마련하여야 한다.
2. 보안시스템 도입 시에는 사내 구매절차와 더불어 보안성에 대한 검토가 이루어지도록 한다. 또한 시스템 도입의 필요성은 용량/성능 측면에서의 문제점과 도입 시의 호환성/안정성/확장성 등을 모두 고려하여 도입하여야 한다.
3. 보안시스템의 보안정책 등록 및 수정・삭제를 위한 지침 또는 가이드를 수립하고 해당 지침에 따른 보안시스템 운영관리 하여야 한다.
4. 기타 세부사항은「정보시스템 및 서비스 보안관리 지침」에서 정한다.

제33조 (프로그램 개발 보안관리)

1. 정보보안관리자는 정보통신망 및 개발인력을 통한 보안사고를 예방하기 위하여 보호대책을 마련하여야 한다.
2. 보안시스템 도입 시에는 사내 구매절차와 더불어 보안성에 대한 검토가 이루어지도록 한다. 또한 시스템 도입의 필요성은 용량/성능 측면에서의 문제점과 도입 시의 호환성/안정성/확장성 등을 모두 고려하여 도입하여야 한다.

3. 개발보안정책 등록 및 수정・삭제를 위한 지침 또는 가이드를 수립하고 해당 지침에 따른 개발보안시스템 운영관리 하여야 한다.
4. 기타 세부사항은「정보시스템 개발 보안 지침」에서 정한다.

제34조 (PC 및 서버 보안)

1. 서버의 구매로 인한 정보침해사고의 방지를 위해 서버 구매 시에는 사내 구매절차와 더불어 보안성에 대한 검토가 이루어져야 하고, 시스템 도입의 필요성은 용량/성능 측면에서의 문제점과 도입 시의 호환성/안정성/확장성 등을 모두 고려하여 도입하여야 한다
2. 정보보안관리자는 PC・LAPTOP(노트북) 등 단말기 사용과 관련하여 일체의 보안관리 지침과 운영책임을 규정하여야 한다.
3. 정보보안관리자는 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위・변조 및 훼손시키지 못하도록 하는 보안대책을 PC 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.
4. 기타 세부사항은「정보시스템 및 서비스 보안관리 지침」에서 정한다.

제11장 비상상황 대응

제35조 (보안사고)

1. 정보보안관리자는 보안사고의 등급 및 유형을 구분하여 그 사안에 따라 신속하게 대응하고 재발방지를 위한 대책을 마련하여야 한다.
2. 내부직원은 회사 내부 또는 외부에서 보안사고 징후를 발견한 경우 신속하게 보안전담조직 비상연락망을 활용하여 신고한다. 이 경우 사안에 따라서는 정보보안책임자의 지시에 의해 부서별 정보보안담당자는 정보보안관리자와 협의하여 접수된 보안사고를 공동 조사, 처리할 수 있으며, 필요 시 외부 전문가 및 전문업체와 협조 체계를 구축할 수 있다.
3. 보안사고 신고 접수 및 징후 발견 시에 회사 경영에 큰 지장을 초래하는 중대한 사고에 대하여는 정보보안책임자의 보안위원회 소집을 통한 경영층의 대응방안 결정에 따른다. 이 경우 개인정보 유출로 확인되면, 상황을 정보주체에게 알리고(유출통지・신고), 피해 최소화를 위한 대책을 마련하여 필요한 조치를 취하도록 한다.
4. 전 항의 경우 정보주체에 대한 통지 결과 및 조치결과를 한국인터넷진흥원에 신고하여야 한다.
5. 보안사고에 대한 세부사항은「보안사고 대응 및 업무연속성 지침」에서 정한다.

제36조 (비상계획)

1. 정보보안관리자는 비상상황 발생 시 사태 유형에 따른 대응방안을 마련하여 신속한 업무 복구가 이루어지도록 하여야 한다.
2. 정보보안관리자는 연 1회 비상상황 유형에 따른 복구목표와 복구방안을 수립한다. 이 경우 IT보안

측면의 비상계획이 함께 포함될 수 있다.

3. 정보보안관리자는 비상사태 유형에 따른 가상의 시나리오를 수립하여 연 1회 비상훈련을 실시한다.
4. 기타 세부사항은「보안사고 대응 및 업무연속성 지침」에서 정한다.

제37조 (IT 재해복구 계획)

1. 정보보안관리자는 각종 재해와 비상사태 발생시 신속하고 조직적인 복구 활동을 전개하고, 사후관리를 철저히 하기 위하여 보고체계, 관리부서 및 관리기준을 수립하여 시행하도록 한다.
2. 기타 세부 사항은「보안사고 대응 및 업무연속성 지침」에서 정한다..

제12장 보안관리체계 유지

제38조 (보안관리체계 범위)

1. 정보보안관리자는 보안관리체계를 운영하기 위하여 보호 대상 자산의 범위를 결정하고 다음 각 호의 내용을 작성하여 관리하여야 한다.

1.1 회사 보안정책, 지침 등 보안관리체계

1.2 보호 대상 자산이 위치한 물리적인 구조 및 네트워크 구성도

1.3 보호 대상 자산의 목록 명세서

2. 제1항 각 호의 내용은 연 1회 이상 정기적인 변경 검토를 실시하고 범위 내의 다음 각 호에 해당하는 경우는 수시로 변경할 수 있다.

2.1 물리적인 구조 및 네트워크 구성의 중대한 변경

2.2 보호 대상 자산의 대규모 변경

2.3 상위 법규 및 감독기관, 계약 관계 회사가 요구하는 보안요구사항의 중대한 변경

3. 주기적 또는 상시적으로 수행하여야 하는 주요 보안 활동 사항(주체, 역할, 업무근거 등)이 포함된 보안관리체계 운영현황표를 작성하고 연 1회 이상 정기적인 검토를 실시한다.

제39조 (보안대책 명세서)

1. 정보보안관리자는 보안관리체계의 효과적인 운영을 위하여 국내 또는 국외 보안관리체계 인증기준을 중심으로 회사 내 운영현황 및 정책 이행증적 등을 확인할 수 있는 명세서(이하 "보안대책명세서"라 한다)를 작성한다.
2. 보안대책명세서는 연 1회 이상 정기적인 변경 검토를 실시하고 제38조(보안관리체계 범위)제2항의 경우에는 수시로 변경할 수 있다.

제40조 (보안관리체계 이행계획)

1. 정보보안관리자는 제18조(자산의 위험평가)의 이행결과로서 **도출된 위험 중 위험 경감을 위한**

대책 이행계획을 수립(이하 "보안관리체계 이행계획서"라 한다)한다.

2. 보안관리체계 이행계획서의 내용은 그 이행 시기에 따라서 보안업무추진계획에 포함되는 경우는 보안관리체계 이행계획서를 별도로 수립하지 않을 수 있다.

제41조 (보안관리체계 재검토)

정보보안책임자는 연 1회 이상 내부보안점검 또는 감사 등의 결과를 통하여 자체적인 보안관리체계를 재검토하고 그 문제점을 개선하여야 한다.

부 칙

제1조 (시행)

이 정책은 2024년 4월 22일부터 시행한다.

제2조 (상위 법·정책의 준수)

1. 이 정책에서 정하지 아니한 사항은 다음 각 호의 관련 법규와 계약관계에서 요구되는 사항 그리고 회사 제(諸) 정책을 준수한다.

1.1 정보통신망이용촉진 및 정보보호 등에 관한 법률

1.2 개인정보보호법

1.3 산업기술의 유출방지 및 보호에 관한 법률

1.4 부정경쟁방지 및 영업비밀 보호에 관한 법률

제3조 (예외적용)

1. 다음 각 호에 해당하는 경우에는 본 정책에서 명시한 내용일지라도 정보보안책임자의 승인을 받아 예외 취급할 수 있다.

1.1 기술환경의 변화로 적용이 불가능할 경우

1.2 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우

1.3 기타 재해 등 불가항력적인 상황일 경우

제4조 (경과조치)

특별한 사유에 의하여 본 정책에 정하는 요건을 충족하지 못한 경우에는 시행일로부터 1 년 이내에 개선방안을 강구하여야 한다.