# □ 현대퓨처넷 정보보안 관리현황

## 1. 정보보안 방침

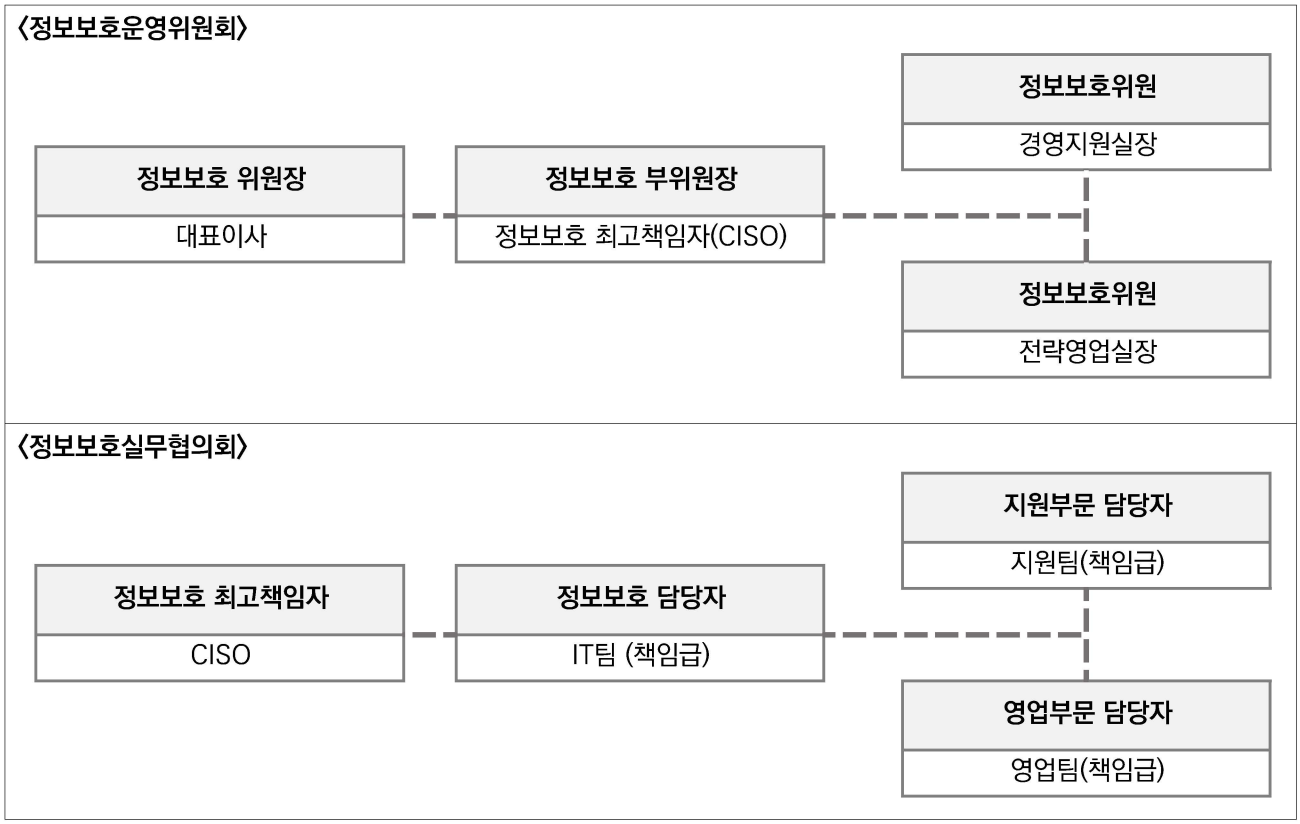
○ 정보보안 목표 : 안정적인 정보보안 서비스를 통한 개인 및 기업 정보 침해 사고 ZERO化

○ 정보보안 관리체계 FLOW


## 2. 정보보안 체계

현대퓨처넷은 고객 정보를 보호하고 정보보호 규제의 변화에 따른 보안 리스크를 최소화하기 위해 정보보호 관리계획을 수립하여 이행하고 있습니다. 2021년 현대퓨처넷 정보보호 정책, 지침, 가이드를 신규 제정하였으며, 2022년 정보보호 정책개정을 통해 대외 요구사항을 반영하고 정보보안을 강화했습니다.

※ 정보보호 체계도



## 3. 정보보안 활동

### 가. 정보보호 및 개인정보보호 관리체계 인증

현대퓨처넷은 2021년 12월 15일 ISMS 신규인증을 최초로 획득하였으며  당사는 ISMS에 부합하는 관리체계를 기반으로 5가지 통합 정보보호 운영 지표를 정기적으로 점검하며, 점검 항목 체계화 작업을 통해 사내 보안 수준을 강화하고 있습니다.
관련 법률 및 신규 제도를 반영하여 정책 1종(정보보호정책), 보안 지침 3종(관리적/기술적/물리적 보안지침)과 가이드라인 4종(개인정보 유출대응, SW개발 보안, 침해사고 대응, 재해복구 대응)을 제·개정 하였습니다.

### 나. 정보보안 리스크 관리

현대퓨처넷은 정보보호 관리체계 운영 및 실태 점검을 통해 대·내외 정보보호 리스크 관리를 강화하고 있습니다. 정보보안 관련 위험요소를 사전예방하고 발생시 체계적인 대응을 위하여 '개인정보 유출 대응 가이드', '침해사고 대응 가이드'를 마련하여 두고 있습니다. 이에 따라 피해 발생 시, 대응 매뉴얼에 따라 유출피해를 최소화하고 신속하고 체계적인 대응과 사후대책 업무수행을 통해 정보의 보안성과 안정성을 유지하고자 합니다. 또한 임직원의 정보보호 의식 수준을 제고하여 리스크를 사전에 예방하기 위해 정보보안 개인화 관리 시스템을 구축하여 임직원 개인별 정보보호 관리지표를 점수화하고 팀차원의 보안점수를  관리하고 있습니다.

### 다. 정보보안 인식 강화

현대퓨처넷은 임직원이 입사할 때부터 매년 보안서약서를 받고 있으며 퇴사 시에는 비밀유지서약서를 받습니다. 정보보안 인식을 내재화하기 위해 매월 사내 인트라넷을 통해 정보보안 관련 중요 사항에 대한 교육 자료를 배포하고 있습니다.

### 라. 정보보안 교육

현대퓨처넷은 관련 법규에 따라 정보보호 교육시간을 충족할 수 있도록 임직원 필수 의무교육으로 지정하여 매년 그룹 인재개발원의 주관 하에 스마트 캠퍼스를 통해 온라인 교육을 실시하고 있습니다. 신입사원 입사 시 개인정보 교육을 필수로 실시하고 임직원은 그룹 인재개발원 주관 교육외 자체적으로 년 1회 정기 교육을 실시하고 있습니다.

### 마. 정보보안 대응훈련

현대퓨처넷은 홈페이지, 주요 업무시스템에 대해 취약성 점검을 하고있으며, 발견된 취약점에 대해 조치계획을 수립하고 조치완료 여부에 대한 이행 결과를 확인하고 있습니다. 또한, 임직원 악성 메일 대응훈련, 정보보호 책임자 및 담당자, 정보보호시스템 관리자 대상 유출·침해사고 모의 훈련을 실시하여 정보보안 침해사고에 대응하고 있습니다.

### 바. 정보보안 점검활동

현대퓨처넷은 외부 전문 컨설팅을 통한 인프라 취약점 진단 및 모의해킹 진단을 진행하여 취약점 보완 조치하고있습니다. 이후 자체감사지표(16개 항목)를 통한 프로그램 보안 및 개인정보 관리에 대한 취약점 점검 후 취약점 개선 조치를 하여 정보보호점검을 실시하고 있습니다.
또한, 외부개발자 점검을 실시하여 프로젝트 투입 전 PC포맷 및 필수 보안프로그램 설치, 노트북 시건장치, 정보보안 서약서 징구를 실시하며 접근 제어(NAC)를 통한 사내망 접속 허용으로 필요한 부분만 접속하도록 관리감독합니다. 프로젝트 철수 시에는 완전 포맷을 통한 철저한 데이터 관리, 비밀유지 서약서 징구하고 있습니다.
더불어, 수탁사 개인정보 체크리스트 기반하여 수탁사 고객정보 관리 실태점검을 실시합니다. ('22년 수탁사 10개 대상 시행 완료)

### 사. 정보보안 모니터링

현대퓨처넷은 외부 보안 전문 업체와의 업무 협약으로 24시간 모니터링을 통해 외부 침입 공격 또는 의심되는 공격에 대해서는 사전 차단을 통해 외부 침입 공격에 대비하며 정보보안 모니터링을 실시하고 있습니다.