정보보호 정책

문서번호 : HFN-PO-001

개정버전 : 1.0

2021.05.

HYUNDAI

현대퓨처넷

< 제·개정 이력 >

제·개정번호	조항번호	제·개정내용 요약	제·개정일자	담당자	비고
1.0	-	신규 제정	2021.05.04.	박진우	

< 목 차 >

제1장 총칙 7

제1조 (목적) 7

제2조 (적용 범위) 7

제3조 (용어 정의) 7

제2장 정보보호 관리체계 수립 9

제4조 (정보보호 목표) 9

제5조 (경영진의 참여) 9

제6조 (최고책임자의 지정) 9

제7조 (정보보호 담당자) 9

제8조 (정보보호 위원회) 9

제9조 (정보보호 운영위원회) 9

제10조 (관리체계 범위 정의) 9

제11조 (정책의 수립 및 운영) 10

제12조 (자원할당) 10

제3장 위험관리 11

제13조 (정보자산 식별) 11

제14조 (현황 및 흐름분석) 11

제15조 (위험 분석 및 평가) 11

제16조 (보호대책의 선정) 11

제4장 관리체계 운영 12

제17조 (보호대책 구현) 12

제18조 (보호대책 공유) 12

제19조 (운영현황 관리) 12

제5장 관리체계 점검 및 개선 13

제20조 (법적 요구사항 준수 검토) 13

제21조 (관리체계 점검) 13

제22조 (관리체계 개선) 13

정보보호 선언문

정보통신 기술의 발달에 따라 새롭게 파생되고 있는 각종 위협들은 현대퓨처넷 정보자산에 심각한 영향을 미칠 수 있게 되었으며, 정보보호 활동은 필수 불가결한 요소가 되었다. 따라서 현대퓨처넷 모든 직원은 내부 및 외부로부터의 해킹, 정보의 유출 등 수많은 보안 위협으로부터 중요 정보자산의 손실과 그에 따른 업무의 지연 및 저하, 그리고 각종 법적, 사회적, 윤리적인 여파를 철저히 고려하여 이에 따른 적절한 대비책을 마련하는데 최선을 다하여야 한다.

이에, 현대퓨처넷은 다음과 같은 사항을 만족하는 정보보호 정책을 수립하고 선포하고자 한다.

첫째, 현대퓨처넷의 정보자산을 불법적인 접근과 유출로부터 보호한다.

둘째, 현대퓨처넷의 정보자산에 대한 기밀성, 무결성, 가용성을 유지한다.

셋째, 현대퓨처넷은 정보보호 관련 법적 보안요구 사항을 준수한다.

넷째, 현대퓨처넷의 모든 직원은 정보보호의 중요성을 인식하고, 사고를 적절하게 예방하며, 탐지하고 대응할 수 있어야 한다.

다섯째, 현대퓨처넷은 정보보호와 관련한 위험의 분석, 보안 점검 및 감사를 주기적으로 실시한다.

정보보호 정책은 현대퓨처넷 정보보호에 관한 최상위 문서로서 권고사항이 아닌 반드시 준수되어야 하는 필요성을 갖는다.

현대퓨처넷 이러한 정보보호 정책의 준수를 위해 필요한 시간과 자원을 투자하며, 정보보호를 관리하는 조직을 구성한다. 이 조직은 정보보호 정책, 지침 및 절차를 수립하고, 유지하며, 점검하고, 교육하는 책임을 갖는다. 그러나, 정보보호는 특정 관리 조직으로만 수행될 수 없으며, 무엇보다도 모든 직원들의 참여와 책임이 필요하다. 따라서 모든 직원들은 정보보호의 중요성을 인식하고, 지속적인 관심을 갖고 선포된 정책을 이해하고 준수하는데 최선을 다해야 한다.

정보보호 강령

정보통신 기술의 발달에 따라 새롭게 파생되고 있는 각종 위협들은 현대퓨처넷(이하 "회사"라 함)의 중요 자산인 정보시스템과 정보에 심각한 영향을 미칠 수 있게 되었으며 정보보호 활동은 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 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 담당부서에 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 운영관리 하는 지역은 비 인가자의 접근, 정전, 화재, 수해 등 각종 재난과 사고로부터 보호되어야 한다.

여섯째, 회사의 정보 자산이 침해사고 및 내외부자의 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.

제1장 총칙

제1조 (목적)

본 정책은 ㈜현대퓨처넷(이하 "회사"라 한다.)의 정보보호를 위해 "정보통신망 이용 촉진 및 정보보호 등에 관한 법률", "개인정보보호법" 및 기타 관련 법 및 제도를 준수한 최상위 기준으로 정보보호관리체계를 수립하고 운영하여 정보보호 수준을 제고하며 이를 통해 사업에 대한 연속성을 보장하기 위해 필요한 정책을 규정하는 데 목적이 있다.

제2조 (적용 범위)

본 정책은 당사 회사에 근무하는 전 임직원을 대상으로 하며, 당사의 출입자, 방문자, 제3자 및 당사와 계약관계에 있는 외주인력에게도 적용한다.

1. 회사의 모든 임직원들이 업무와 관련하여 생성 또는 입수하여 소유하고 있는 지적 자산 등의 정보로서, 컴퓨터나 저장매체에 기록된 정보와 각종 인쇄물 등을 포함한다
2. 회사에서 사용 또는 관리하는 모든 하드웨어, 소프트웨어, 네트워크 등을 포함한다.
3. 정보 및 정보시스템에 관련된 인력, 시설 등을 포함한다.

제3조 (용어 정의)

본 정책에서 사용되는 용어는 정보보호 지침에서 규정된 '용어의 정의'를 사용한다.

1. "정보통신망"이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "외부자"란 회사와 계약에 의해 용역 및 서비스를 제공하는 외부 전문가 및 협력업체, 기타 회사의 정보자산에 접근이 허용된 자 및 업체를 말한다.
3. "정보보호관리체계(Information Security Management System)"라 함은 회사의 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영함을 말한다.
4. "보안사고"라 함은 보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출, 변조되어 업무수행에 지장을 초래하는 사고를 말한다.
5. "정보시스템"이라 함은 업무목적을 위해 도입된 정보시스템 장비를 의미하며, 서버, 네트워크, 정보보호시스템, 어플리케이션 등을 총칭한다.
6. "정보자산"이라 함은 회사가 보유하고 있는 가치를 지닌 것으로서, 정보 및 데이터, 소프트웨어, 정보시스템, 단말기(PC, 모바일기기 등), 문서, 물리적/환경적 자산, 인적자산, 서비스 등이 포함된다.
7. "전산자료"라 함은 전산장비에 의해 입력, 보관, 출력되어 있는 자료를 말하며 그 자료가

입력, 출력되어있는 자기테이프, 디스크, 디스켓, 콤팩트디스크(CD)등 보조 기억매체를 포함한다.

8. “제한구역”이라 함은 중요 문서 등이 보관되어 있는 공간을 의미하며, 비밀 또는 주요시설 및 자재에 대한 비인가자의 접근을 방지하기 위하여 그 출입에 안내가 요구되는 구역을 말한다.
9. “통제구역”이라 함은 서버 등 정보시스템 및 통신장비와 같이 중요시설물을 운용하는 곳을 말하며, 비인가자의 출입이 금지되는 보안상 극히 중요한 구역을 말한다.
10. "기밀성(confidentiality)"이라 함은 정보가 인가되지 않은 자에게 노출되지 않는 속성을 말하며, 기밀성이 보장되지 않는다는 것은 중요 정보가 인가되지 않은 내부 사용자나 외부인에게 전송, 백업, 보관 중 유출된다는 것을 의미한다.
11. "무결성(Integrity)"이라 함은 정보가 인가되지 않은 자에 의해 변조되지 않는 속성을 말하며, 무결성이 보장되지 않는다는 것은 중요 정보가 인가되지 않는 내부 사용자나 외부인에 의해 전송, 백업, 보관 중 불법적으로 변조/파괴된다는 것을 의미한다.
12. “가용성(Availabiltiy)”이라 함은 인가된 사용자가 자산을 이용하고자 할 때, 해당 자산의 이용 가능한 정도를 나타내며, 해당 정보와 관련한 자산에 접근할 수 있음을 보장하는 것을 의미한다.

제2장 정보보호 관리체계 수립

제4조 (정보보호 목표)

정보보호의 목표는 회사 업무의 연속성을 보장하고, 정보보호 사고로 인한 시스템 및 자원의 피해를 최소화하는 것이다. 이를 위하여 최고경영자는 정보보호의 중요성을 인식하여 이에 대한 최대한의 지원을 하여야 한다.

제5조 (경영진의 참여)

최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.

제6조 (최고책임자의 지정)

1. 최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
2. 정보보호 최고 책임자는 겸직을 금지한다.
3. 정보보호 최고책임자의 역할 및 권한과 같은 세부적인 사항은 '관리적 보안지침'에 정의한다.
4. 개인정보보호 책임자의 역할 및 권한과 같은 세부적인 사항은 '개인정보 내부 관리계획'에 정의한다.

제7조 (정보보호 담당자)

1. 정보보호 담당자는 정보보호최고책임자가 지정한자로서 회사의 정보보호 관리체계 구축 및 운영에 대한 실무를 담당한다.

제8조 (정보보호 위원회)

1. 회사의 정보보호 및 개인정보보호업무의 효율적인 수행과 운영관리에 관한 주요 사항에 대하여 검토·의결하기 위해 정보보호위원회를 둔다.

제9조 (정보보호 운영위원회)

1. 정보보호위원회는 전사적 정보보호 및 개인정보보호 활동을 위하여 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자로 구성된 정보보호 운영위원회를 구성할 수 있다.

제10조 (관리체계 범위 정의)

정보보호 최고책임자는 조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 정보보호관리체계의 범위를 정의하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.

제11조 (정책의 수립 및 운영)

1. 정보보호와 개인정보보호 정책 및 시행문서를 수립·작성한다.
2. 정보보호 정책 및 시행문서에 대해 정기적으로 타당성을 검토하고 필요 시에 개정한다.
3. 정책은 정보보호위원회의 심의를 거쳐 대표이사가 최종 승인 후 시행한다.
4. 정책의 시행문서를 제·개정하는 경우에는 정보보호최고책임자의 승인을 득하여 시행한다.
5. 정책 및 시행문서를 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
6. 정책 및 시행문서의 이력관리를 위하여 제·개정, 배포, 폐기 등의 이력을 관리하여야 한다.

제12조 (자원할당)

1. 최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하여 책임과 역할을 정의하여야 한다.
2. 최고경영자는 정보보호 관리체계의 효과적 구현과 지속적 운영을 위해 예산 및 자원을 할당하여야 한다.

제3장 위험관리

제13조 (정보자산 식별)

1. 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위내의 모든 정보자산을 식별 및 분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.

제14조 (현황 및 흐름분석)

1. 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화 하여야 한다.
2. 정보서비스 및 개인정보 처리 현황 문서를 주기적으로 검토하여 최신성을 유지하여야 한다.

제15조 (위험 분석 및 평가)

1. 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여야 한다.
2. 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.

제16조 (보호대책의 선정)

1. 회사는 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 회사에 적합한 보호대책을 선정하여야 한다.
2. 정보보호 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.

제4장 관리체계 운영

제17조 (보호대책 구현)

1. 선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.

제18조 (보호대책 공유)

1. 보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.

제19조 (운영현황 관리)

1. 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하여야 한다.
2. 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.

제5장 관리체계 점검 및 개선

제20조 (법적 요구사항 준수 검토)

1. 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다

제21조 (관리체계 점검)

1. 관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하여야 한다.
2. 관리체계 점검을 통해 발견된 문제점을 경영진 및 이해관계자에 에게 보고하여야 한다.

제22조 (관리체계 개선)

1. 법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하다.
2. 경영진은 관리체계 점검을 통해 식별된 문재점 및 개선 필요사항에 대한 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.