지속가능경영(ESG) 헌장

Document No : HSESG-001

Change History

Version	Date	Status	Handled by	Comment
No.1	2024.01.01.	제정	ESG사무국	

0. 목차

1. ESG 경영 선언문

(주)화신은 모든 구성원과 핵심 이해관계자와 함께 사회적 가치를 확장하고 친환경 경영, 사회적 책임 경영, 윤리경영을 적극 실천하여 인류와 자연의 상생 공존에 기여하기 위해 다음과 같이 ESG경영을 추진해 나갈 것을 선언한다.

하나, 미래세대를 위한 환경 경영을 추진하고, 조직의 Net-Zero 2050 달성에 적극 동참한다.

둘, 상생과 협력을 기반으로 사회 문제 해결에 적극 기여한다.

셋, 준법경영과 투명한 지배구조 확립을 위해 적극 노력한다.

넷, ESG 사무국을 구성하여 이사회 중심의 ESG 경영을 실천한다.

다섯, 우리는 환경경영 실천을 통해, 에너지 절감, 기후변화 대응 등 전 지구적 환경문제 대응에 적극적으로 노력한다.

2024년 01월 01일

(주)화신 대표이사 정서진

2. 용어 정의

2.1. 개요

본 장은 ㈜화신의 ESG 경영 각 영역에서 사용되는 개념적인 용어들로 정의된다.

2.2. 용어 및 정의

2.2.1. ESG (Environment, Social, Governance)

친환경, 사회적 책임경영, 지배구조 개선 등 투명경영을 고려한 지속 가능 발전

2.2.2. 탄소중립

대기 중 배출/방출 또는 누출되는 온실가스 양에서 온실가스 흡수량을 상쇄한 순배출량이 "0"이 되는 상태

2.2.3. NDC (Nationally Determined Contribution : 국가온실가스감축목표)

파리기후변화 협정에 따라 2050 탄소중립 실현을 위해 당사국의 국가 온실가스 감축 이행을 위한 중간 단계 목표

2.2.4. 이니셔티브

각 산업계에 속한 주요 글로벌 기업이 해당 산업만의 특성을 고려해 행동강령 내지 가이드라인이라는 자율 규범을 만들고 상호 이행을 독려하고 협력하는 기업 단체

2.2.5. 녹색채권

신재생에너지 등 친환경 프로젝트나 사회기반시설에 투자할 자금을 마련하기 위해 발행하는 채권

2.2.6. 녹색분류체계 (Taxonomy)

민간기업 활동을 저탄소 등의 경영활동 수준에 따라 '녹색'과 '비녹색'으로 구분하는 체계

2.2.7. CDP (Cabon Disclosure Project)

영국의 비영리기구로 전 세계 약 91개국에서 수행하고 있는 글로벌 기후변화 대응을 위한 탄소정보 공개 프로젝트

2.2.8. TCFD (Task Force on Climate - Related Financial Disclosure)

주요 20개국(G20)국가들이 재무장관 및 중앙은행 총재들의 협의체인 금융안정위원회가 기업들의 기후관련 전략정보 공개를 목적으로 만든 협의체

2.2.9. SBTi (Science Based Target initiative)

파리기후변화 협약의 목표달성(산업 수준대비 지구온도 상승폭 1.5도 이하 제한)을 위해 기업들이 과학에 기반한 온실가스 배출감축 목표를 설정할 수 있도록 지침과 방법론을 제공하는 글로벌기관간 파트너십으로 만들어진 프레임워크

2.2.10. 전 과정 평가 (Life-Cycle Assessment)

제품 또는 시스템의 모든 과정에서 발생하는 환경영향 등을 평가(원료 채취 단계, 가공, 조립, 수송, 사용, 폐기 등 모든 과정 포함)

2.2.11. ISO14001 (환경경영시스템)

조직의 모든 활동이나 제품, 서비스와 관련된 환경영향들을 체계적으로 관리하기 위한 시스템

2.2.12. ISO50001 (에너지경영시스템)

에너지 사용자/공급자간 에너지 이용 효율 개선 및 지속적인 관리를 위한 시스템

2.2.13. RE100 (Renewable Energy 100%)

2050년까지 사용전력 100%를 재생에너지로 전환하자는 자발적 국제 협약

3. ESG 경영 기본 원칙

3.1. 일반사항

사회적 책임을 인식하고 기업과 사회의 지속가능한 발전을 위해 노력한다.

3.2. 설명책임

사회와 경제 그리고 환경에 미치는 영향을 인식하며 이를 설명해야 하는 책임을 인식한다.

3.3. 투명성

주요 의사결정 및 활동을 투명하게 공개한다.

3.4. 윤리적 행동

기업 및 기업 구성원은 윤리적으로 행동한다.

3.5. 이해관계자 존중

다양한 이해관계자의 이해를 존중하고 이들과 적극적으로 소통하기 위해 노력한다.
또한 기업 활동에 이해관계자가 참여할 수 있는 다양한 방법을 보장한다.

3.6. 법률 및 규정 준수

기업의 모든 활동은 법률 및 규정 준수를 전제로 한다

3.7. 국제 행동규범 존중

법치를 존중하는 동시에 국제 행동규범을 존중한다.

3.8. 인권 존중

구성원 및 이해관계자의 인권을 존중하고 인권의 중요성과 보편성을 존중한다.

4. ESG 경영 체계

4.1. 개요

4.1.1. 수립 목적

ESG 관점의 비전과 목표를 설정하고 이러한 목표를 달성할 수 있는 전략과 과제, 실행 체계를 구축함으로써 (주)화신 ESG 경영을 고도화한다.

4.1.2. 수립 근거

당사 현황과 대내외 ESG 리스크 및 주요 이해관계자 등을 고려해 ESG 비전과 환경, 사회, 지배구조 영역의 목표를 수립한다.

4.2. ESG 비전

4.2.1. ESG 비전은 기업 비전과 연계하여 경영 목표 및 전략의 토대가 될 수 있도록 한다.

4.2.2. ESG 비전은 사업 내용과 환경, 사회, 지배구조 각 영역에서 달성하고자 하는 목표를 고려해 설정한다.

4.3. ESG 경영 목표

ESG 경영 목표 및 추진전략의 수립과 실행 등 일련의 과정들은 PLAN(계획), DO(실행), CHECK(확인), ACTION(검토.개선) 반복을 통해 운영방법 및 절차를 수립하여 실행한다.

4.3.1. 환경 영역

1) 환경오염 예방

- 대기오염
- 수질오염
- 폐기물 관리
- 화학물질관리
- 온실가스 인벤토리 제3자검증

2) 지속가능한 자원 이용

- 에너지 이용 효율
- 용수사용 및 용수에 대한 접근
- 원자재 이용 효율
- 제품의 자원 사용 최소화

3) 기후변화 완화 및 적용

- 직·간접적 온실가스 배출 출처 식별과 조직의 책임 경계 정의
- 표준에 따른 온실가스를 측정, 기록, 보고
- 조직 통제 내 온실가스 배출 감소 노력과 조직 영향권 내 유사한 행동 격려
- 조직의 주요한 연료 사용량과 유형 검토
- 에너지 효율성과 효과성을 증진하는 프로그램 시행
- 난방, 환기, 공기조절기기를 포함하는 프로세스와 장비에 대한 온실가스 배출 예방과 감소 조치
- 에너지 효율 상품을 구매와 관련 제품 및 개발

4) 생물다양성

- 환경친화적인 도시와 농촌 개발 촉진

4.3.2. 사회 영역

1) 인권존중

- 인권 실사
- 인권 리스크 관리
- 인권침해 연루 회피
- 인권 관련 고충 처리
- 차별 및 취약집단 존중
- 시민권 및 정치적 권리 보장
- 경제적, 사회적 문화적 권리 보장
- 근로에서의 근본 원칙 및 권리 보장(강제노동 및 아동노동 금지, 고용과 직업에서의 차별 금지)

2) 노동관행

- 고용 및 고용관계 내 사회적 가치 창출
- 근로조건 및 사회적 보호
- 근로자의 결사의 자유 및 단체교섭권 보장
- 근로에서의 보건 및 안전 보장
- 작업장에서의 인적 개발 및 훈련 기회 보장

3) 공정 운영관행

- 부패방지
- 자유롭고 책임있는 정치 참여
- 공정 경쟁
- 가치사슬에서의 사회적 책임 촉진
- 재산권 존중

4) 지역사회 참여 및 발전

- 지역사회 참여
- 교육 및 문화
- 고용창출 및 기능 개발
- 기술개발 및 기술 접근성

- 부와 소득의 창출
- 보건, 사회적 투자

4.3.3. 지배구조 영역

1) 지배구조 구성

- 전문위원회 설치 및 활동 내역 공개
- 이사회 구성원의 독립성, 전문성, 다양성 보장
- 이사회 구성원 선임 기준 및 절차 공개

2) 이사회 역할

- ESG 안건 관리 및 지속가능성 보고 관련 이사회의 역할 및 활동 내역 공개
- 이해상충 방지 절차 및 발생 내역 공개

3) 보상 정책

- 이사회 구성원의 보수 결정 절차 내 ESG 안건 관리 성과 및 목표 반영

4) 지속가능한 발전 관련 전략, 정책, 조직 활동

- ESG 경영 전략, 목표, 세부목표 수립 및 결과 공개

4.4. ESG 경영 전략

4.4.1. 수립 근거

환경, 사회, 지배구조 각 영역에서 수립된 경영 목표를 토대로 전략을 마련한다.

4.4.2. 수립 방법

ESG 전략은 달성 가능성과 측정 가능성이어야 하며, 명확하게 입증될 수 있도록 수립한다.

5. ESG 추진 체계

5.1. 개요

화신 ESG 경영 추진 체계로 환경, 사회, 지배구조 영역의 목표 및 전략과 관련 실행 체계를 규정한다.

5.2. ESG 추진조직

ESG 추진 조직은 의사결정 조직인 ESG사무국과 실무 추진부서인 전담조직으로 구성한다.

5.2.1. ESG 전담 조직

환경, 사회, 지배구조 영역별 ESG 목표 및 전략의 추진 사항과 관련 리스크을 보고한다.

5.2.2. ESG 사무국

이사회에서 지정한 ESG 전담 조직의 장들로 구성된 ESG 관련 사무국
ESG 경영 추진 전체 내용 검토, 이사회 안건 상정 여부 검토 후 이사회 안건 상정

5.2.3. 이사회

ESG사무국에서 보고한 ESG 경영 추진 사항과 성과 및 계획에 관한 안건을 검토하고 승인한다.

부서명	***직급/이름***
대표이사	사장 / 정서진
전략기획본부장	상무 / 김태용
안전환경보건팀	상무 / 류우성
내부회계감사팀	상무 / 김종필
총무팀	책임 / 최준희
협력업체지원팀	책임 / 조충래
경영관리팀	책임 / 송명선
글로벌기획팀	책임 / 조보연
구매팀	책임 / 김민수
글로벌스트럭쳐팀	책임 / 채정한
설비관리3팀	책임 / 박진수
경영관리팀	책임 / 이원도
내부회계감사팀	책임 / 이정환
안전환경보건팀	선임 / 김동현
경영관리팀	주임 / 이경민

5.3. ESG 사무국 운영

ESG 사무국은 연간 ESG 추진 업무, 일정 등 계획을 마련하여 운영한다.

5.3.1. ESG 사무국 조직 구성

1) 사무장

- 대표이사

2) 조직 구성

- 환경, 안전, 인사, 상생협력, 동반성장, 구매, 지배구조 등

3) 역할

- 환경부문/사회부문/지배구조
  : ESG 평가결과 및 주요 보완사항 보고 및 차년도 계획 공유

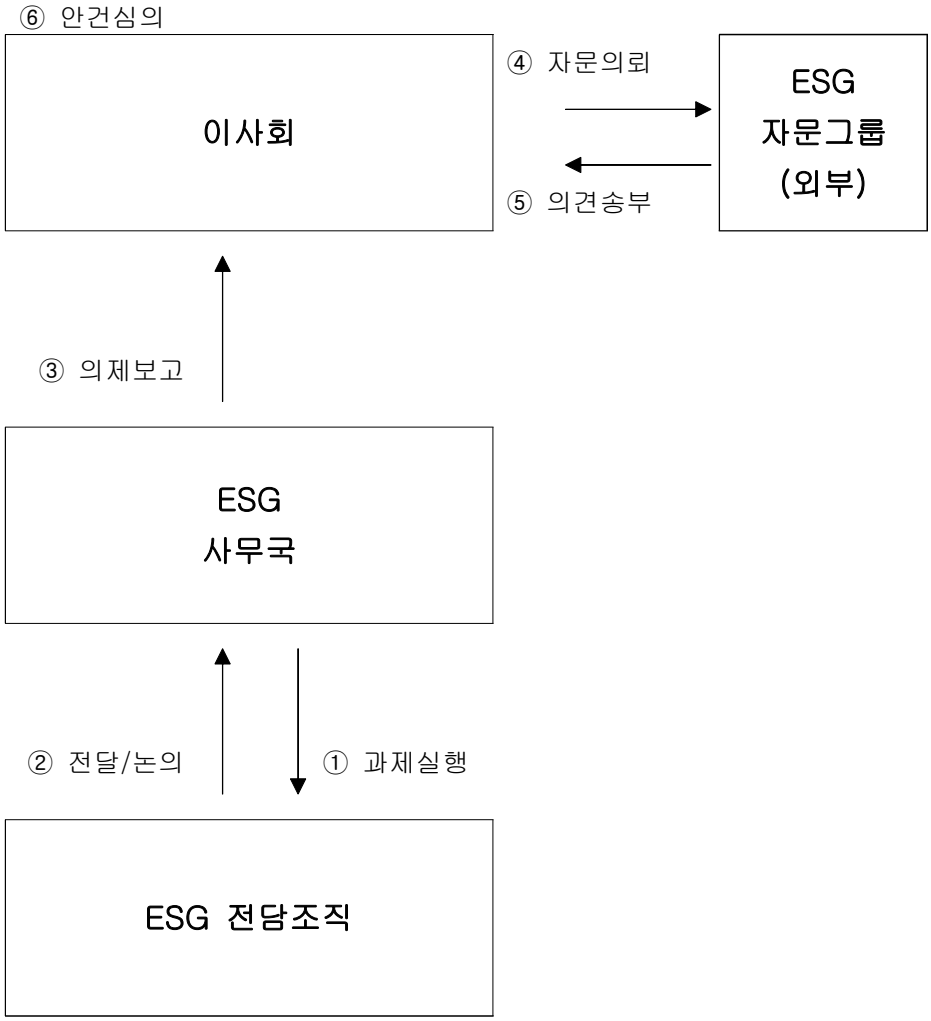
4) 운영주기

- 이사회 내 ESG 사무국 : 1회/년 이상
- ESG 사무국 산하 조직 : 1회/년, 필요 시 수시

5) 운영절차

- 이사회 내 ESG 사무국 주요 추진실적/계획보고(1~2월)
- ESG 추진과제 KPI 수립(1~2월)
- ESG 주요 추진 업무 실행(3월)
- ESG 사무국 개최(격월)
- 부문별 ESG 추진과제 실행(~11월)
- ESG 평가등급 분석(11월)

[ESG 거버넌스 체계]



6. ESG 영역별 업무내용

6.1. 개요

본 장은 ESG 경영에 있어 기업의 투명한 경영을 통해 지속가능한 발전이 될 수 있도록 업무 범위 및 내용을 규정, 기업 경영 현황을 고려한 ESG 경영 이행이 될 수 있도록 한다.

6.2. 업무 범위 및 내용

6.2.1. 환경(E)

전 지구적으로 문제가 되고 있는 기후변화에 대한 대응과 대기오염 관리, 수질오염 관리, 폐기물 관리, 화학물질 관리 등 비온실가스 분야 환경오염 예방 및 저감활동, 자원절약과 효율적 관리를 통해 지속가능한 친환경 기업 이미지를 구축한다.

1) 환경경영 조직구성

- 환경경영을 위한 전사적 실무조직 구성

2) 환경경영 목표 수립

- 환경오염물질(대기, 수질, 폐기물 등) 저감 목표 설정 및 관리
- 원부자재 재활용·절감 목표 설정 및 관리
- 용수 재활용·절감 목표 설정 및 관리
- 에너지·온실가스 저감 목표 설정 및 관리

3) 환경경영 성과 관리

- 환경경영 성과에 대한 평가 체계 구축 및 모니터링
- 환경(ISO 14001)시스템 경영체계 유지를 위한 정기심사
- 에너지(ISO 50001)시스템 구축 검토

4) 교육

- 임직원 대상으로 환경 교육 실시

5) 친환경기술 개발 및 분류 사용 구매

- 설계·생산 전 과정 친환경 기술 개발 적용
- 협력사 및 공급업체 선정에 친환경 선정 기준 반영
- 녹색분류체계(Taxonomy) 기반 친환경 제품 및 서비스 분류체계 구축

6) 환경 리스크 관리

- 환경사고 예방 시스템 구축 관리 및 정기적 대응 훈련 실시
- 환경 규제 준수 및 동향 파악/데이터 관리 체계화

7) 친환경 시설 투자

- 친환경 설비 및 시스템 투자 확대 강화

8) 이니셔티브 대응

- 각종 이니셔티브 이행 선언 검토 및 목표 달성 계획 수립
- 제품 생애 주기적 관점 환경영향 평가

9) 대외 친환경 이미지 활동 강화

- 전사적 제품 환경성 개선 활동에 대한 정보 강화

6.2.2. 사회(S)

안전·보건경영, 인권 및 복지, 사회공헌, 노동 및 고용, 소비자 보호, 공급망 관리, 윤리경영 등을 통해 지속가능한 사회적 책임을 다하기 위해 노력한다.

1) 안전보건

- 전사 안전·보건 전담조직 구성
- 임직원의 안전보건교육 실시
- 안전사고 예방을 위한 정량적 목표 관리
- 지표관리 및 공시(산업재해 건수(률), Near Miss 기준 등)
- 안전을 고려한 설계 기술 개발 서비스 강화

2) 인권 및 복지

- 일과 생활 균형 프로그램 운영
- 인권 침해 예방 프로그램 운영
- 취약 계층 고용 및 차별 방지 정책 운영
- 구조 조정 및 해고 등 절차 마련
- 근로자의 임금수준 공개 및 복지혜택 제도
- 임직원 만족도 조사

3) 고용형태 및 근속

- 근속년수, 여성 근로자 및 기간제 근로자 비중, 이직률 공개 등

4) 인적관리 교육 프로그램

- 계층 및 대상별 다양한 교육 프로그램 운영
- 교육 프로그램별 지표 및 만족 관리

5) 노사

- 노동조합 설립 및 가입 비율, 파업 사례

6) 공정거래 부패방지 조세제도 정치 참여

- 공정거래 원칙 선정 및 프로그램 운영
- 독점 금지정책 공개
- 내부고발자 및 부정 비리 프로그램 운영
- 정치참여·의사표명·로비활동 등 공개 금지

7) 윤리경영 제반사항

- 윤리관련 주요사항에 대한 이사회 또는 C-Level 위원회 등 공론화
- 윤리규정의 감사 점검 및 윤리경영체계 공개
- 윤리위험평가 체계 고도화
- 이니셔티브 가입(UN Global Compact) 여부 검토

8) 공급망 관리

- 협력사 선정기준에 사회적 기준과 환경적 기준 반영

- 협력사 대상 공정거래·상생협력을 위한 조직 구성
- 협력사와 소통을 위한 각종 프로세스 도입 및 프로그램 운영
- 분쟁광물 미사용 정책 수립
- 공급망 표준수립(평가모델, 등급화 등) 및 적용

9) 생산제품 서비스

- 소비자 안전을 고려한 제품 위험성 평가
- 소비자에 대한 공정거래 원칙 설정 및 공개
- 품질관리 인증

10) 사회공헌

- 사회공헌 정책수립 및 프로그램 운영·성과 관리
- 주요 사업 연계 사회공헌 프로그램 운영
- 임직원의 사회공헌 활동 장려 도입 운영
- 이해관계자(주민, NGO, 시민단체 등)와의 협의채널 마련
- 지역사회 기여도 및 기부에 대한 사항

6.2.3. 거버넌스(G)

이사회의 독립적이고 민주적 운영, 회계와 공시의 투명성, 투명한 내부거래와 부패방지, 주주권리 보장 등을 통해 기업 투명성을 높이기 위해 노력을 한다.

1) 이사회 경영진 운영능력

- 이사회 및 감사위원회 산업군 전문가 포함 공개
- 전담조직 구성(내부 이사회 내 위원회 보유 등)
- 부당 거래 행위 확인
- 경영진/이사회 주식 소유 가이드라인 여부 및 정책
- 경영진/이사회 부정 및 비리 여부
- 주주의 경영 참여 현황 및 대응성

2) 이사회 구성

- 이사회 구성원 및 재직기간 정보 공개, 성 다양성 추구
- ESG 사무국, 리스크 관리 위원회 설립 및 운영

- 사외이사 후보 추천위원회 설치 및 운영
- 선임 사회 이사제도 운영

3) 이사회 운영

- 이사회 운영(정기이사회, 이사의 책임 감경제도 등) 등 정관 규정
- 사내이사 과도한 겸직 여부
- 사외이사 연임 기한 및 출석률, 반대/수정의견 제시 안건수 공개
- 사외이사 외부 전문인력 지원 관련 이사회 규정 명문화 규정
- 사외이사 후보 활동정보에 관한 사항
- 주주 제안에 따른 이사 및 감사인 재직 여부
- 위원회 및 사외이사에 대한 규정 및 평가결과 보유

4) 이사회 보수

- 이사회 독립성, 운영정보 공시
- 사외이사 보수 공개
- 이사 보수 한도 적정 설정 여부
- 주주배당금액, 직원 평균 보수 증감률
- 배당수준 분석 및 주당 배당금 관리
- 성과연계보상제도 도입 여부
- 경영진, 이사진 주식 보유 현황 및 거래 정관 공시 여부
- CEO 퇴직 시나리오 검토

5) 감사기구

- 감사위원회 설치, 지원 독립부서 운영 등 감사기구 조직
- 전문가 포함, 사외이사 구성 등 감사위원회 구성
- 감사위원회 운영 및 관련 활동사항 공개
- 감사위원회 내부감사 계획 및 외부감사인 비감사용역 검토
- 외부감사인의 감사용역 외 비감사 용역 수행 및 보수 비율
- 감사위원 장기 재직 검사
- 감사사업체 순환 및 감사인 정책 변경 공개

6) 재무회계

- 회계기준 위반·이상 여부
- 매출 산정 관련 사항
- 자산/부채 비율 및 비용 관련사항
- 우발 채무수준
- 계열사간 출자총액, 신용공여 금액 규모 공개

7) 거버넌스

- 기업지배구조헌장 및 지배구조 정보 공시
- 최대주주, 특수관계인, 계열회사 지분율 5% 이상 보유자 공시
- ESG경영 조직 운영
- ESG 거버넌스 반영 및 보고서 표준 준수·검증·성과목표 공시

8) 기업공시

- 자율공시 및 조회공시
- 불성실공시법인 지정
- 손익 예측정보(영업실적전망) 및 장래 사업계획 공시
- 사업보고서 공시 여부
- 기업지배구조 모범기준과 차이 공개 여부
- ESG 평가 등급 공개 여부
- 이사회 정부/주총 의결권 공개
- 배당정보 공개

6.3. ESG 영역별 추진업무 및 수행 조직

6.3.1. 환경(E) 분야 추진업무 및 수행 조직

분야	추진업무	수행조직
환경	- 환경목표 수립 및 이행 - 온실가스/비온실가스 저감 목표 설정 - 환경사고예방시스템 구축 - 용수, 자재, 에너지 사용 절감 및 목표 수립/모니터링 - 환경경영시스템 운영 - 환경영향 및 성과평가 체계 구축 이행 - 환경리스크 관리 및 규제 준수 - 공정 및 설비별 탄소배출 집약도 개선 - 전사 환경오염물질 통합 모니터링 구축 이행 - 환경설비 투자관리 확대 및 모니터링 - 친환경 생태 사업활동 - 그 밖의 친환경 기술 개발·활동 등에 관한 사항	**안전환경보건팀** **외 유관부서**

6.3.2. 사회(S) 분야 추진업무 및 수행 조직

분야	추진업무	수행조직
사회	- 안전보건 경영시스템 운영 - 안전보건 정량적 목표 설정 및 교육 - 산업재해 등 정량적 지표 관리 - 제품 안전설계 및 고객 안전 강화 - 소비자 안전 고려한 제품 고도화 - 작업자 안전 고려한 기술 개발 - 소비자 안전 제품 및 서비스 기준 수립 - 그 밖의 안전보건의 사회적 책임 등에 관한 사항	**안전환경보건팀** 외 유관부서
	- 인권경영 기반 관련 제반 운영사항 강화 - 사회공헌 활동 및 프로그램 운영 - 노사문화 우수기업 제반사항 수행 - 공급망 관리 및 평가 프로세스 수립 - 임직원 역량 강화 프로그램 운영/지표관리 - 복리후생 관련 제반 운영 제도 강화 - 공정거래, 부정부패방지 등 윤리경영체계 고도화 및 관련 제도 제반사항 수행 - 그 밖의 사회적 책임 운영 등에 관한 사항	경영관리팀 노경팀 구매팀 부품개발팀 협력업체지원팀 총무팀

6.3.3. 거버넌스(G) 분야 추진업무 및 수행 조직

분야	추진업무	수행조직
지배 구조	- 주주 권리 보호제도 도입 - 배당 정책 고도화 - 공시 범위 고도화 - 이사진 구성 다양성 마련 - 이사회 리스크 관리체계 수립 - 이사회 평가 및 보상 제도 합리화 마련 - 그 밖의 지배구조 행사 등에 관한 사항	내부회계 감사팀

7. 첨부

7.1.1 인권경영헌장

7.1.2. 인권경영 세부원칙

7.2.1 윤리헌장 및 실천규범

7.2.2 윤리준법경영

7.2.3 윤리준법 행동지침

7.2.4 윤리강령

7.3.1 협력사 행동규범

7.3.2 공정거래 및 동반성장 협약

7.4.1 책임있는 광물 구매 정책

7.5.1 정보보안 관리

7.6.1. 안전환경보건 경영방침

7.6.2. 환경관리

7.6.3. 생물다양성 정책

7.7.1. 기업지배구조헌장

7.7.2. 이사회 규정

㈜화신 인권경영헌장

(주)화신은 세계인권선언(Universal Declaration of Human Rights),
UN 기업과 인권 이행원칙(UN Guiding Principles on Business and Human Rights) 등의
인권·노동 관련 국제 표준 및 가이드라인을 준수하겠습니다.

하나, 우리는 국내외 법인의 모든 임직원(임원과 직원, 비정규직 포함)과 이해관계자들의 인간의 존엄과 가치를 존중하며, 경영활동 전반에서 인권존중의 책임을 실현하기 위해 노력한다.

하나, 우리는 세계인권선언, UN 기업과 인권에 관한 이행원칙, OECD 다국적 기업 가이드라인, UN 아동권리협약을 비롯한 국제 인권 원칙과 규범 등의 인권·노동 관련 국제 표준 및 가이드라인을 존중한다.

하나, 우리는 인간의 존엄과 가치가 경영 활동으로 구현되어 기업 내 조직문화로 정착될 수 있도록 인권경영 원칙을 수립하여 따른다.

하나, 우리는 협력사에 대한 책임을 다하기 위해 그들의 인권 및 노동권이 침해되지 않도록 인권침해 예방 활동과 동반성장 및 상생발전을 위한 다양한 채널의 V.O.C 활동 등을 시행하여 인권경영을 실천하도록 지원한다.

하나, 우리는 지역사회의 인권 증진을 위해 모든 업무 수행 시 지역주민의 인권이 침해되지 않도록 유의하며, 필요시 그 예방을 위한 조치를 적극 강구한다.

하나, 우리는 지속 가능한 환경에 대한 권리를 인권으로 인식하여, 환경 보호를 위해 국내외 환경법규 준수를 노력하며, 탄소중립, 생물다양성, 자원순환 달성과 친환경 사업장 조성에 적극 노력한다.

하나, 우리는 아동노동, 강제노동, 착취, 인권유린, 분쟁조장 등의 인권 침해 우려가 있는 방법 혹은 불법적이거나 비윤리적인 방법으로 생산된 원자재는 사용하지 않는다.

하나, 본 인권헌장에서 다루는 사항이 현지 국가의 법규와 상충되는 경우에는 현지 법규를 우선적으로 준수하고, 해당 국가에서 요구하는 법규 및 산업 특성을 반영하여 본 인권헌장을 개정하여 사용할 수 있으며, 필요 시 별도의 세부 정책을 수립할 수 있다.

㈜화신 인권경영 세부원칙

① 인권존중

인권 침해에 해당하는 어떠한 행위도 발생하지 않도록 구성원 모두가 서로 존중한다.

② 차별금지 및 괴롭힘 금지

합리적인 이유 없이 모든 임직원의 성별,인종,민족,국적,종교,장애,나이,가족관계,임신 및 출산,사회적 신분 및 정치적 견해 등을 이유로 채용,승진,교육,임금,복리후생 등과 관련하여 차별하지 않는다. 말이나 행동으로 성적 굴욕감 및 혐오감을 유발하는 행위나 성희롱과 집단 따돌림, 비인도적 행위, 위협과 같은 괴롭힘을 금지한다.
임직원이 종교적 활동을 위해 편의가 요구될 경우, 필요 시 합리적인 편의를 제공할 수 있도록 한다.

③ 인도적 대우

임직원의 사생활을 존중하고 동등한 기회를 제공하며, 불합리한 대우를 하지 않는다.
또한 정신적 육체적 강압과 학대 등 비인도적대우가 발생하지 않도록 노력한다.

④ 근로시간 준수 및 개선

사업을 영위하는 국가의 근로조건과 관련된 법적 기준을 철저히 준수하며, 근로조건 개선을 위해 노력한다.
근로 시간에 대해 엄격한 기준을 따르며, 초과근무의 경우 법규에서 정하는 기준에 따라 초과근로수당을 지급한다.
모든 임직원에게 생활임금을 고려하여 근로에 대한 합당한 보수를 급여명세서와 함께 지급한다.

⑤ 강제노동 및 아동노동 금지

모든 근로자는 자발적이어야 한다. 임직원 및 이해관계자에게 폭행, 협박, 감금, 인신매매 등을 수반한 자유의사에 반하는 모든 형태의 비자발적 강제노동을 배제하며, 강제노동과 아동노동에 대한 인식 교육을 진행한다.
현지 법률에 따라 아동은 고용하지 않으며, 그 고용이 불법이 아닌 경우에 한하여 근로의 기회를 제공하며 이 경우 교육을 받을 권리가 제한되지 않도록 노력한다. 아동노동이 발견된 경우에는 지원과 교정이 이루어져야 되며, 즉각적으로 아동에 대해 보호조치를 한다.
노동력 착취를 목적으로 협박, 강요, 강제, 납치, 사기 등으로 사회적 약자를 채용, 이동, 전근시키는 등의 모든 행위는 하지 않는다.

⑥ 결사 및 단체교섭의 자유

헌법 및 노동관계 법령에서 보장하는 결사의 자유 및 단체 교섭 권리를 존중한다.
모든 임직원에게 충분한 근로 의사소통 기회를 제공하며, 노동조합 가입 및 활동 결성 등의 이유로 불합리한 처우를 하지 않는다.

⑦ 지역주민에 대한 인권 보호

모든 임직원은 업무 수행 시 지역주민의 인권, 환경 및 안전보건 등에 미치는 영향을 파악하고 필요한 경우 영향 평가를 실시한다. 또한, 관련한 문제가 발생한 경우 지역주민의 의견을 수렴하고 협의 과정을 통해 문제가 해결될 수 있도록 노력한다.
새로운 토지 구매 전, 토지의 법률상 소유자와 지역주민 및 토착민의 법과 관습에 따른 권리 존재를 확인해야 되며, 저작권 또는 지적재산의 소유권 확인 시에는 관습적으로 보호되는 지적재산권 여부도 함께 검토 한다.

⑧ 고객 인권 보호

모든 임직원은 제품과 서비스를 제공할 시, 고객의 안전과 건강보호를 최우선으로 해야 하며 경영활동으로 수집한 개인정보 보호를 위해 최선의 조치를 취한다. 고객의 정당한 요구와 합리적인 제안은 적극 수용하도록 한다.

⑨ 산업안전에 대한 보장

모든 임직원의 안전 및 보건을 최우선으로 고려하여 사업장 시설 장비 도구 등을 정기적으로 점검하여 임직원의 안전한 근로환경을 보장한다. 위험 예방을 위한 적절한 조치와 관리방안을 마련한다.

⑩ 책임감있는 공급망 관리

자회사뿐만 아니라 공급망 내에서도 인권경영을 실천할 수 있도록 지속적으로 관리한다.

㈜화신 윤리헌장 및 실천규범

① 사회적 책임 이행

우리는 사회가 요구하는 기본적인 가치관을 존중하고 각종 법규를 준수하며 국가경제와 사회발전에 기여한다.

1. **사회적 책임**
   사회의 목적이나 가치에 적합한 경영 및 정책을 통해 경제성장, 지역사회에 대한 기여 등의 사회적 책임을 다한다.
2. **지속가능발전 목표**
   기업이 직면한 환경적, 사회적 문제를 해결하기 위해 투자와 혁신을 통한 기업성장으로 일자리 창출 등의 사회적 기여를 한다. 환경적 사회적 기여를 통해 지속가능한 발전 목표달성에 책임을 다한다.
3. **환경보존**
   사업 전 영역에서 환경에 대한 피해를 최소화하기 위해 환경관련 규제 및 법규를 준수하여 사회적 책임을 다한다.
4. **사회공헌 및 기부활동**
   사회적으로 당면한 문제를 발굴하고, 해결 방안을 적극 모색한다. 기부는 기업 내부에서 공정하고 투명하게 추진하고, 정치적 목적 또는 부당한 이익을 목적으로 하는 기부활동은 금지한다.

② 신뢰받는 기업 추구

우리는 회사의 명예를 지키고 도덕성과 정직성을 바탕으로 한 공정한 직무 수행으로 신뢰받는 기업을 이룩한다.

1. **공정거래**
   협력업체 및 거래관계에 있는 업체와 공정한 거래를 하며, 상생관계를 추구한다.
2. **반독점 행위**
   시장에서의 지위를 이용하여 불공정한 거래를 통해 공정한 경쟁을 저해하는 행위를 하지 않는다.
3. **담합**
   사업자가 계약이나 협정 등의 방법으로 다른 사업자와 함께 가격을 결정하거나 거래 상대방을 제한함으로써 실질적인 경쟁을 제한하는 행위를 하지 않는다.
4. **부정방지**
   거래관계에 있는 업체로부터 부정하게 정보를 획득하지 않으며, 획득한 정보를 사용해서는 안된다.
5. **지식재산권**
   협력사의 영업비밀을 보호하고, 부당하게 지식재산권을 침해하지 않는다.
6. **납세의무**
   세법에 위반되는 조세처리 행위는 하지 않으며, 정당한 납세의무를 다하여 기업에 주어진 책임을 다한다.
7. **자금세탁**
   고객, 협력업체, 개인 및 관련 기관의 자금세탁과 관련된 행위를 하지 않는다.
8. **위조부품 방지**
   회사는 승인되지 않은 원재료 및 부품 등을 생산, 사용하지 않으며, 위조된 원재료 및 부품 등을 사용하거나 판매하지 않는다.
9. **수출제한 준수**
   회사는 수출제한과 관련한 국가별 법률 및 국제적 규약을 준수한다.
10. **이해상충 방지**
    회사, 주주, 또는 고객과의 이해상충 방지를 위해 노력하여야 하며, 이해상충 발생이 예상되는 경우 적법한 절차에 따라 관리하여야 한다.

㈜화신 윤리헌장 및 실천규범

③ 인간존중 경영

우리는 직원 개개인의 존엄과 가치를 존중하고 공정한 인사와 복지를 구현한다.

1. **인권**
   모든 임직원을 독립된 인격체로 존중하고 인권이 보호 받을 수 있도록 제도적 문화적 조치를 취한다.
2. **차별금지**
   국적,출신지,인종,성별,연령,문화,종교,장애,학력,가족관계,임신 및 출산,사회적 신분,정치적 성향 등을 이유로 차별하지 않는다.
3. **공정한 보상**
   모든 임직원에게 동등한 기회를 제공하고 공정한 평가를 통해 성과에 대해 적절하게 보상한다.
4. **직장 내 괴롭힘**
   직장에서의 지위 또는 우위를 이용하여 언어적 또는 신체적 폭력, 성희롱, 따돌림, 협박 등과 같이 인격모독, 신체적 · 정신적 고통을 주는 모든 행위를 금지한다.
5. **일 · 가정 양립**
   모든 임직원의 일과 가정이 조화롭게 균형을 이루는 업무환경을 조성한다.
6. **안전 및 보건**
   모든 임직원의 안전을 우선시하며 직무상 사고 및 부상 재난 재해 질병 및 전염으로부터의 안전한 작업환경을 유지한다.
7. **노동법 준수**
   아동 및 강제노동 등 위법한 노동을 금지하고 근로시간을 준수하며,사업장이 위치한 각 국의 노동법을 준수한다. 임직원의 생활을 제약할 수 있는 신분증, 여권 등을 보관하지 않으며, 채용에 대한 비용과 대가를 요구하지 않는다.
8. **내부 고발자 보호 제도**
   내부 고발자의 신변을 보호하며, 불합리한 대우나 차별, 보복을 당하지 않도록 필요한 조치를 이행해야 한다. 제보자의 익명성을 보장하며, 제보 접수 후 처리절차에 대해서는 개별 안내를 한다.

④ 고객을 위한 가치 창조

우리는 고객의 입장에서 고객이 필요로 하는 새로운 가치를 창조하고 제공한다.

1. **정보제공**
   고객에게 적절한 정보를 제공하여 올바른 의사결정을 할 수 있도록 돕는다.
2. **정보보호**
   고객의 정보 보호를 위해 법규와 규정을 준수하며 정보를 침해할 수 있는 행위를 하지 않는다.
3. **의견수렴**
   고객의 의견을 경청하여 정당한 요구와 제안은 적극 반영한다.
4. **차별적 영업활동 금지**
   영업활동과 무관한 사항을 근거로 고객이 제품 사용을 부당하게 제약 받지 않도록 필요한 조치를 취한다.
5. **품질보장**
   제품 생산 과정에서 품질 확보를 위해 노력하고 고객에게 최상의 제품을 공급하기 위하여 적절한 기준을 통해 최선의 품질을 유지한다.
6. **고객안전**
   연구개발, 원자재 조달, 생산, 판매 및 유통, 판매 후 서비스 전 과정에서 고객의 안전과 타협하는 의사결정을 하지 않는다.

⑤ 주주 이익 극대화

우리는 원가절감과 생산성 향상을 통해 기업 가치를 극대화하여 주주 이익에 기여한다.

1. **주주가치 증진**
   주주의 가치 증진 및 기업의 가치도 동반 증진하여 기업가치 극대화를 추구한다.
2. **정보공개**
   회사의 규정 및 정보 관련 법규에 따라 기업의 공시 정보는 적시에 공개한다.

㈜화신 윤리준법경영

화신은 인간 본위의 경영, 모두가 참여하는 열린 경영의 가치 아래 전 직원이 일치단결하여 고객이 신뢰하는 파트너로서 나아가 지역사회의 일원으로서 맡은바 역할과 책임을 완수할 것이며,

좋은 생각을 바르게 실천한다는 좌우명과 함께 현실로 다가온 무한 경쟁시대를 앞서서 헤쳐 나갈 것입니다.

이에 화신은 임직원 개개인의 품위와 회사의 명예를 유지하고 협력사와의 거래에 있어서 공정성을 확보하여 올바른 기업문화를 정립하기 위하여 모든 임직원이 지켜야 할 올바른 행동과 가치판단의 기준으로서 윤리준법규범을 제정하고 그 실천을 다짐합니다.

화신 임직원의 기본 자세

화신의 임직원은 각 개인의 행위가 회사의 명예와 부합됨을 인식하고, 건전한 기업문화 구현 및 회사의 대내외적 공신력을 더욱 공고히 하기 위해 다음의 자세를 견지해야 한다.

1. 제반 업무 처리에 있어서 항상 공정하고, 투명하게 적법한 절차에 따라 직무를 수행한다.

2. 우월한 권한과 지배적 지위를 이용한 어떠한 형태의 불법・부당행위(반경쟁행위)도 하지 않는다.

3. 직위를 이용한 사적 이익 추구와 비공개 정보를 이용한 불공정 거래를 방지한다.

4. 고의적인 업무 지연으로 어떠한 대가도 의도하지 않는다.

5. 업무를 수행하는데 있어서 상호간에 예의를 갖추어 임한다.

6. 업무의 수행과 보고는 공정하고 정직하게 한다.

7. 임직원 및 경영 활동과 관련된 모든 문서는 정확하게 기록, 유지 및 보고 한다.

8. 회사의 재산을 보호하고 거래과정에서 발생된 정보 및 업무상 知得한 회사의 기밀사항에 대하여 철저한 보안을 준수한다.

9. 일상생활 및 직무와 관련하여 국가의 법령과 화신 규정을 준수하며, 사회로부터 지탄받을 수 있는 비도덕적, 비윤리적 행위를 하지 않는다.

㈜화신 윤리준법 행동지침

① 불법·부당한 사익 도모 금지

직무와 관련하여 그 직위 또는 권한을 남용하거나 국가의 법령 또는 화신 규정을 위반하여 회사 내부 및 외부의 이해관계자로부터 다음과 같은 형태의 이익을 도모해서는 안 된다.

1) 금전적 이익
현금, 수표 및 유가증권, 선물 및 상품권, 회원권, 항공권, 숙박비, 부채에 대한 상환 및 보증 기타 현물화 가능 물품

2) 접대
향응 접대 및 사회통념상 인정되는 범위를 초과하는 식사 접대(통상적으로 인당 3만원 이상)

3) 직원 또는 임원으로의 이중 취업

4) 자본적 수익의 취득 또는 보장
미공개 정보를 이용한 비공식적인 주식 등의 취득, 공동 투자, 공동재산 취득

5) 편의의 제공 및 수수

6) 기타 상기에서 언급하지 않은 금품 수수 및 이에 준하는 행위.

② 부당한 요청 금지

우월적인 지위 또는 호의적인 관계를 이용하여 회사 내부 및 외부의 이해관계자에게 다음의 행위를 요청해서는 안 된다.

1) 사회적으로 지탄 받을 수 있는 청탁이나 압력

2) 사적인 부탁 및 의뢰(상품판매, 보험가입, 할인권 판매 등)

③ 회사 자산의 불법·부당 사용 금지

회사의 유·무형자산이나 경영정보를 자기 또는 제3자의 사적 이익을 위하여 다음과 같이 이용해서는 안 된다.

1) 회사의 승인 없는 개인적 이용 또는 제3자에게 양도 또는 대여

2) 회사 예산의 개인적 용도 사용 또는 회사가 정한 목적과 다른 지출 및 회계장부 허위 기재

3) 회사의 특허권 등 지적재산권과 사업정보 및 기술정보를 포함한 회사 정보자산의 영리 목적 이용 또는 무단 유출

④ 건전한 기업문화 저해행위 금지

건전한 기업문화를 해치는 다음의 행위를 하여서는 아니 된다.

1) 성희롱 등 개인의 인권을 침해하고 근무 분위기를 저해할 수 있는 풍기문란 행위

2) 성별, 학력, 출신지역, 결혼, 인종, 국적, 종교 등을 이유로 한 부당한 차별대우행위

3) 폭행, 폭언 등 질서를 해치는 행위

4) 회사와 관련된 정보의 왜곡·날조 또는 무단 훼손행위 및 조직 구성원 간에 불신을 조장하는 회사 또는 개인에 대한 허위사실이나 유언비어 유포행위

5) 기타 개인의 품위와 회사의 명예를 훼손할 수 있는 비도덕적, 비윤리적 제반 행위

⑤ 기타 법령 및 사규 위반행위 금지

기타 일상생활 및 직무와 관련하여 국가의 법령과 화신 규정을 위반해서는 안 된다.

㈜화신 윤리강령

제 1장 총 칙

제 1조 [명칭]

본 규칙은 주식회사 화신(이하 "회사"라 한다)의 윤리 행동강령이하(이하 "강령"이라 한다)이라 칭한다.

제 2조 [목적]

이 행동강령은 회사의 부패방지와 깨끗한 직무환경조성을 위하여 임직원이 준수하여야 할 행동의 기준을 규정하는 것을 목적으로 한다.

제 3조 [정의]

이 강령에서 사용하는 용어의 정의는 다음과 같다.

1. 사원(직원)이라 함은 취업규칙에 의하여 채용된 사원(직원)을 말한다.
2. 임원이라 함은 이사([상법] 제401조의 2 제1항 각 호의 어느 하나에 해당하는 자를 포함한다) 및 감사를 말한다.
3. “직무관련자” 라 함은 직원의 소관업무와 관련되는 임직원 외의 자로서 다음 각 호에 해당하는 자(개인 또는 단체)를 말한다.
   1) 회사 관련 민원을 제기하였거나 제기할 것이 명백한 자
   2) 감사, 감독, 검사 등의 대상인 자
   3) 회사에 보상을 요청하였거나 요청하려는 것이 명백한 자
   4) 회사와 계약을 체결하였거나 체결하려는 것이 명백한 자
   5) 회사에 대하여 특정한 행위를 요구하였거나, 직원의 직무상 권한의 행사 또는 불행사로 인한 금전적 이해관계가 있는 자
   6) 정책, 사업 등의 결정 또는 집행으로 이익 또는 불이익을 직접적으로 받는 자
   7) 그 밖에 회사에서 부패방지를 위하여 정하는 업무와 관련된 자
4. “직무 관련 임직원” 이라 함은 임직원의 직무수행과 관련하여 이익 또는 불이익을 직접적으로 받는 다른 임직원 중 다음에 해당하는 직원을 말한다.
   1) 직원의 담당업무와 관련하여 직무상 명령을 받는 하급자
   2) 인사, 예산, 감사, 상벌 또는 평가 등의 직무를 수행하는 담당직원 이외의 임직원
   3) 업무를 위임, 위탁하는 경우 그 업무를 위임, 위탁하는 직원, 위탁 받는 직원
   4) 그 밖에 회사에서 정하는 직원
5. “금품 등” 이란 다음 각 목에 해당하는 것을 말한다.
   1) 금전, 유가증권, 부동산, 물품, 숙박권, 회원권, 입장권, 할인권, 초대권, 관람권, 부동산 등의 사용권 등 일체의 재산적 이익
   2) 음식물・주류・골프 등의 접대・향응 또는 교통・숙박 등의 편의 제공
   3) 채무 면제, 취업 제공, 이권 부여 등 그 밖의 유형・무형의 경제적 이익
6. “공직자 등” 이란 부정청탁 및 금품 등 수수의 금지에 관한 법률에서 정하고 있는 공직자 또는 공적 업무 종사자를 말한다.
7. “내부정보” 라 함은 회사의 경영 또는 재산상황 등에 관한 것으로서 투자자의 투자판단에 영향을 미칠 수 있는 일체의 미공개 정보를 의미한다
8. “협력업체” 란 회사가 발주하는 공사 및 물품을 구매하는 등록한 외부업체를 말한다.
9. 강령에서 사용하는 용어 중 본조에서 별도로 규정하지 않은 용어의 정의에 관 하여는 관련 법령과 규정에서 사용하는 용어의 정의에 의한다.

㈜화신 윤리강령

제 4조 [적용범위]

이 강령은 회사의 모든 임직원(근로계약에 따른 파견근로자를 포함한다)에게 적용한다.

제 5조 [준수의무와 책임 등]

모든 임직원은 행동강령을 숙지하고 준수하여야 하며 위반 사항에 대하여는 그에 따른 책임을 진다.

제 6조 [준수서약]

모든 임직원은 매년 「준법서약서」 [별지 제1호 서식]를 내부회계감사팀에게 제출하고 이를 준수하여야 한다.

제 2장 공정한 직무수행

제 7조 [공정한 직무수행을 저해하는 지시]

1. 임직원은 하급자에게 자기 또는 타인의 이익을 위하여 법령이나 규정에 위반하여 공정한 직무수행을 현저하게 해치는 지시를 하여서는 아니 된다.
2. 상급자로부터 공정한 직무수행을 위반하는 지시를 받은 직원은 그러한 지시에 따르지 아니하여야 하고, 내부신고제도에 따라 회사에 해당 사실을 신고한 후 회사의 별도 지시를 받을 수 있다.
3. 임직원은 제2항에 따른 지시 불이행을 이유로 어떠한 차별이나 불이익을 받지 아니한다.

제 8조 [이해관계 직무의 회피]

1. 임직원은 자신이 수행하는 직무가 자신, 자신의 직계 존속·비속, 배우자 및 배우자의 직계 존속·비속과 금전적 이해관계가 있거나 다음 각 호의 어느 하나 에 해당하는 자가 직무관련자인 경우에는 그 직무의 회피 여부 등에 관하여 소속 팀장 또는 내부회계감사팀에 보고 후 처리하여야 한다.
   1) 친족(「민법」 제777조에 따른 친족을 말한다)
   2) 자신이 2년 이내에 재직하였던 단체의 대리인
   3) 300만원 이상의 금전거래가 있는 자
   4) 배우자, 자신의 직계 존속·비속과 형제자매, 배우자의 직계존속과 형제 자매가 대표이사 또는 임직원으로 재직하고 있는 영리를 목적으로 하는 단체
   5) 회사 퇴직임직원으로서 퇴직 전 5년 이내 같은 부서에서 근무하였던 자
   6) 학연, 지연, 종교, 채용 동기, 종래에 같은 직장에서 근무한 경우 등 지속적인 친분 관계가 있어 공정한 직무수행이 어렵다고 판단되는 자
   7) 최근 2년 이내에 인·허가, 계약의 체결, 정책·사업의 결정 또는 집행 등 직무 수행으로 직접적인 이익을 주었던 자 중 지속적인 친분 관계가 형성되어 공정한 직무 수행이 어렵다고 판단되는 자
   8) 그 밖에 대표이사가 공정한 직무수행이 어려운 관계에 있다고 정한 자 다만, 대표이사가 공정한 직무수행에 영향을 받지 아니한다고 판단하여 정하는 업무의 경우에는 제외한다.
2. 임직원은 제1항에서 정하고 있는 사항에 해당하는지 여부가 불분명한 경우 소속 팀장 또는 내부회계감사팀과 반드시 상의하여야 한다.

㈜화신 윤리강령

제 9조 [특혜의 배제]

임직원은 직무를 수행함에 있어 지연, 혈연, 학연, 종교 등을 이유로 특정인에게 특혜를 주거나 특정인을 차별하여서는 아니 된다.

제 10조 [예산의 목적 외 사용 금지]

임직원은 업무활동을 위한 예산을 목적 외의 용도로 사용하여 회사에 재산상 손해를 입혀서는 아니 된다.

제 11조 [투명한 회계 관리]

임직원은 관련 법령과 일반적으로 인정된 회계원칙 등에 따라 사실에 근거하여 정확하고 투명하게 회계를 기록, 관리하여야 한다.

제 12조 [인사 청탁 등의 금지]

1. 임직원은 자신의 승격, 이동, 보직 등 인사에 관하여 부당한 영향을 미치기 위하여 타인으로 하여금 인사업무를 담당하는 자에게 청탁하게 하여서는 아니 된다.
2. 직위를 이용하여 다른 임직원의 승격, 이동, 보직 등 인사에 부당하게 개입해서는 아니 된다.

제 3장 부당 이득의 수수 금지 등

제 13조 [이권 개입 등의 금지]

임직원은 직위를 이용하여 부당한 이익을 얻거나 타인이 부당한 이익을 얻도록 해서는 아니 된다.

제 14조 [직위 등의 사적 이용 금지]

임직원은 직무의 범위를 벗어나 사적 이익을 위하여 회사의 명칭이나 직위를 공표·게시하거나 이를 이용하거나 타인으로 하여금 그러한 행위를 하게 하여서는 아니 된다.

제 15조 [알선·청탁 등의 금지]

1. 임직원은 자기 또는 타인의 부당한 이익을 위하여 다른 직원의 공정한 직무수행을 해치는 알선, 청탁 등을 해서는 아니 된다.
2. 임직원은 직무수행과 관련하여 자기 또는 타인의 부당한 이익을 위하여 직무 관련자를 다른 직무관련자에게 소개해서는 아니 된다.
3. 임직원은 자신과 주변에 대한 부패개연성을 항상 점검하고 부패 유혹으로부터 자신을 지키기 위하여 노력하여야 한다.

제 16조 [미공개정보 이용 행위의 금지]

임직원은 내부정보를 적법한 절차에 따라 공개되기 전까지는 회사 외부의 누구에게도 누설하여서는 아니 된다.

HWASHIN

㈜화신 윤리강령

제 17조 [직무관련 정보를 이용한 거래 등의 제한]

1. 임직원은 직무수행 중 알게 된 내부정보를 이용하여 유가증권, 부동산 등과 관련된 재산상 거래 또는 투자를 하거나 타인에게 그러한 정보를 제공하여 재산 상 거래 또는 투자를 돕는 행위를 해서는 아니 된다.
2. 직무 관련 정보라 함은 다음 각 호에 해당하는 정보를 말한다.
   1) 기술개발 관련 정보
   2) 대내 · 외 사업 관련 정보
   3) 판매, 공사, 용역, 구매 등 각종 계약 관련 정보
   4) 업무수행 중 취득한 개인정보

제 18조 [내부자의 단기투자 및 공매도 금지]

1. 자본시장과 금융투자업에 관한 법률 및 기업공시규정에 의거 회사의 미공개 중요 정보를 알 수 있는 임직원은 회사 증권에 대한 단기 투자(회사 주식 등을 6 월 이내에 매수 후 매도하거나, 매도 후 매수하여 차익이 발생한 거래) 행위를 해서는 아니 된다.
2. 임직원은 회사 유가증권 중 자신이 소유하지 아니한 것을 공매도하여서는 아니 된다.

제 19조 [회사 자산의 사적 사용, 수익 금지]

1. 임직원은 회사의 자산을 사업 활동 및 승인된 목적으로만 사용해야 한다.
2. 임직원이 제1항을 위반하는 경우 공용재산 사적 사용으로 취득한 경제적 이익 및 회사 자산의 취득 가액 전액을 그 비위 행위로 인한 회사의 피해액의 3배 이내에서 환수 조치할 수 있다.

제 20조 [금품 등의 수수 금지]

1. 임직원은 직무와 직간접적으로 관련하여 기부 · 후원 · 증여 등 그 명목에 관계 없이 금품 등을 받거나 요구 또는 약속해서는 아니 된다.
2. 다음 각 호의 어느 하나에 해당하면 금품 등에 해당하지 아니한다.
   1) 대표이사가 소속 직원이나 파견 직원에게 지급하거나 상급자가 위로,격려,포상 등의 목적으로 하급자에게 제공하는 금품
   2) 원활한 직무수행 또는 사교, 의례 또는 부조의 목적으로 제공되는 음식물, 경조사비, 선물 등으로서 법령에서 정하는 가액 범위 안의 금품 등
   3) 임직원과 관련된 동호회 · 동창회 · 향우회 · 친목회 · 종교단체 · 사회단체 등이 정하는 기준에 따라 구성원에게 제공하는 금품 등 및 그 소속 구성원 등 직원과 특별히 장기적 · 지속적인 친분관계를 맺고 있는 자가 질병 · 재난 등으로 어려운 처지에 있는 직원에게 제공하는 금품 등
   4) 그 밖에 사회상규에 따라 허용되는 금품 등
3. 임직원은 위 제2항 제3호에도 불구하고 특별히 장기적 · 지속적인 친분관계를 맺고 있는 자가 직무관련자 또는 직무 관련 임직원으로서 금품 등을 제공한 경우에는 그 수수 사실을 내부 신고제도를 통해 신고하여야 한다.

제 21조 [청렴한 계약의 체결 및 이행]

1. 임직원은 회사에서 시행하는 모든 공사·용역·물품구매의 입찰·계약 및 계약 이행 등에 있어서 독점규제 및 공정거래에 관한 법률, 하도급법 등 관계 법령 및 규정에서 정한 절차에 따라 공정하고 투명하게 업무를 수행해야 한다.
2. 임직원은 제1항의 업무 수행 과정에서 관계 법령 및 규정에서 정한 절차를 위반하여 거래상 우월적 지위를 이용하여 금지된 금품 등을 요구하거나 불공정한 거래 조건의 강요, 경영간섭 등 부당한 요구를 해서는 아니 된다.
3. 임직원은 하도급거래의 상대방에게 품질유지·개선 등 정당한 사유가 있는 경우를 제외하고는 그가 지정하는 물품·장비 공급 등을 매입 또는 사용하도록 강요해서는 아니 된다.

㈜화신 윤리강령

제 4장 부정한 청탁 및 뇌물 공여 금지

제 22조 [부정한 청탁 및 뇌물 공여 금지]

1. 임직원은 공직자 등에 대해 직접 또는 제3자를 통해 부정한 청탁을 하여서는 아니 된다.
2. 임직원은 공직자 등에게 금품 등을 제공하거나 그 제공의 약속 또는 의사표시를 해서는 아니 된다
3. 제2항에도 불구하고 임직원은 예외적으로 다음 각 호의 금품 등을 공직자 등에게 제공할 수 있다.
   1) 원활한 직무수행 또는 사교 · 의례 또는 부조의 목적으로 제공하는 음식물 · 경조사비 · 선물 등으로 1회에 제공되는 가액이 다음 각 목의 범위 내인 금품 등
      가. 음식물(제공자와 공직자 등이 함께 하는 식사, 다과, 주류, 음료 등을 말한다. 이하 같다)의 경우: 3만원
      나. 경조사비(축의금·조의금 등을 말한다. 이하 같다)의 경우: 5만원. 다만, 축의금·조의금을 대신하는 화환·조화는 10만원(축의금·조의금과 화환·조화를 함께 제공한 경우 그 가액을 합산하고, 이 경우 한도는 10만원으로 하되 각각의 범위를 초과해서는 안된다)
      다. 선물(금전, 유가증권, 음식물 및 경조사비를 제외한 일체의 물품을 말한다. 이하 같다)의 경우: 5만원. 다만, 농수산물 품질관리법에 따 른 농수산물 및 농수산가공품(농수산물을 원료 또는 재료의 50퍼센트를 넘게 사용하여 가공한 제품에 한정함. 이하 같다)은 10만원(선물과 농수산물·농수산가공품을 함께 제공한 경우 그 가액을 합산하고, 이 경우 한도는 10만원으로 하되 각각의 범위를 초과해서는 안된다)
      라. 음식물, 경조사비 및 선물 중 2가지 이상을 함께 제공한 경우 그 가액을 합산하고, 이 경우 그 한도는 함께 제공한 가액 범위 중 가장 높은 금액으로 하되, 가액 범위를 각각 초과해서는 안 된다.
   2) 사적 거래(증여는 제외한다)로 인한 채무의 이행 등 정당한 권원에 의하여 제공하는 금품 등
   3) 친족(「민법」 제777조에 따른 친족을 말한다)인 공직자 등에게 제공하는 금품 등
   4) 특별히 장기적 · 지속적인 친분관계를 맺고 있는 공직자 등 중에서 질병 · 재난 등으로 어려운 처지에 있는 공직자 등에게 제공하는 금품 등
   5) 공직자 등의 직무와 관련된 공식적인 행사에서 주최자가 참석자에게 통상적인 범위에서 일률적으로 제공하는 교통, 숙박, 음식물 등의 금품 등
   6) 불특정 다수인에게 배포하기 위한 기념품 또는 홍보 용품 등이나 경연 · 추첨을 통하여 받는 보상 또는 상품 등
   7) 그 밖에 다른 법령 · 기준 또는 사회상규에 따라 허용되는 금품 등
4. 임직원은 직무와 관련하여 개인, 정당 또는 정부 단체에 금품 등을 제공하거나 그 제공의 약속 또는 의사표시를 해서는 아니 된다.

제 23조 [제3자 대리인]

1. 임직원은 회사의 제3자 대리인과의 계약 체결에 앞서 제3자 대리인의 부패 이력 등에 대하여 확인하여야 하고 부적절한 자와는 계약을 체결하여서는 아니 된다.
2. 임직원은 제3자 대리인과 계약 체결을 함에 있어서 법령 및 이 강령에서 금지 하는 부패행위를 하여서는 아니 된다는 점을 계약서에 명시하여야 하고, 정기적으로 이를 확인하여야 한다.

HWASHIN

㈜화신 윤리강령

제 5 장 직장문화의 조성

제 24조 [건강한 직장문화의 조성]

1. 임직원은 건강한 직장문화를 조성하기 위해 항상 서로를 존중하고 배려해야 하며, 폭언, 욕설, 성희롱 등 개인의 기본 인권을 침해하는 행동을 해서는 아니 된다.
2. 임직원은 건강한 직장문화 조성을 위하여 노력하여야 하며 이를 위하여 과도한 음주행위 자제 등 건전생활 실천에 솔선수범하여야 한다.
3. 임직원은 인종, 국적, 성별, 연령, 학벌, 종교, 출신지역, 장애, 결혼여부 등을 이유로 차별 등을 해서는 아니 된다.
4. 회사는 세대, 국가/지역, 성별 간 정서적, 관습적, 문화적 차이를 이해하고 존중하며 이를 바탕으로 근로환경을 유지하여야 한다.

제 25조 [성희롱 금지]

1. 임직원은 상호간에 성적 유혹 및 성적 수치심을 유발시키는 다음 각 호의 해당하는 행위를 하여서는 아니 된다.
   1) 특정 신체부위를 만지거나 접촉하는 행위
   2) 음란한 농담을 하거나 음탕하고 상스러운 이야기를 하는 행위
   3) 상대방의 외모에 대해 성적인 비유나 평가를 하는 행위
   4) 음란한 사진이나 그림 등을 게시하거나 보여주는 행위
   5) 회식자리 등에서 술시중이나 춤을 강요하는 행위
   6) 기타 사회통념상 성적 수치심을 유발하는 행위

제 6 장 위반행위 신고 및 확인 권한

제 26조 [위반행위의 신고]

1. 누구든지 임직원이 이 강령을 위반한 사실을 알게된 때에 내부신고제도를 통해 내부회계감사팀 담당자에게 신고할 수 있다.
2. 내부회계감사팀 담당자는 제1항에 따른 신고 접수 후 지체없이 사실관계를 확인하고 조사에 착수하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 사실관 계에 관한 조사 없이 종결 처리할 수 있다.
   1) 신고대상이 아니거나 위반의 정도가 경미하여 조사의 실익이 없는 경우
   2) 신고내용이 모호하고 증거가 불충분하여 사실 확인이 불가능한 경우
   3) 이미 신고되어 처리결과를 통지 받은 사안에 관하여 정당한 사유 없이 다시 신고가 된 경우
   4) 정부기관 또는 감독당국에 의한 조사가 이미 시작되었거나 완료된 경우
3. 내부회계감사팀 담당자는 제1항에 따른 신고의 사실 여부 확인을 위하여, 직접 조사하거나 외부 변호사, 회계사 등 전문가에게 조사를 의뢰할 수 있다.
4. 내부신고제도를 통해 신고한 신고인과 신고내용에 대하여는 법률상 허용되는 범위 내에서 비밀을 보장하여야 하며, 신고인이 신고에 따른 불이익을 받지 아니하도록 하여야 한다.
5. 제1항에 따른 신고를 이유로 신고인에게 차별적 취급을 가한 자는 해고 등을 포함하여 징계의 대상이 된다.
6. 차별적 취급을 받은 신고인은 대표이사에게 보호조치 및 차별적 취급의 구제 등을 요청할 수 있으며 차별적 취급이 발생할 시 대표이사는 신속히 그 경위를 조사하여 그에 필요한 적절한 조치를 취하여야 한다.

㈜화신 윤리강령

제 27조 [위반에 대한 징계]

1. 회사는 이 규정을 위반하거나 임직원의 위반 사실을 묵인 또는 방조하는 임직원에 대해서는 징계 등 필요한 조치를 취할 수 있다.
2. 징계 등에 관한 사항은 「인사규정」 등 관련 사규가 정하는 바에 따른다.

제 28조 [위반행위의 예방 확인 권한]

회사는 관련 법령에서 허용하는 범위에서 임직원의 이메일, 인터넷 사용, 컴퓨터 파일을 포함, 회사 내 보관되어 있는 모든 물품 및 기록을 확인할 수 있으며 부적절한 자산/자원 사용, 기록 현황 등을 파악 및 방지하고 법률, 강령, 다른 회사 정책 위반 사실을 확인할 수 있는 권한을 가진다.

부칙

1. 이 규정은 2019년 12월 31일부터 시행한다.

㈜화신 협력사 행동규범

화신에 재화와 용역을 제공하기 위해 계약을 체결한 모든 협력사는 본 행동규범을 준수해야 한다
또한 모든 협력사의 거래업체 등이 본 행동규범에서 제시하는 사항을 준수하도록 권고할 수 있다.

최근 자동차 산업은 미래지향적인 혁신이 진행 중이며 화신은 지속가능한 협력관계를 통해 산업의 변화를
극복하고자 한다 본 행동규범은 모든 협력사에게 기업경영과 관련된 윤리 환경 노동 인권 안전 보건
운영시스템 각 부분을 적절하게 운영하도록 요구한다 화신의 모든 협력사가 본 행동규범을 준수하여
동반 성장할 수 있도록 노력한다.

협력사의 행동규범 준수에 대해 화신은 운영상 발견된 문제점에 대한 개선을 권고할수 있으며 협력사는 협의를
통해 문제점 개선계획 수립 및 조치를 취한다 본 행동규범은 협력사와의 지속가능한 공급망 구축을 위해
정기적으로 검토하여 보완 및 개정될 수 있다.

1. 윤리

1) 투명경영
① 협력사의 임직원은 뇌물수수 횡령 청탁 알선 등을 해서는 아니되며 업무상 지위를 이용하여 부당한 대가를 의도해서는 안된다.

2) 불공정 거래 방지
① 협력사는 공정한 거래 행위를 하며 상생관계를 추구한다.

② 협력사는 시장적 지위를 이용하여 공정한 경쟁을 저해하는 행위를 하지 않는다.

③ 협력사는 부정하게 정보를 획득한 경우 부당하게 사용하거나 공개해서는 안된다.

3) 정보보호
① 협력사는 보안이 요구되는 정보를 유출하지 않고 허가나 승인 없이 보관이나 사용을 하는 행위는 하지 않는다.

② 협력사는 거래업체가 보유한 지식재산권을 존중해야 하며 적절한 조치를 통해 보호해야 한다.

4) 위조부품 방지
① 협력사는 승인된 원재료와 부품 등을 생산, 사용해야 하며 승인되지 않은 원재료를 이용하여 부적합한 방식으로 생산된 부품은 사용 또는 판매하지 않는다.

② 협력사는 위조부품 생산 및 사용 방지를 위해 주기적으로 발생 가능한 위험을 확인하며, 관련 문제가 확인될 경우 고객사에 관련 내용을 즉각 통보해야 한다.

③ 협력사는 생산한 원재료 및 부품 등이 목적 또는 조건 등에 적합하게 사용되고 있는지 확인해야 한다.

5) 수출제한 준수

① 협력사는 수출제한과 관련된 국가별 법률 및 규악을 준수해야 한다.

② 협력사는 수출제한, 경제 제재에 해당되는 국가, 지역, 개인 등과 거래하지 않는다.

③ 협력사는 수출제한 관련 내용을 준수하기 위해 주기적으로 확인해야 하며, 화신의 현황 파악이 필요한 경우 적극 협조해야 한다.

HWASHIN

㈜화신 협력사 행동규범

2. 환경

1) 환경경영체계
① 협력사는 사업장의 환경경영을 위해 현황 점검 및 성과관리 등 전반적인 운영프로세스를 관리하도록 한다.

2) 온실가스 관리
① 협력사는 온실가스 배출 저감을 위한 체계를 구축한다.

② 협력사는 에너지의 효율적 사용을 위해 온실가스 배출에 대한 모니터링을 강화한다.

3) 용수/폐수 관리
① 협력사는 용수를 적절하게 사용할 수 있게 정기적으로 설비를 점검한다.

② 협력사는 용수의 효율적 사용을 위해 모니터링을 강화한다.

4) 폐기물 관리
① 협력사는 폐기물의 효율적인 처리를 위한 체계를 구축한다.

② 협력사는 폐기물을 적법하게 처리하고 자체적으로 실적을 관리한다.

3. 노동/인권

1) 차별금지
① 협력사는 성별,인종,민족,국적,종교,장애,나이,가족관계,사회적 신분 및 정치적 견해 등을 이유로 차별적인 대우는 하지 않는다. 개인의 존엄성과 다양성을 존중하며 모든 이들의 기본적인 권리를 존중한다.

② 협력사는 임직원 채용 시 직무수행과 무관한 조건은 요구하지 않는다.

2) 복리후생
① 협력사는 쾌적한 업무환경을 제공하며 삶의 질을 높이는 제도를 운영한다.

② 협력사는 임직원의 역량강화를 위해 교육을 실시하도록 노력하며 법률에서 제시하는 의무 교육을 준사하여 실시한다.

3) 인도적 대우
① 협력사는 임직원의 사생활을 존중하고 부당하게 침해해서는 안된다.

② 협력사는 업무시간 이외에 불필요한 지시를 하지 않으며 신체적 정신적 고통을 주지 않으며 직장 내 괴롭힘을 금지해야 한다 직장 내 괴롭힘에 따른 피해가 발생할 경우 필요한 조치를 취한다.

4) 근로시간
① 협력사는 법정 근로시간을 준수해야 하며 초과근무의 경우 정당한 수당을 지급한다.

② 협력사는 임직원에게 휴일을 보장해야 하며 근로시간을 관리해야 한다.

5) 노동법 준수
① 협력사는 법률에 따라 어떠한 형태의 아동노동도 금지해야 한다.
아동노동과 관련된 위반사항 발생시 거래업체와의 거래를 중단하며 적절한 조치를 취한다.
② 협력사는 법률에 따라 어떠한 형태의 강제노동도 금지해야 한다.
임직원의 개인정보를 이용한 강제노동은 금지하며, 위반 사항 발생 시 적절한 조치를 취한다.

6) 결사의 자유
① 협력사는 임직원의 결사의 자유 및 단체 교섭 권리를 보장한다.

② 협력사는 노동조합 가입 및 활동 등의 이유로 불합리한 처우를 하지 않는다.

㈜화신 협력사 행동규범

4. 안전/보건

1) 안전 · 보건체계
① 협력사는 안전 및 보건사고를 예방하기 위해 계획, 절차, 결과 등의 체계를 운영한다.
② 협력사는 법률 및 규정에 따라 사업장 운영에 필요한 안전 · 보건 인허가를 취득 및 유지해야 한다.

2) 설비 등의 안전 관리
① 협력사는 사업장 내 안전에 유의해야할 기계나 설비 등에 대해 정기적으로 점검을 한다.
② 협력사는 사업장 내 설비관련 안전사고 예방을 위한 보호장치 및 안전장치를 설치한다.

3) 사고 관리
① 협력사는 산업재해나 질병 발생을 모니터링 할 수 있는 시스템을 구축한다.
② 협력사는 산업재해나 질병이 발생한 경우 원인 파악을 통해 개선방안을 마련한다.

4) 보건
① 협력사는 임직원을 대상으로 건강검진을 정기적으로 실시한다.
② 협력사는 임직원을 대상으로 식당 휴게공간 등을 제공하고 해당 시설을 청결하게 유지하기 위해 노력한다.

운영시스템

1) 행동규범 공유
① 협력사는 행동규범과 상응하는 사회적 책임 의지를 신년사 사내게시판 및 그룹 홈페이지 등을 통해 공유해야 한다.
② 협력사는 행동규범과 상응하는 사회적 책임 의지를 대내 외에 전파해야 한다.

2) 사내소통
① 협력사는 행동규범의 사항과 관련 법률 및 규정 제도에 대해 임직원에게 전파 및 교육을 실시한다.

3) 정보관리
① 협력사는 행동규범에 명시되는 각 분야의 현황과 문제점 관련 정보를 기록하고 관리한다.

4) 신고제도 운영
① 협력사는 임직원이 행동규범 각 분야의 위반 사실을 제보하는 경우 관련 사실을 처리할 제도를 운영해야 한다.
② 협력사는 임직원이 신고한 경우 불합리한 조치를 받지 않도록 하고 신고자의 신분을 철저히 보장해야 한다.

5) 규범 준수
① 협력사는 본 행동규범의 준수 여부를 적절한 문서로 관리하며 사실을 기반으로 작성한다.
② 협력사는 본 행동규범을 적절하게 준수하기 위한 실행계획 및 운영 중 문제점에 대한 개선계획을 수립하여 이행한다.

㈜화신 공정거래 및 동반성장 협약

1. 목적

주식회사 화신(이하 "당사" 라 함)과 거래를 시작하는 기업(이하 "협력사" 라 함)이 계약 체결에 있어 상호 준수해야 할 내용을 제시함으로써 합리적이고 공정한 거래관행을 구축함을 목적으로 한다.

2. 적용범위

당사와 협력사의 계약 체결 관련 인프라 구축과 계약 체결 및 그 이행에 대하여 적용한다.

3. 계약 체결 인프라

3.1 업체선정방식

당사의 협력사 POOL에 신규 등록한 업체는 기본거래계약 체결 후 신규부품 개발 시 품목 별로 업체 선정을 거쳐 개발업체로 선정되어야 당사와 거래를 개시하게 되며 업체선정방식에는 아래의 3가지가 있다.

업체 선정 방식		정의	선택 기준
1	심의 경쟁 구매	사전에 정해진 협력사 POOL의 소싱그룹 별로 입찰을 실시하여 업체선정평가표에 의거한 심의를 통해 외주부품업체를 선정하는 것	자동차의 성능과 직접적으로 관련되어 제조사의 설계 및 개발능력에 따라 품질이 크게 달라지는 부품
2	가격 경쟁 구매	사전에 정해진 협력사 POOL의 소싱그룹 별로 입찰을 실시하여 원칙적으로 최저가 견적제출업체를 외주부품업체로 선정하되, 업체 생산 및 공급 대응 능력을 감안하여 외주부품업체를 선정하는 것	심의경쟁구매에 따라 특정업체에 수주가 집중되어 협력사 운영정책 및 제품 개발 일정/품질 등에 문제가 예상되는 부품
3	전략 구매	경쟁구매절차에 의하지 않고 특정업체에 대하여 개발타당성과 가격만을 확인한 후 업체를 선정하는 것	고객의 요청에 의한 경우, 특허 및 특수공법업체 또는 독과점업체 기타 특정 전문업체의 선정이 필요한 경우

3.2 PRM(Partner Relationship Management)

3.2.1 당사는 협력사와의 정보 공유 및 상생협력을 위하여 KMS를 운영한다.

※ KMS(Knowledge Management System): kms.hwashin.co.kr

3.2.2 당사는 협력사 간의 정보 교류 및 상생협력을 지원하기 위하여 당사의 수탁기업협의체인 협력사 협의회(협력회) 활동을 지원한다.

3.3 거래희망업체의 제안제도

당사는 당사와의 거래를 원하는 신규업체에 대해 직접 제안을 할 수 있는 현장설명회를 운영한다.

3.4 중소기업 지원조직 운영

당사는 협력사에 대한 품질·기술 육성, 자금 지원, 교육 훈련 등의 상생협력을 위하여 관련주관부서 내에 전담조직인 상생협력추진팀을 운영한다.

4. 계약 체결 시 준수사항 및 금지사항(자기결정권이 보장된 계약 체결)

4.1 당사와 협력사는 계약 체결에 있어 다음과 같은 사항을 준수하여야 한다.

4.1.1 서면의 사전발급

가. 사전에 계약서를 발급하는 것을 원칙으로 하되 최소한 납품 등을 위한 작업에 착수하기 전에 기명날인이 있는 계약서를 발급하여야 한다.

나. 계약서에는 하도급대금과 그 지급방법 등 하도급계약의 내용과 원자재 가격 변동에 따른 하도급대금의 조정 요건, 방법 및 절차 등 하도급거래공정화에 관한 법률(이하 "하도급법" 이라 함) 시행령에서 규정하고 있는 내용이 반드시 포함되어야 한다.

다. 납품이 빈번한 거래인 경우에는 기본계약서를 먼저 발급한 후 각각의 납품에 대해서 당사가 교부한 발주서(전산발주서 포함)를 개별계약으로 갈음한다.

라. 통상 허용되는 기간보다 현저히 짧은 기간 내에 추가로 요구할 경우에는 주요 내용에 대해 사전에 서면으로 합의하여야 한다.

㈜화신 공정거래 및 동반성장 협약

4.1.2 합리적인 산정방식에 의한 단가 결정

가. 부품의 단가는 수량, 품질, 사양, 납기, 대금지급방법, 재료가격, 노무비 또는 시가의 동향 등을 고려하고 적정한 관리비 및 이익을 가산한 합리적인 산정방식에 따라 협의하여 결정하여야 한다.

나. 위 가.에서 정한 단가에는 별도의 약정이 없는 한 상호 협의하여 정하는 납품장소까지의 포장비, 운임, 하역비 및 보험료 기타 일체의 비용을 포함한다.

다. 계약기간 중 최초 단가에 변경사유가 발생한 때에는 상대방에게 단가조정신청을 할 수 있으며 이 경우 신청일로부터 30일(30일 연장 가능) 이내에 상호 협의하여 다시 정하여야 한다.

라. 단가 결정이 특별한 사유로 인하여 지연될 경우에는 협의하여 정한 임시단가를 적용하되, 이 경우 임시단가와 확정단가의 차액은 확정단가를 정하는 때에 소급하여 정산하여야 한다.

마. 원가산정에 있어 기준이 되는 임률을 정기적으로 조사하여 현실에 맞는 단가를 제시하되, 동종업계의 인건비를 고려하여 작업여건, 협력사 규모, 기술수준 등 업체별 특성에 따른 임률을 책정하여야 한다.

바. 최초 정해진 단가가 변경될 때 당사자간 협의할 수 있는 기준 및 절차를 계약서에 규정하여야 한다.

사. 단가변경의 사유(물가, 원자재 가격, 환율 변화 등), 협의기간, 대금지급조건 등 구체적인 내용을 적시하여야 한다.

4.1.3 명확한 납기

가. 당사는 업종별 특성을 고려하여 정상적인 관행에 적합한 납기를 협력사와 충분한 협의를 거쳐 결정하여야 한다.

나. 계약 체결 시 납기를 정하고 납기를 변경할 경우 이를 명확히 하여야 하며, 긴급발주 등의 명목으로 평소보다 짧은 납기를 정할 경우에는 협력사와 협의를 거쳐 합의하여야 한다.

다. 당사는 협력사에 책임을 돌릴 사유가 없음에도 불구하고 부당한 수령지연 또는 거부로 인하여 협력사가 손해를 입은 경우에는 이를 배상하여야 한다.

4.1.4 객관적 검사기준

가. 발주부품에 대한 검사에 있어 협력사와 협의하여 객관적이고 공정·타당한 검사의 기준 및 방법을 정하여야 한다.

나. 납품 등이 있는 때에는 검사 전이라도 즉시 수령증을 교부하여야 하며, 검사는 미리 정한 검사규정 및 절차에 따라 신속히 실시하여야 한다.

다. 정당한 사유가 있는 경우를 제외하고는 협력사로부터 발주부품을 수령한 날로부터 10일 이내에 검사결과를 통지하여야 한다.

라. 검사 전 또는 검사기간 중의 발주부품에 대하여 선량한 관리자의 주의를 가지고 관리하여야 한다.

4.1.5 합리적인 대금 지급 기일 결정

가. 협력사에 제조 위탁을 하는 경우에는 발주부품의 수령일(납품 등이 빈번하여 월 1회 이상 세금계산서의 발행일을 정한 경우에는 그 정한 날을 말한다 이하 같다)부터 60일 이내의 가능한 짧은 기한으로 정한 지급기일까지 대금을 지급하여야 한다.

나. 협력사에 제조 위탁을 한 경우로서 발주자로부터 제조행위의 완료에 따라 준공금 등을 받은 때에는 대금을 그 지급받은 날부터 15일(대금의 지급기일이 그 전에 도래하는 경우에는 그 지급기일) 이내에 지급하여야 한다.

다. 제조행위의 진척에 따라 기성금 등을 받은 때에는 협력사가 위탁 받은 과업을 수행한 부분에 상당한 금액을 그 지급받은 날부터 15일(대금의 지급기일이 그 전에 도래하는 경우에는 그 지급기일) 이내에 지급하여야 한다.

라. 대금을 지급함에 있어서는 발주자로부터 당해 제조 위탁과 관련하여 지급 받은 현금비율 이상으로 지급하여야 한다.

마. 당사는 협력사에 하도급대금을 어음으로 지급하는 경우 당해 제조 위탁과 관련하여 발주자로부터 교부 받은 어음의 지급기간(발행일로부터 만기일까지) 내의 어음을 교부하여야 한다.

바. 당사가 하도급대금을 어음으로 지급하는 경우에 그 어음은 법률에 근거하여 설립된 금융기관에서 할인이 가능한 것이어야 하며, 어음을 교부한 날로부터 어음의 만기일까지의 기간에 대한 할인료(공정위가 정하여 고시하는 할인율)를 어음을 교부하는 날에 협력사에 지급하여야 한다. 다만, 발주부품의 수령일로부터 60일 이내에 어음을 교부하는 경우에는 발주부품의 수령일로부터 60일을 초과한 날 이후 만기일까지의 기간에 대한 할인료를 발주부품의 수령일로부터 60일 이내에 협력사에 지급하여야 한다..

㈜화신 공정거래 및 동반성장 협약

사. 당사가 하도급대금을 어음대체결제수단을 이용해 지급하는 경우 지급일(기업구매전용카드의 경우는 카드결제승인일을, 외상매출채권담보대출의 경우는 납품 등의 내역전송일을, 구매론의 경우는 구매자금결제일을 말한다)부터 하도급대금 상환기일 까지의 기간에 대한 수수료(대출이자를 포함한다)를 지급일에 협력사에 지급하여야 한다. 다만, 발주부품의 수령일로부터 60일 이내에 어음대체결제수단을 이용하여 지급하는 경우에는 발주부품의 수령일로부터 60일을 초과한 날 이후 하도급대금 상환기일까지의 기간에 대한 수수료를 발주부품의 수령일로부터 60일 이내에 협력사에 지급하여야 한다.

아. 당사가 하도급대금을 발주부품의 수령일로부터 60일을 초과하여 지급하는 경우에는 그 초과기간에 대하여 공정위가 정하여 고시하는 이율에 의한 이자를 지급하여야 한다.

4.1.6 납품 이후 발견되는 하자에 대한 합리적인 반품 처리

납품 이후 발견되는 불합격품에 대해서는 불합격 원인을 규명하고 그에 따른 책임부담비율 등을 규정하여 당사와 협력사의 합의에 의하여 반품 처리한다. 세부기준은 클레임보상협정서에 의한다.

4.1.7 계약 해제・해지

가. 사유는 당사와 협력사 간의 합의에 의해 정하고 '최고 없이 가능한 경우'와 '최고가 필요한 경우'를 구분하되, 해제・해지사유가 발생한 경우에는 서면으로 지체 없이 통보하여야 한다.

나. 최고 없이 가능한 경우는 다음과 같으며, 이 경우에는 당사 또는 협력사는 본 계약 또는 개별계약에 대하여 그 전부 또는 일부를 해제・해지할 수 있다.

① 상대방이 금융기관으로부터 거래정지처분을 받거나, 감독관청으로부터 영업취소, 영업정지 등의 처분을 받은 경우

② 상대방이 어음・수표의 부도, 제3자에 의한 강제집행(가압류 및 가처분 포함), 파산, 화의개시 및 회생절차의 신청 등 영업상의 중대한 사유가 발생하여 계약 내용을 이행할 수 없다고 인정될 경우

③ 상대방이 해산, 영업의 양도 또는 타 회사로의 합병을 결의한 경우

④ 상대방이 재해 기타 사유로 인하여 기본계약 또는 개별계약의 내용을 이행하기 곤란하다고 쌍방이 인정한 경우

다. 최고가 필요한 경우는 다음과 같으며, 이 경우에는 상대방에게 1개월 이상의 기간을 정하여 그 이행을 최고하고, 그 기간 내에 이행하지 아니한 때에 본 계약 또는 개별계약의 전부 또는 일부를 해제・해지할 수 있다.

① 상대방이 본 계약 또는 개별계약의 중요한 내용을 위반한 경우

② 당사가 정당한 사유 없이 발주부품의 제작에 필요한 사항의 이행을 지연하여 협력사의 작업에 지장을 초래한 경우

③ 협력사가 정당한 사유 없이 발주부품의 제작을 거부하거나 착수를 지연하여 납기 내에 납품이 곤란하다고 인정되는 경우

④ 협력사의 기술, 생산 및 품질관리능력이 부족하여 계약 내용을 원만히 이행할 수 없다고 인정되는 상당한 이유가 있는 경우

4.2 당사와 협력사는 계약 체결에 있어 다음과 같은 사항은 지양하여야 한다.

4.2.1 서면을 발급하지 않거나 보존하지 않는 행위

가. 정당한 사유 없이 위탁시점에 확정하기 곤란한 사항에 대하여 해당사항을 기재하지 아니한 서면을 발급하면서 해당사항이 정하여지지 아니한 이유, 그 사항을 정하게 되는 예정기일을 기재하지 않고 발급하는 행위

나. 일부사항을 기재하지 아니한 서면을 발급한 이후 해당사항이 확정되었음에도 불구하고 협력사에 새로운 서면을 지연 발급하거나 발급하지 아니하는 행위

다. 구두위탁(발주)한 내용에 대해 협력사로부터 위탁한 작업의 내용, 하도급대금, 위탁일시 등 위탁 내용의 확인을 요청 받고도 15일 이내에 인정 또는 부인 의 의사를 서면으로 회신하지 아니하는 행위

라. 구두위탁(발주)한 내용에 대해 위탁 내용의 인정 또는 부인의 의사를 회신하면서 당사(계약담당임원 등 회사 계약 책임자)의 서명 또는 기명날인을 하지 아니하는 행위

마. 추가작업의 범위가 구분되고 금액이 상당함에도 이에 대한 구체적인 추가계약서나 작업지시서 등을 발급하지 아니한 행위

바. 법정서류를 3년간 보존하지 아니하고 당사의 규정 등에 따라 임의적으로 3년 이내 폐기하는 행위

사. 거래종료일로부터 3년간 서면(서류)을 보존하고 있으나 허위 서면(서류)이거나 허위 내용의 서류를 사후 작성하여 보존하는 행위

아. 입찰내역서, 낙찰자 결정품의서, 견적서 등 하도급대금 결정과 관련된 서류를 보존하지 아니하는 행위

㈜화신 공정거래 및 동반성장 협약

4.2.2 부당한 하도급대금 결정행위

가. 정당한 이유 없이 일률적인 비율로 단가를 인하하여 하도급대금을 결정하는 행위

나. 협조 요청 등 명목 여하를 불문하고 일방적으로 일정금액을 할당한 후 당해 금액을 감하여 하도급대금을 결정하는 행위

다. 정당한 이유 없이 특정 협력사를 차별취급 하여 대금을 결정하거나, 협력사와의 합의 없이 일방적으로 낮은 단가에 의하여 대금을 결정하는 행위

라. 발주량 등 거래조건에 대하여 착오를 일으키게 하거나 다른 사업자의 견적 또는 거짓견적을 내보이는 등의 방법으로 협력사를 기만하고 이를 이용하여 대금을 결정하는 행위

마. 경쟁입찰에 의하여 계약을 체결함에 있어서 정당한 사유 없이 최저가로 입찰한 금액보다 낮은 금액으로 대금을 결정하는 행위

바. 자재의 가격 하락 및 노임 하락 등 객관적으로 타당한 단가인하 사유가 없이 일률적으로 단가를 인하하여 대금을 결정하는 행위

사. 대금지급조건, 거래수량, 작업의 난이도 등의 차이가 없음에도 특정 협력사를 차별취급 하여 대금을 낮게 결정하는 행위

아. 다량 발주를 전제로 하여 견적하도록 한 후, 실제로는 소량 발주하면서 그 견적가격을 기준으로 대금을 결정하는 행위

자. 대금을 정하지 않은 채 제조 위탁을 한 후 협력사와 협의를 거치지 않고 통상 지급되는 대가를 하회하여 대금을 결정하는 행위

차. 납품 관련 기술자료 등을 요구하여 넘겨받은 후, 이를 다른 사업자에게 제공하고 다른 사업자의 견적가격 등을 근거로 대금을 인하하는 행위

카. 원도급 대금에 비하여 현저히 낮은 실행예산을 작성하여 같은 실행예산 범위 내로 제작하여야 함을 이유로 대금을 낮게 결정하는 행위

타. 수출, 할인특별판매, 경품류, 견본용 등을 이유로 통상 지급되는 대가보다 현저하게 하회하여 대금을 결정하는 행위

4.2.3 구두에 의한 제안서 제시 요구 혹은 개발 의뢰 행위

설비 완료 혹은 생산 준비 완료 후 개발을 취소하거나 구두로 요구시 제시한 단가를 인하할 것을 요구하는 행위

4.2.4 부당한 경영간섭 행위

가. 협력사가 임직원을 선임·해임함에 있어 자기의 지시 또는 승인을 얻게 하거나 협력사의 의사에 반하여 특정인을 채용하게 하는 등의 방법으로 인사에 간섭하는 행위

나. 재하도급거래에 개입하여 자신의 위탁한 발주부품의 품질 유지 및 납기 내 납품 여부 등 하도급거래의 목적과 관계 없이 선정·계약조건 설정 등 재하도급거래 내용을 제한하는 행위

다. 협력사의 생산품목·시설규모 등을 제한하거나 협력사로 하여금 자신 또는 자신의 계열회사의 경쟁사업자와 거래하지 못하도록 하는 행위

라. 협력사에 납품 관련 기술자료 등을 정당한 이유 없이 요구하여 제공하도록 하는 행위

마. 경품부판매, 할인특매 등의 특별판매행사에 협력사가 참여토록 강요하거나, 상품이나 상품권 등의 구입을 강요하는 행위

4.2.5 설계 변경 등에 따른 하도급대금의 미조정 행위

가. 발주자로부터 설계 변경 또는 경제상황의 변동 등을 이유로 추가금액을 수령하고도 이를 지급하지 아니하거나 또는 받은 비율이나 내용보다 적게 지급하는 행위

나. 발주자로부터 설계 변경 또는 경제상황의 변동 등을 이유로 계약금액을 조정 받고도 30일을 초과한 날까지 증액 또는 감액하지 아니하거나 30일을 초과하여 조정하는 행위

다. 발주자로부터 설계 변경 또는 경제상황의 변동 등을 이유로 추가금액을 수령한 날부터 15일이 지난 후에 대금을 현금 또는 어음이나 어음대체결제수단을 이용하여 지급하면서 그 초과기간에 대한 지연이자, 어음할인료, 수수료를 지급하지 아니하는 행위

라. 설계 변경 또는 경제상황의 변동 등의 사유로 발주자로부터 계약금액을 증액 또는 감액 받고도 받은 날부터 15일 이내에 증액 또는 감액 받은 사유와 내용을 협력사에 통지(발주자가 직접 통지한 경우 제외)하니 아니하는 행위

㈜화신 공정거래 및 동반성장 협약

4.2.6 원재료 가격 변동에 따른 하도급대금의 미조정 행위
가. 협의신청에 응답하지 않거나 협의를 개시하겠다고 통보한 후 회의 개최, 의견 교환, 단가조정안 제시 등 실질적인 협의절차를 진행하지 아니하는 행위
나. 협의를 신청한 후 30일이 경과하였음에도 불구하고, 실질적인 단가 조정 권한을 가지고 있는 책임자가 협의에 임하지 아니하는 행위
다. 단가 조정을 위한 시장조사, 원가 산정 등 객관적 근거 없이 상대방이 수용할 수 없는 가격을 되풀이하여 제시하는 행위

4.2.7 전속적 거래 요구 행위
협력사로 하여금 자신 및 자신이 지정하는 업체와는 거래하지 못하게 하는 행위(기술 개발을 협력사와 공동으로 하는 것을 이유로 협력사와 전속적 거래에 합의하는 경우를 제외)

4.2.8 부당특약 행위
가. 협력사의 이익을 부당하게 침해하거나 제한하는 계약조건을 설정하는 행위
나. 계약에 기재되지 아니한 사항을 요구함에 따라 발생된 비용을 협력사에 부담시키는 약정을 설정하는 행위
다. 당사가 부담하여야 할 민원 처리, 산업재해 등과 관련된 비용을 협력사에 부담시키는 약정을 설정하는 행위
라. 입찰내역에 없는 사항을 요구함에 따라 발생된 비용을 협력사에 부담시키는 약정을 설정하는 행위

5. 계약 이행 시 준수사항 및 금지사항(계약서 및 관련 법령에 의한 충실한 계약 이행)

5.1 당사와 협력사는 계약 이행에 있어 다음과 같은 사항을 준수하여야 한다.

5.1.1 민법 등 관련 법령의 준수
신의성실의 원칙, 하도급법, 공정거래법 등 관련 법령을 준수하되, 분쟁 발생 시 서면 자료에 의해서 해결하여야 한다

5.1.2 단가 인하 시 사전 충분한 합의 및 서면 발급
원자재 가격 하락, 물량 증대 등을 이유로 한 단가인하의 경우 물량 증대에 따른 단가인하폭에 대한 합리적인 근거를 제시하여야 한다.

5.1.3 계약 변경에 따른 대금 조정
추가적인 사양 요구 등 계약 변경으로 인해 추가비용이 소요될 경우 그에 따른 대금을 지급하여야 한다.

5.2 당사와 협력사는 계약 이행에 있어 다음과 같은 사항은 지양하여야 한다.

5.2.1 부당한 수령거부 행위
가. 위탁내용이 불명확하여 납품한 발주부품의 내용이 위탁내용과 상이한지 판단이 곤란함에도 불구하고 수령을 거부하는 행위
나. 발주자・외국수입업자・고객의 클레임, 판매 부진 등을 이유로 이미 위탁한 물품의 수령을 거부하는 행위
다. 공급하기로 되어 있는 원자재 등을 늦게 공급함으로써 납기 내 납품이 불가능함에도 납기 지연을 이유로 수령을 거부하는 행위
라. 검사기준을 정하지 아니하고도 통상의 기준보다 높은 기준을 적용하는 행위
마. 검사기준을 정하였다고 하더라도 내용이 불분명하거나 당초계약에서 정한 검사기준보다 높은 기준을 적용하여 수령을 거부하는 행위
바. 협력사로부터 납품 등의 수령 요구가 있었음에도 보관장소 부족 등 정당한 이유 없이 수령을 거부하는 행위
사. 협력사의 부도 등에 따라 안정적인 공급이 어렵다고 판단해서 이미 발주한 물품의 수령을 임의로 거부하는 행위
아. 여러 품목을 제조 위탁하고 일부 품목의 불량을 이유로 다른 품목에 대하여도 수령을 거부하거나, 발주자의 발주 취소 또는 발주 중단 등을 이유로 수령을 거부하는 행위

5.2.2 부당 반품 행위
가. 거래상대방으로부터의 발주 취소 또는 경제상황의 변동 등을 이유로 반품하는 행위
나. 검사의 기준 및 방법을 불명확하게 정함으로써 부당하게 불합격으로 판정하여 이를 반품하는 행위
다. 공급한 원재료의 품질 불량으로 인하여 불합격품으로 판정되었음에도 불구하고 이를 반품하는 행위
라. 원재료 공급 지연에 의한 납기 지연임에도 불구하고 이를 이유로 반품하는 행위
마. 이미 수령한 물품을 발주자・외국수입업자・고객의 클레임, 판매 부진 등을 이유로 반품하는 행위
바. 협력사 이외의 제3자에게 검사를 위탁한 경우로서 협력사가 제3자의 검사를 필하여 납품하였음에도 이를 반품하는 행위
사. 협력사의 납기 지연이 있었으나 이를 용인한 객관적 사실이 있었음에도 이를 수령한 후 납기 지연을 이유로 반품하는 행위

㈜화신 공정거래 및 동반성장 협약

5.2.3 부당한 대금 감액 행위
가. 정당한 사유에 대한 입증 및 다음 각 호의 사항을 기재한 서면 교부 없이 계약 시 정한 대금을 감액하는 행위
① 감액 사유 및 기준
② 감액 물량, 금액, 감액방법
나. 위탁할 때 대금을 감액할 조건 등을 명시하지 아니하고 위탁 후 협조 요청 또는 거래상대방으로부터의 발주 취소, 경제상황의 변동 등 불합리한 이유를 들어 대금을 감액하는 행위
다. 단가인하에 관한 합의가 성립한 경우 당해 합의 성립 전에 위탁한 부분에 대하여도 일방적으로 이를 소급 적용하는 방법으로 대금을 감액하는 행위
라. 대금을 현금으로 또는 지급기일 전에 지급함을 이유로 과다하게 대금을 감액하는 행위
마. 손해 발생에 실질적 영향을 미치지 아니하는 경미한 협력사의 과오를 이유로 일방적으로 대금을 감액하는 행위
바. 제조에 필요한 물품 등을 자기로부터 사게 하거나 자기의 장비 등을 사용하게 한 경우에 적정한 구매대금 또는 사용대가 이상의 금액을 대금에서 공제하는 행위
사. 대금 지급시점의 물가나 자재가격 등이 납품 등의 시점에 비하여 떨어진 것을 이유로 대금을 감액하는 행위
아. 경영적자 또는 판매가격 인하 등 불합리한 이유로 부당하게 대금을 감액하는 행위
자. 당초 계약내용과 다르게 간접노무비, 일반관리비, 이윤, 부가가치세 등을 감액하는 행위
차. 고용보험 및 산업재해보장보험의 보험료 징수 등에 관한 법률, 산업안전보건법 등에 따라 당사가 부담하여야 하는 고용보험료, 산업안전보건관리비 그 밖의 경비 등을 협력사에 부담시키는 행위
카. 자재 및 장비 등을 공급하기로 한 경우 이를 지연하여 공급하거나 사실상 무리한 납기를 정해 놓고 이 기간 내에 납품하지 못함을 이유로 감액하는 행위
타. 계속적 발주를 이유로 이미 확정된 하도급대금을 감액하거나, 총액으로 계약한 후 제조의 구체적 내역을 이유로 감액하는 행위
파. 발주부품을 저가로 수주하였다는 등의 이유로 당초계약과 다르게 대금을 감액하는 행위
하. 위탁 내용 및 조건에는 변함이 없음에도 계약을 변경하는 등 결과적으로 대금을 감액하는 행위 및 환차손 등을 협력사에 당초 계약조건과 다르게 전가시켜 대금을 감액하는 행위

5.2.4 경제적 이익의 부당요구 행위
가. 거래 개시 또는 다량거래 등을 조건으로 협찬금, 장려금, 지원금 등 경제적 이익을 요구하는 행위
나. 수익 또는 경영여건 악화 등 불합리한 이유로 협찬금, 장려금, 지원금 등 경제적 이익을 요구하는 행위
다. 기타 협력사가 부담하여야 할 법률상 의무가 없음에도 협찬금, 장려금, 지원금 등 경제적 이익을 요구하는 행위

5.2.5 자사 원인에 기인한 비용 전가행위
자사의 임금 상승, 내부적인 품의절차 지연으로 인한 비용을 협력사에 전가하는 행위

5.2.6 부당한 대물변제 행위
최초 계약과는 달리 협력사의 의사에 반하여 정해진 대금을 물품으로 지급하고 이를 받아들일 것을 요구하는 행위

5.2.7 보복 조치 행위
협력사가 공정위에 하도급법 위반으로 신고한 것을 이유로 수주 기회를 제한하거나 거래의 정지 기타 불이익을 주는 행위

5.2.8 탈법 행위
가. 하도급거래와 관련하여 우회적인 방법에 의하여 실질적으로 하도급법의 적용을 면탈하려는 행위
나. 공정위의 시정조치에 따라 대금 등을 협력사에 지급한 후 이를 회수하거나 납품대금에서 공제하는 등의 방법으로 환수하는 행위
다. 어음할인료, 지연이자 등을 협력사에 지급한 후 이에 상응하는 금액만큼 일률적으로 단가를 인하하는 행위

5.2.9 물품 등의 구매강제 행위
가. 정당한 사유 없이 자사, 계열사 또는 특정회사 등의 제품이나 서비스 등을 협력사에 강제로 판매하거나 이용하게 하는 행위
나. 정당한 사유 없이 협력사가 구매의사가 없다고 표시하였거나, 의사표시가 없어도 명확히 구매의사가 없다고 인정됨에도 재차 구매를 요청하는 행위

5.2.10 물품구매대금 등의 부당결제청구 행위
가. 협력사에 납품 등에 필요한 물품 등을 자기로부터 사게 하거나 자기 장비 등을 사용하게 하고, 대금 지급기일에 앞서 구매대금이나 사용대금의 전부 또는 일부를 지급하게 하는 행위
나. 협력사에 납품 등에 필요한 물품 등을 자기로부터 사게 하거나 자기 장비 등을 사용하게 하고 자기가 구입·사용 또는 제3자에게 공급하는 조건보다 현저하게 불리한 조건으로 지급하는 행위

㈜화신 공정거래 및 동반성장 협약

5.2.11 기술자료 제공 강요 행위

가. 정당한 사유 없이 협력사에 다음 기술자료를 자기 또는 제3자에게 제공하도록 강요하는 행위

① 상당한 노력에 의하여 비밀로 유지된 제조 수행 방법에 관한 자료

② 특허권, 실용신안권, 디자인권, 저작권 등 지식재산권과 관련된 정보

③ 그 밖에 영업활동에 유용하고 독립된 경제적 가치가 있는 기술상 또는 경영상의 정보

협력사로부터 취득한 기술자료를 자기 또는 제3자를 위해 유용하는 행위

6. 기록보존

계약 체결 및 이행과 관련한 문서는 하도급거래에서의 바람직한 서면 발급 및 보존에 관한 실천사항 규정에서 정한 바에 따라 보관, 유지한다.

7. 관련규정

하도급거래에서의 바람직한 서면 발급 및 보존에 관한 실천사항 규정

8. 첨부

해당 없음

㈜화신 책임있는 광물 구매 정책

① 배경

당사는 최근 이슈되고 있는 콩고민주공화국 코발트 광산 및 그 인근 국가에서 광물 채굴로 인해 야기되는 아동노동 착취, 인권유린, 환경파괴, 분쟁조장 등의 문제를 심각하게 인식하고 있습니다.

이에 따라 콩고민주공화국을 포함한 분쟁지역인 아프리카 10개국의 광물 채굴 과정에서 발생하는 인권침해와 환경 파괴를 근절하기 위해 함께 노력하겠습니다.

당사는 자동차용 Chassis&Body 제조 업체로서 생산제품에 분쟁/책임광물이 포함되고 있지 않지만, 글로벌 기업으로서 지속 가능한 미래를 위해 분쟁광물 정책과 관리체계를 사전 구축하여 책임있는 기업시민이 되겠습니다.

② 정의

1. 분쟁지역 : 콩고민주공화국, 수단, 르완다, 브룬디, 우간다, 콩고, 잠비아, 앙골라, 탄자니아, 중앙아프리카
2. 분쟁광물 : 주석, 탄탈륨, 텅스텐, 금
   1) 주석(Tin, 원소기호 Sn) : 전성과 연성이 뛰어난 은백색 결정성 금속으로서, 녹는점이 비교적 낮기 때문에 가공이 용이한 금속입니다. 주로 납땜에 사용되며, 현재 대부분의 전자제품 및 부품에 사용되고 있습니다.
   2) 탄탈륨(Tantalum, 원소기호 Ta) : 강회색의 단단한 금속으로 전성과 연성이 풍부하고, 철과의 합금은 인장강도가 크며, 내산성이 좋아 화학공업용 내산제의 재료로 쓰입니다. 주로 전기전자 제품, 자동차 및 항공우주 제품에 걸쳐 널리 사용되고 있습니다. 전 세계 매장량의 70-80%가 콩고민주공화국에 매장되어 있습니다.
   3) 텅스텐(Tungsten, 원소기호 W) : 굳고 단단한 백색 또는 회백색의 금속원소이며, 높은 강도와 융점을 가지고 있어 전자, 자동차 및 항공우주 제품 등에 사용되고 있습니다.
   4) 금(Gold, 원소기호 Au) : 성질이 연하여 가공하기가 쉽고 전성, 연성, 열전도율, 전기전도율 등이 우수하여 IT, 반도체, 의료용 기기 등에 사용되고 있습니다. 광택이 찬란하고 희귀하여 예로부터 귀금속의 취급을 받아 장식류로도 사용 됩니다.
3. 책임광물 : 코발트, 운모
   1) 코발트(Cobalt, 원소기호 CO) : 단단하고 광택이 나는 은회색 금속으로 주로 리튬이온 배터리에 사용됩니다.
   2) 운모(Mica) : 화강암 가운데 많이 들어 있는 규산염 광물의 하나로 주로 건설용 시멘트, 페인트, 자동차 도장 등에 주로 사용 됩니다.

③ 정책

㈜화신은 분쟁광물 이슈에 적극 대응하여 불법적으로 채굴한 광물에 대한 사용 등을 금지하는 등 윤리적인 광물 구매를 할 수 있도록 노력하고 있습니다.

이에 당사는 관련 OECD 실사지침과 같이 국제 가이드라인과 규제를 준수하여, 사용 정책을 수립하고 그에 따라 당사 뿐만 아니라 협력사들의 '책임있는 구매'까지 함께 관리하도록 하겠습니다.

1) 당사는 경영 활동과 관련하여 적용받는 법과 규제를 기반으로 분쟁광물 관련 규범 및 가이드라인을 협력사에 제공하고, 교육을 통한 인식 제고와 해당 규범 준수를 요구하겠습니다.
2) 당사와 협력사는 분쟁광물 사용현황을 지속적으로 모니터링하여 사업 운영 전반에서 발생하는 부정적 환경영향을 저감하도록 노력하겠습니다.
3) 당사는 협력사가 사용하는 분쟁광물이 인권 침해와 간접, 직접적으로 기여하지 않았는지 확인하고 조치하겠습니다.
4) 당사와 협력사는 원부자재 생산 과정에 참여하여 위험 요소를 점검 및 개선할 것을 요청하여 임직원의 안전 및 보건 증진에 노력하겠습니다.

④ 적용범위

1. 본 정책은 본사, 국내/외 법인 등 회사의 재무적 연결범위에 속하는 모든 임직원에게 적용됩니다.
2. 임직원과 내/외부 이해관계자들은 협력사를 대할 때에도 분쟁광물 정책을 준수하도록 권장합니다.

⑤ 정책 위반

당사에서 제정한 분쟁광물 정책은 당사와 관련된 다양한 이해관계자들이 함께 준수할 수 있도록 노력해야 됩니다.

해당 정책 위반사항을 발견했을 경우, 신속하게 유관부서 및 사내신문고를 통해 신고해야 되며, 사회와 환경에 부정적인 영향, 회사의 명예 실추 등과 같은 심각한 문제 야기 시 협력사와의 계약 종료까지 이어질 수 있습니다.

㈜화신 정보보안관리

1. 총칙

1.1 목적

본 규정은 주식회사 화신(이하 '당사' 라 한다)의 정보보호 관리체계(이하 'ISMS' 라 한다) 운영에 대한 업무 요건 및 절차를 규정함으로서 당사 정보보호 수준의 유지를 목적으로 한다.
본 규정은 ISMS 내 영역별 보안 요건과 프로세스의 기본 구조에 관한 사항을 정의하므로, 표준 프로세스로도 기능한다.
본 규정은 정보보호 관련 법률 및 비즈니스 보안요건 해당 시, 관련 요건을 포함한다.

1.2 ISMS 범위

본 규정은 당사의 정보 보안, 정보 보안 지역 관리 및 정보 자산의 반출입 관리, 서버 보안 관리를 효율적으로 수행하기 위한 업무내용과 처리 방법에 대하여 적용한다.

구분	범위 원칙	ISMS 전체	TISAX 대상
중요정보 범위	■ 보호대상으로 지정할 핵심 정보	■ 파트너사 제공 도면 ■ 자사 설비도면 ■ 회사 오피스 문서	■ 독일 파트너사 제공 도면
사업장 범위	■ 중요정보 생명주기 과정에 존재하는 사업장	■ 본사 포함 전 사업장 - 기술연구소 포함 - 국내공장, 해외법인 전체	
시스템 범위	■ 중요정보 생명주기 과정에 해당정보를수집,저장,처리하는 각종 시스템	■ 시스템 전체	■ 좌동
조직 범위	■ 중요정보 관련 사업장 운영 조직 ■ 중요정보 관련 시스템 운영조직 ■ 중요정보 사용조직	■ 조직 전체	■ 총무부서 ■ IT운영부서 ■ 도면 취급부서

1.3 용어의 정의

1.3.1 정보보호 기본

※ 참고 문서: ISO 27000:2014 Information security management systems - Overview and vocabulary

1) CIA (Confidentiality, Integrity, Availability: 기밀성, 무결성, 가용성)
회사가 보호대상으로 정의한 정보자산, 업무, 서비스에 대해 보호해야 할 3대 보안 속성.

2) ISMS (Information Security Management System: 정보보호 관리체계)
회사의 정보자산, 업무, 서비스의 CIA를 보호하기 위해 관리적, 기술적, 물리적 요건과 요건 수행 절차를 정의한 관리체계.

3) SoA (Statement of Applicability: 적용성 보고서)
특정 보안요건 리스트 대비 당사의 해당 여부, 적용 수준을 종합한 보고서.
국내외 인증표준 별로 각각 다음과 같은 명칭을 가진다.
① ISO 27001 인증: SOA (동일 명칭)
② 국내 ISMS-P 인증: 관리체계 운영명세서
③ TISAX: Assessment Report

4)보안 위협
시스템 또는 조직에 위해를 초래할 수 있는 사고의 잠재적 원인.

5)보안 취약점
하나 혹은 그 이상의 위협에 활용될 수 있는, 자산 또는 보안통제의 취약요소.

㈜화신 정보보안관리

6) 보안 위험
보안 취약점의 존재로 인해 보안 위협이 성공할 수 있는 가능성.
7) DoA (Degree of assurance: 위험 수용 수준)
식별한 위험요소의 조치 여부 또는 조치 수준을 결정하는 데에 참고하기 위한 수치.
당사의 상황에 따라 다양한 관점에서 정의할 수 있음.
8) 방화벽
외부에서 조직내의 컴퓨터 및 네트워크로 침입하는 것을 방지하기 위한 시스템.
9) 해킹
정보 시스템의 취약성을 이용하여 접근을 허가 받지 않는 시스템에 불법으로 침투하거나 허가되지 않는 권한을 불법으로 갖는 행위.
10) 해커
타인의 컴퓨터에 불법으로 접속하여 컴퓨터에 고장을 일으키게 하거나, 컴퓨터에 수록된 정보를 변조하거나 파괴하는 사람.
11) 스파이웨어
사용자의 동의 없이 또는 사용자를 속여 설치되어 광고나 마케팅용 정보를 수집하거나 중요한 개인 정보를 빼 가는 악의적 프로그램.
12) PMS
시스템 보안 패치, 백신 업데이트, 기타 응용프로그램 같이 특정 프로그램을 전산기기 사용자에게 강제로 배포/적용하기 위한 시스템.
13) 자산 폐기
정보를 저장한 정보 자산이나 매체의 폐기.
14) 보안 구역
정보가 보관되거나 처리되는 지역.
15) 정보 자산
정보를 관리 및 저장할 수 있는 자산 및 매체.
16) 데이터 공유
정보를 관리 및 저장하고 있는 자산 및 매체의 공유.
17) BCM (Business Continuity Management: 사업 연속성 관리)
정상 업무가 불가한 비상 상황 발생 시 평시 업무의 연속성을 유지하기 위한 절차.
18) NDA (Non-disclosure agreement: 비밀유지 협약서)
당사와 외부조직 간 업무 교류가 있는 경우, 비밀유지를 위해 체결하는 협약서.
통상적으로 임직원이 작성하는 문서는 보안서약서로, 회사 간 체결하는 협약서를 NDA로 칭한다.

1.3.2 TISAX 관련

1) TISAX (Trusted Information Security Assessment eXchange: 신뢰 가능한 보안평가 공유방식)
VDA가 개발한, 독일 자동차 기업과 거래하는 모든 벤더의 ISMS 수준 평가를 위한 정보보호 인증제도.
2) VDA (Verband Der Automobilindustrie: 독일 자동차 산업 협회)
TISAX 인증제도를 개발한 기관.
3) ENX association (European Network Exchange: 유럽 자동차 제조 협회)
VDA의 위탁에 따라 TISAX 인증제도 대행 운영 총괄하는 기관.
심사업체 인정(accreditation) 업무 담당, 수검업체 인증 결과 및 심사보고서 관리.
수검업체는 ENX 공인 심사업체(audit provider)에게 TISAX 심사를 받고, ENX로부터 인증서를 발급받는다.
4) ISA (Information Security Assessment: 보안 평가)
사전적으로는 보안 평가를 의미하나, TISAX에서는 '심사'의 의미로도 사용된다.
5) VDA-ISA
TISAX 인증을 위해 VDA가 개발한 보안평가 기준.
6) 글로벌 OE
폭스바겐, BMW 등 비즈니스 대상이 되는 글로벌 파트너기업을 칭하는 용어.

㈜화신 정보보안관리

7) 기준 카탈로그(criteria catalogue)
VDA-ISA는 총 4개 카탈로그로 구성됨.
① Information security: 정보보호 일반 카탈로그. TISAX의 최소 요구수준.
② Connection 3rd parties: 제3자 연결 카탈로그. 당사가 파트너사의 시스템을 사용하거나, 파트너사 사업장 내 출장사무소를 운영할 경우 해당되는 것을 원칙으로 함. 실제 해당 여부는 파트너사와의 협의에 따른다.
③ Data protection: 개인정보 보호 관련 카탈로그. 파트너사가 보유한 고객의 개인정보를 수탁하는 경우 해당된다.
④ Prototype protection: 차량 완제품, 구성품, 부품 등의 프로토타입 관련 카탈로그.

8) 평가목표(AO: Assessment Objective)
총 10가지 AO로 구성되어 있고, AO1은 최소 평가 범위이다.

9) 평가수준 (AL: Assessment Level)
AL2와 AL3 등 2가지로 구분한다. (AL1은 없음)
① AL2: high protection needs에 해당하는 AL.
② AL3: very high protection needs에 해당하는 AL.

10) 통제요건
각 프로세스 영역별로 필요한 통제사항을 정의한 요건을 의미한다.
강제성 수준에 따라 총 5개 유형으로 구분하고, 25번 카탈로그의 경우에 한하여 1개 유형(additional prototype)이 추가된다.
① Must (요건코드 식별자: -M)
예외 없는 필수 통제요건.
② Should (요건코드 식별자: -S)
필요 통제요건. 보안책임자의 의사결정에 따라 예외 처리할 수 있다. 단, TISAX의 엄격성을 고려할 때 불가피한 경우 외에는 사실상 필수 요건인 것으로 간주한다.
③ May (요건코드 식별자: -m)
선택 요건.
④ Additional high (요건코드 식별자: -ah)
AL2 선택 시 포함되는 통제요건. 강제성 수준은 must와 동일하다.
AL2는 TISAX 인증 시 선택할 수 있는 최소 수준이므로, 결과적으로 must와 동일한 수준의 강제성을 가진다.
⑤ Additional very high (요건코드 식별자: -av)
AL3 선택 시 포함되는 통제요건. 강제성 수준은 must와 동일하다.
⑥ Additional prototype (요건코드 식별자: -ap)
25번 카탈로그인 <prototype protection>에만 해당되는 요건. 강제성 수준은 must와 동일하다.

11) ML (Maturity Level: 성숙도 수준)
통제요건과 별개로, 통제요건 충족을 위해 수립한 프로세스의 수준을 의미한다.

12) ML요건
각 프로세스의 성숙도 수준을 만족하기 위해 충족해야 하는 요건을 의미한다. 통제요건 만족 시에도 ML요건의 미충족이 발생할 수 있다.

13) TML (Target Maturity Level: 목표 성숙도 수준)
TISAX의 78개 Q영역 각각이 만족해야 할 목표 성숙도 수준을 의미한다. 대부분의 Q영역이 TML3으로 지정되어 있고, TML2와 TML4가 각각 7개 Q영역에 지정되어 있다.

14) YML (Your Maturity Level: 실제 성숙도 수준)
Q영역에 대한 ISA 평가 결과 실제로 부여된 ML을 의미한다.

15) CLV (Control Limits of variation: 변동 통제 한계)
프로세스 효과성 수준에 대한 정량 평가 시, 평가 결과를 심각하게 인지해야 하는 수치 한계를 의미한다.
TML4 이상인 7개 Q영역만 해당된다.

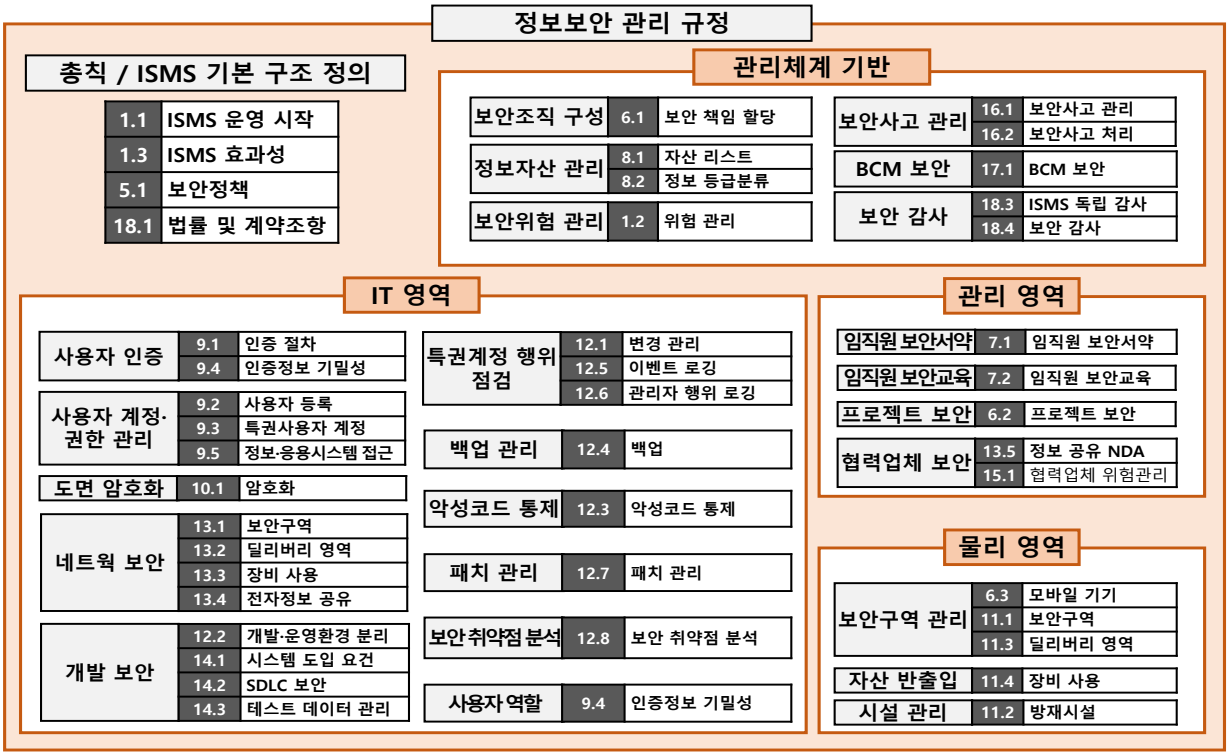
㈜화신 정보보안관리

1.4 ISMS 프레임웍

1.4.1 ISMS는 4가지 주요 카테고리로 구분한다

1) 관리체계 기반: 보안정책, 조직, 자산, 위험, 감사, 사고 등
2) 관리 영역: 프로젝트 보안, 협력업체 보안 등
3) 기술 영역: 시스템 보안 공통, 응용시스템, DBMS, 네트웍, 사용자 단말 등
4) 물리 영역: 출입 통제, 시설 관리 등

1.4.2 ISMS 프로세스 프레임웍을 다음과 같이 정의한다.



1.5 관련 법률 · 계약 조항 반영

1.5.1 관련 법률

5) 개인정보보호법: 회사 임직원 인사정보, 방문자 신상정보 관련.
6) 지식재산권법: 불법 소프트웨어 사용 금지 관련.
7) 기타 보안 관련 법률 해당사항 없음.

1.5.2 관련 계약 조항

없음.

1.6 규정 위반 시 징계

본 규정 위반 시 징계는 인사규정에 따른다.

▶ HS-GP-HR08(상벌)

㈜화신 정보보안관리

1.7 규정 공표

1.7.1 규정 승인

■ 본 규정의 승인권자는 대표이사로 정한다.

1.7.2 규정 공표 및 통지

■ 보안책임자는 본 규정을 사내 그룹웨어를 통해 전 임직원에게 공표한다.

■ 보안책임자는 본 규정을 해당 외부 파트너에게 통지한다.

1.7.3 연락정보 공지

■ 규정 공표 시 보안책임자, IT보안담당자, 총무보안담당자의 연락정보를 포함한다.

1.8 규정 검토 · 개선

1.8.1 검토 목표

본 규정의 검토 목표는 다음과 같이 정의한다.

8) ISMS 프로세스별 효과성 평가
9) ISMS 프로세스별 적용범위의 적합성 평가
10) ISMS 산출물의 타당성 평가
11) 새로 발생한 법률 이슈 및 비즈니스 요건의 반영
12) 기타 ISMS 운영 개선을 위해 개정할 사항 반영

1.8.2 검토 시기

보안책임자는 본 규정을 다음 시기에 평가한다.

① 연 1회 (매년 12월)
② 보안사고 발생 · 조치 후, 보안책임자가 ISMS 검토 필요성 판단 시
③ 기타, 보안책임자가 필요하다고 판단 시

1.8.3 규정 검토 회의

1) 규정 검토 회의 소집

보안책임자는 본 규정 검토에 필요한 인원을 지정하여 회의를 소집한다.

2) 규정 검토 회의 소집 대상

규정 검토 회의 소집 대상은 다음과 같이 정의한다.

① 보안책임자
② IT보안담당자
③ 총무보안담당자
④ 총무시설담당자 (필요 시)
⑤ 각 시스템 운영자 (필요 시)

3) 규정 검토 · 개선 체크리스트

보안책임자는 본 규정 검토를 위한 체크리스트를 다음 기준에 따라 정의한다.

① 효과성 · 적합성 평가

구분		TM L 3	TM L 4 이상
효과성	평가 데이터	■ 프로세스 산출물을 활용할 것	■ 평가 지표를 정의할 것
	평가 목표	-	■ 정량적 목표를 정의할 것
	평가 항목	■ 정성적 평가 항목을 정의할 것	■ 수치에 따른 등급을 정의할 것
	CLV		■ 수치에 따른 CLV를 정의할 것
적합성	평가 데이터	■ 프로세스 산출물을 활용할 것	■ 평가 지표를 정의할 것
	평가 목표		■ 정량적 목표를 정의할 것
	평가 항목	■ 정성적 평가 항목을 정의할 것	■ 수치에 따른 등급을 정의할 것
	CLV	-	-

② 관련 법률·비즈니스 요건 검토
③ 산출물 타당성 검토
④ 보안 영향도가 있는 변경작업 반영 검토

1.8.4 보안책임자는 본 규정의 평가 결과를 KMS에 정식 등록하여 저장한다.

1.8.5 산출물

산출물명	형태/위치	보존기한
정보보안 규정 검토·평가 결과	KMS	5 년
정보보안 규정	KMS	5 년

2. ISMS 기본 구조

2.1 프로세스 정의

2.1.1 관리체계 기반

1) 보안조직 구성
ISMS 운영에 필요한 보안 관련 역할을 정의하고, 업무 영역별 보안담당자 및 팀별 보안담당자 지정 및 필요 권한에 관한 요건을 정의한다.

2) 정보자산 관리
보호대상 정보의 생명주기에 관련된 모든 자산을 관리하기 위한 요건을 정의한다.

3) 보안위험 관리
보호대상의 생명주기 과정에 존재하는 각종 위협 및 취약점과 이로 인한 위험을 식별하고, 위험도를 분석·평가하여 효율적인 위험 조치 방안을 수립한다.

4) 보안사고 관리
보안 이슈 또는 사고 징후 발견시 즉각 대응하기 위한 보고체계를 수립한다.
보안 이슈 및 사고의 원인을 분석·조치하고 추후 유사 사고 재발 가능성을 최소화한다.

5) BCM 보안
정상적인 업무 수행이 불가한 비상 상황에서도 최소한의 ISMS 수준을 유지하도록 필수 요건과 대체 요건을 정의하고, 비상 대응 절차를 수립한다.

6) 보안감사
정보보호 정책 준수 여부를 점검하기 위한 보안감사 수행 절차를 수립한다.

2.1.2 관리 영역

1) 임직원 보안서약
임직원 보안서약서 징구에 관한 요건을 정의한다.

2) 임직원 보안교육
임직원 보안교육에 관한 요건을 정의한다.

3) 프로젝트 보안
상주 외부 프로젝트 사업 수행 시 필요한 보안 요건을 정의한다.

4) 협력업체 보안
상주 외부 프로젝트를 포함하여, 외부 협력업체 업무 위탁 시 비밀 유지 사항에 관한 요건을 정의한다.

㈜화신 정보보안관리

2.1.3 IT 영역

1) 인증절차
관리대상 정보자산 중 사용자가 접속하는 시스템에 대해, 사용자측과의 연결 세션과 사용자 인증정보의 관리에 관한 요건을 정의한다.

2) 계정 관리
관리대상 정보자산에 대해, 사용자 계정 등록 · 변경 · 회수 · 삭제에 관한 요건을 정의한다.
관리대상 정보자산에 대해, 사용자 권한 할당 · 변경 · 회수 · 삭제에 관한 요건을 정의한다.

3) 암호화
핵심 중요정보에 대해, 암호화 대상, 알고리즘, 키 관리 등 암호화 관련 요건을 정의한다.

4) 네트웍 보안
관리대상 정보자산이 구축된 네트웍에 대해, 네트웍 연결 통제, 인터넷 접점구간 통제, 중요 네트웍 내 행위 감시를 비롯한 각종 네트웍 보안 조치에 관한 요건을 정의한다.

5) 개발 보안
응용시스템 개발 시 분석-설계-구현-테스트-유지보수로 구분되는 각 개발 단계별로 필요한 요건을 정의한다.

6) 보안 로깅 · 점검
관리대상 정보자산에 대해, 특권 계정을 최소화하고 특권 계정의 사용자를 특정하여 사후추적의 기반을 보장하기 위한 요건을 정의한다.
보안 취약점을 유발할 수 있는 특권계정의 중요 변경 행위를 정의하고, 각 변경 행위를 통제하기 위한 요건을 정의한다.

7) 백업 관리
관리대상 정보자산 중 핵심시스템에 대해, 시스템 장애, 데이터 손실 등의 장애 상황 시 신속한 복구를 위해 필요한 백업 요건을 정의한다.

8) 악성코드 통제
관리대상 정보자산 중 악성코드 감염 가능성이 있는 시스템에 대해, 인터넷 경로, 물리적 인터페이스 등을 통해 유입되는 악성코드를 통제하기 위한 요건을 정의한다.

9) 패치 관리
관리대상 정보자산 시스템에 대해, 각 시스템의 코어 영역에 존재하는 취약점 제거를 위해서는 벤더가 제공하는 보안 패치가 필수적이므로, 이를 위한 요건을 정의한다.

10) 보안 취약점 분석
관리대상 정보자산 중 핵심시스템에 대해, 시스템 인프라 진단, 웹 진단, 모바일 진단 등 시스템 보안 취약점 분석에 관한 요건을 정의한다.

11) 사용자 역할
ISMS를 통해 구현하는 각종 통제와 별개로, 사용자의 자발적 협조가 필요한 사항을 정의한다.

2.1.4 물리 영역

1) 보안구역 관리
관리대상 정보자산이 위치한 사업장에 대해, 각 업무 공간의 중요도에 따른 물리적 보안조치를 차별화하기 위한 보안구역 통제 관련 요건을 정의한다.
외부 방문자의 사업장 출입 시 적용 절차에 관한 요건을 정의한다.

2) 자산 반출입
관리대상 정보자산 중 내부 시스템의 외부 반출입 또는 폐기 시 시스템 저장장치 내 중요 데이터 유출 방지를 위한 요건을 정의한다.

3) 방재시설 관리
관리대상 정보자산이 위치한 사업장에 대해, 보안구역 내 중요 시스템 · 시설 영역에 대한 방재 관련 요건을 정의한다.

㈜화신 정보보안관리

2.2 프로세스 오너십

역할	프로세스 오너십	역량 요건 (경력)
보안책임자	■ ISMS 운영 총괄	■ IT 경력 10 년 이상
IT보안 담당자	■ 보안조직 구성 ■ 정보자산 관리 ■ 보안위험 관리 ■ 프로젝트 보안 ■ 보안 취약점 분석 ■ 외부 협업 관리 ■ 보안감사 ■ BCM 보안 ■ 특권계정 행위 점검 ■ 보안사고 관리	■ IT 경력 10 년 이상
서버 운영자 응용시스템 운영자 DBA 보안시스템 운영자 네트웍 운영자	■ 사용자 인증 ■ 사용자 계정·권한 관리 ■ 백업 관리 ■ 패치 관리 ■ 악성코드 통제	■ IT 경력 5 년 이상
응용시스템 운영자	■ 개발보안	■ IT 경력 5 년 이상
네트웍 운영자	■ 네트웍 보안	■ 네트웍 운영 경력 3 년 이상
서버 운영자	■ 자산 반출입	■ IT 경력 5 년 이상
총무보안 담당자	■ 임직원 보안서약 ■ 임직원 보안교육 ■ 보안구역 관리	■ 물리보안 경력 5 년 이상
총무시설 담당자	■ 방재시설 관리	■ 시설관리 경력 5 년 이상

2.3 영역별 프로세스 서술 방식

순번	구분	서술 내용	TISAX 관련성	
			통제요건	ML요건
1	프로세스 목표	■ 해당 프로세스가 추구할 목표를 정의한다. ■ TISAX 기준 TML 4 이상에 해당하는 프로세스의 경우, 프로세스 목표를 정량적으로 정의한다.	-	PA2.1-1
2	공식 요건 관련성	■ 관련 법률, 계약 요건, TISAX, ISO27001, 파트너사 보안점검 기준 등 국내외 보안기준과 관련된 요건 영역을 정의한다.	-	-
3	적용 범위	■ 해당 프로세스의 적용 범위를 정의한다 ■ 표준 적용 범위, 실제 적용 범위, 제외 가능 범위로 구분하여 정의한다.	-	PA3.1-1 PA3.2-1
4	필요 자원	■ 해당 프로세스의 운영에 필요한 자원을 유형별로 정의한다. ■ 각 프로세스별 필요 자원은 ISMS 및 보안정책 전반의 필요 자원으로 간주한다.	-	PA2.1-5 PA3.1-4 PA3.2-4 PA3.2-5
5	표준 통제요건	■ 해당 프로세스의 운영에 필요한 표준 통제요건을 정의한다. ■ 적용범위 내 대상 중, 위험 발생가능성이 낮고 적용 난이도가 높은 대상의 경우 제외할 수 있다.	O	PA2.1-2 PA2.1-3 PA3.1-1 PA3.2-1
6	세부 통제요건	■ 해당 프로세스의 운영에 필요한 세부 통제요건을 정의한다. ■ 세부 통제요건은 표준 통제요건의 테일러링 기준을 포함한다. ■ 각 프로세스별 세부 통제요건은 ISMS 및 보안정책 전반의 세부 통제요건으로 간주한다.	O	PA2.1-2 PA2.1-3 PA3.1-1 PA3.2-1

7	산출물	■ 해당 프로세스의 산출물을 정의한다. ■ 각 프로세스별 산출물은 ISMS 및 보안정책 전반의 산출물로 간주한다. ■ 산출물의 보호 관련하여, 산출물의 형태/위치 및 보존기한을 명시한다.	0	PA2.2-1 PA2.2-2 PA2.2-3

3. 영역별 프로세스: 관리체계 기반

3.1 보안조직 구성

3.1.1 프로세스 목표

ISMS 운영에 필요한 보안 관련 역할을 정의하고, 업무 영역별 보안담당자 및 팀별 보안담당자 지정 및 필요 권한에 관한 요건을 정의한다.

3.1.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 6.1 보안 책임 할당

3.1.3 적용 대상

4) 표준 적용 대상

본 규정의 적용 범위와 동일

5) 실제 적용 대상

N/A

6) 제외 가능 대상

N/A

3.1.4 필요 자원

정보	인프라·업무환경
■ 회사 조직도 ■ 팀별 직무기술서 ■ 인사정보	■ KMS

3.1.5 표준 통제요건

1) 보안 책임사항 정의

① 보안책임자는 본 규정의 이행 및 영역별 프로세스의 보안 관련 책임사항을 정의한다.

② 보안책임자는 정의한 보안 책임사항을 담당할 인력을 선정하여 책임을 할당한다.

2) 필요 자원 제공

보안책임자는 본 규정의 이행을 위해 필요한 자원을 영역별 담당자에게 제공한다.

3) 역할 분리

보안책임자는 본 규정의 이행 과정에서 이해관계 충돌 방지를 위해 역할 분리 기준을 수립 · 운영한다.

㈜화신 정보보안관리

3.1.6 세부 통제요건

1) 보안 책임사항 정의

보안책임자를 비롯하여, 영역별 보안담당자를 다음과 같이 정한다.

① 보안책임자

A. 보안책임자는 총무부서장으로 정한다.

B. 보안책임자는 다음과 같은 책임을 담당한다.

a. 보안책임자는 정보보안 규정 이행의 최종 책임

b. 보안규정 제·개정의 지시 및 승인

c. 회사 보안 감사 지시 및 감독

d. 회사 보안 관련분야 (문서, 인원, 교육, IT 등) 총괄 관리

e. 보안사고 사전 예방 및 사고 발생 시 대응팀 소집·운영 권한

② IT보안담당자

A. IT보안담당자는 IT운영부서장이 부서 내 지정한 인력으로 정한다.

B. IT보안담당자는 다음과 같은 책임을 담당한다.

a. 본 규정의 IT 영역 프로세스 이행 관리

b. IT 영역 보안 규정 제·개정 추진

c. 각 시스템 운영자의 보안정책 변경작업에 대한 관리·점검

③ 총무보안담당자

A. 총무보안담당자는 총무부서장이 부서 내 지정한 인력으로 정한다.

B. 총무보안담당자는 다음과 같은 책임을 담당한다.

a. 본 규정의 관리·물리 영역 프로세스 이행 관리

b. 관리·물리 영역 보안 규정 제·개정 추진

c. 회사 보안감사 수행 및 보고

d. 회사 비밀 소유 현황 파악 및 보고

e. 회사 보안조직 관리 및 제도 운영

f. 보안 관련 대외 업무 수행

g. 정보 유출 신고센터 운영

④ 총무시설담당자

A. 총무시설담당자는 총무부서장이 부서 내 지정한 인력으로 정한다.

B. 총무시설담당자는 본 규정의 물리 영역 중 방재 시설 프로세스의 이행을 관리한다.

⑤ 부문 보안책임자

A. 부문 보안책임자는 회사 조직도 상의 본부, 실, 총괄, 공장별 최고 책임자로 정한다.

B. 부문 보안책임자는 다음과 같은 책임을 담당한다.

a. 각 부문별 보안관리 업무 책임 수행

b. 각 부문별 보안관리 지시 및 감독

c. 각 부문별 보호구역 승인 및 지정

⑥ 부문 보안담당자

A. 부문 보안담당자는 회사 조직도 상의 본부, 실, 총괄, 공장별 임원급 이상의 인력으로 정한다.

B. 부문 보안담당자는 다음과 같은 책임을 담당한다

a. 부문 보안 업무 총괄 수행

b. 부문 보안 및 교육 및 점검 시행 주관

c. 부문 내 보호구역 승인 및 지정 검토

⑦ 부서 보안책임자

A. 부서 보안책임자는 회사 조직도 상의 각 부서장으로 정한다.

B. 부서 보안책임자는 다음과 같은 책임을 담당한다.

a. 부서 보안담당자 선정 및 업무 관리

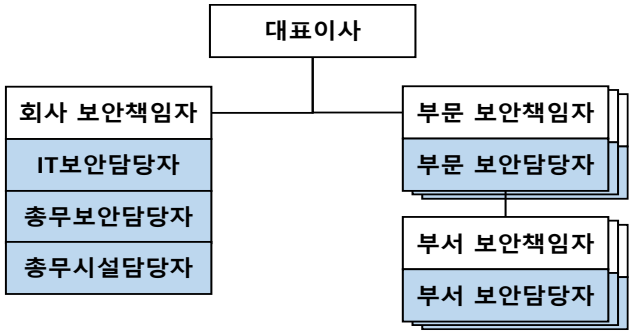
b. 부서 보안교육 및 감사 수검 주관

c. 보호구역 승인 요청 및 관리

㈜화신 정보보안관리

⑧ 부서 보안담당자
A. 부서 보안담당자는 부서 보안책임자가 지정한 인력으로 정한다.
B. 부서 보안담당자는 부서 보안책임자의 지시 하에 실무를 수행한다.

2) 보안 조직도
회사 보안조직도는 다음과 같이 정한다.



3) 역할 분리
보안책임자는 관리의 독립성 보장을 위해, 다음 기준에 따라 역할을 분리한다.
① IT보안담당자 - 시스템 운영자
② IT보안담당자 - 특권계정 사용자
③ 응용시스템 운영자 - 배포관리자
④ 서버·네트웍 운영자 - 보안시스템 운영자

4) 보안담당자 지정
① 보안책임자는 각 영역별 담당자 및 부서 보안담당자에게 자격을 부여한다.
② IT보안담당자는 보안책임자의 지시에 따라 보안조직도를 문서화한다.

3.1.7 산출물

산출물명	형태/위치	보존기한
보안조직도	파일	5 년

3.2 정보자산 관리

3.2.1 프로세스 목표
보호대상 정보의 생명주기에 관련된 모든 각종 시스템자산을 관리하기 위한 요건을 정의한다.
자산의 CIA 가치에 근거하여 중요도와 등급을 분류하기 위한 기준을 정의한다.

3.2.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 8.1 자산 리스트 ■ 8.2 정보 등급분류

3.2.3 적용 대상
1) 표준 적용 대상
ISMS 적용범위 내 보호대상 정보 관련 전산장비, 응용시스템, IT 지원시설, 문서
2) 실제 적용 대상
ISMS 적용범위 내 보호대상 정보 관련 전산장비, 응용시스템, IT 지원시설, 문서
3) 제외 가능 대상
없음

㈜화신 정보보안관리

3.2.4 필요 자원

정보	인프라·업무환경
■ 전산장비 리스트 ■ 시설장비 리스트 ■ 전산장비 배치도 ■ 응용시스템 리스트	■ N/A

3.2.5 표준 통제요건

1) 자산 유형 정의
IT보안담당자는 자산을 유형별로 식별하여 기록한다.

2) 자산 책임자 지정
IT보안담당자는 식별한 자산별 책임자를 지정한다.

3) 자산 중요도 기준
IT보안담당자는 자산 중요도 기준을 수립한다.

4) 자산 리스트 관리
IT보안담당자는 자산 리스트를 작성하고, 정기 갱신한다.

5) 시스템 자산 명시적 사용
IT보안담당자는 각 자산별 운영 책임자가 자산 사용 권한을 해당 사용자에게 부여 시, 지정된 권한자의 승인 하에 부여한다.

6) 자산 회수
총무보안담당자는 사용자 퇴사 및 계약만료 시, IT보안담당자와의 협조 하에 자산 및 계정 · 권한 회수 절차를 수립 · 운영한다.

3.2.6 세부 통제요건

1) 자산 유형 정의
IT보안담당자는 자산 유형 분류 기준을 다음과 같이 정의한다.

① 코어 영역 시스템
A. 응용시스템
B. 서버
C. DBMS
D. 보안시스템
E. 네트웍장비

② IT 지원시설
A. UPS
B. 항온항습기
C. 기타 전산장비 성능 유지를 위한 지원시설

③ 전자정보, 종이문서

④ 공정 내 PLC 프로그램
A. XG5000
B. XP builder
C. Labview

⑤ 공정 내 장치 컨트롤러

2) 자산 책임자 지정
IT보안담당자는 자산별 책임자 지정 시, 다음과 같이 책임 수준 및 유형을 고려한다.
① 자산 소유자 (소유권 기준)
② 자산 운영 책임자 (메인 오너십. 계정 · 권한 할당 처리)
③ 계정 · 권한 할당 승인권자
④ 실제 운영 담당자 (예: 외부업체 대행 운영 시)
⑤ 일반사용자 범위
⑥ 일반사용자에 대한 사용 승인권자
⑦ 기타 관련 책임사항
3) 자산 중요도
IT보안담당자는 자산 중요도 기준에 다음 사항을 포함한다.
① 기밀성, 무결성, 가용성으로 구분하여 중요도를 부여할 것
② 기밀성, 무결성, 가용성 침해 시 영향도를 기준으로 중요도 등급을 구분할 것
③ 기밀성의 경우, 반출 시 결재권자를 명시할 것
④ 무결성 · 가용성의 경우, 복구 소요기간을 지정할 것
4) 자산 리스트 관리
① IT보안담당자는 자산 리스트 갱신 시기를 다음과 같이 정한다.
A. 정기: 연 1회 (매년 12월)
B. 비정기: 자산 신규 등재, 변경, 폐기 시
② IT보안담당자는 각 자산의 현재 상태를 다음 기준에 따라 기록한다.
A. 사용 준비 중
B. 사용 중
C. 사용 중단
D. 폐기
5) 시스템 자산 명시적 사용
① 승인대상 자산은 일반사용자가 직접 사용해야 하는 자산을 대상으로 한다.
② 승인대상 자산의 유형은 다음과 같이 정한다.
A. 응용시스템 사용자 계정 승인: 해당 운영자 또는 IT운영부서장
B. PLC 접속자 승인: 사용팀 팀장
③ 전산장비, 시설장비 등 일반사용자의 직접 사용과 무관한 자산은 승인대상에서 제외할 수 있다.
6) 자산 회수
① 총무보안담당자는 회수할 물리 자산을 다음과 같이 정한다.
A. 사원증
B. RF 출입키
C. 기타 개인에게 발급했던 개인 업무 자산
② IT보안담당자는 총무보안담당자의 요청에 따라, 퇴사자 또는 계약만료자에 대해 다음 사항을 수행한다.
A. PC 회수
B. 시스템 계정 · 권한 회수
7) 세부 기준
문서 자산의 세부 분류 기준은 다음 기준에 따른다.
▶ 정보자산 평가 및 분류 기준

3.2.7 산출물

산출물명	형태/위치	보존기한
자산 리스트	파일	5 년
자산 사용 승인 이력	파일	5 년
자산 사용자 내역	파일	5 년
정보자산 평가 및 분류 기준	파일	5 년

㈜화신 정보보안관리

3.3 보안위험 관리

3.3.1 프로세스 목표

보호대상의 생명주기 과정에 존재하는 각종 위협 및 취약점과 이로 인한 위험을 식별하고, 위험도를 분석·평가하여 효율적인 위험 조치 방안을 수립한다.

3.3.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 1.2 위험 관리

3.3.3 적용 대상

8) 표준 적용 대상

ISMS 적용범위 내 보호대상 정보 관련 정보자산 및 서비스

9) 실제 적용 대상

ISMS 적용범위 내 보호대상 정보 관련 정보자산 및 서비스

10) 제외 가능 대상

없음

3.3.4 필요 자원

정보	인프라·업무환경
■ 각 프로세스 세부내역 ■ 각 프로세스 산출물	■ N/A

3.3.5 표준 통제요건

11) 위험 평가 수행

IT보안담당자는 다음 시기에 위험 평가를 수행한다.

① 정기: 연 1회 (매년 12월 ISMS 정기 검토 시)

② 비정기: 위험평가가 필요한 수준의 중대한 이슈가 발생했다고 보안책임자가 판단 시

A. 사업장 이동

B. IT인프라의 대규모 변경

C. 대규모 조직 개편

D. 심각한 보안사고 발생

12) 위험 분석 기준

IT보안담당자는 위험 분석 시 다음 2가지 항목을 기준으로 분석·평가한다.

① 위험도: 식별한 위험이 실현될 경우 서비스에 미칠 영향의 정도

② 발생가능성: 식별한 위험이 실제 발생할 가능성의 정도

13) 위험 조치·수용 기준

IT보안담당자는 식별한 위험에 대한 위험 조치 및 수용 기준을 정한다.

14) 위험 평가 필수 대상 업무

IT보안담당자는 다음 업무를 필수적으로 위험 평가 대상에 포함한다.

① 사용자 인증

② 외부 XaaS 사용

③ 보안구역별 보호조치

④ 개발-실환경 분리

15)위험 평가·조치 문서화

IT보안담당자는 위험 평가·조치 과정을 문서화한다.

㈜화신 정보보안관리

3.3.6 세부 통제요건

1) 위험 분석 기준

IT보안담당자는 위험도 판단을 위해 위험도와 발생가능성의 등급을 다음과 같이 정의한다.

① 위험도

등급	기준
3	■ 위험이 실현될 경우 서비스에 심각한 영향이 발생하여 회사 운영에 치명적인 피해가 예상되는 경우
2	■ 위험이 실현될 경우 서비스에 높은 영향이 발생하여 회사 운영에 피해가 예상되는 경우
1	■ 위험이 실현될 경우 서비스에 낮은 영향이 예상되는 경우로서, 발생시 간단히 조치 가능하거나 방치해도 무방한 경우

. ② 발생가능성

등급	기준
3	■ 해당 위험의 발생가능성이 높은 경우
2	■ 해당 위험의 발생가능성이 있는 경우
1	■ 해당 위험의 발생가능성이 낮아 무시 가능한 경우

2) 위험조치 유형

위험조치 유형을 다음과 같이 정의한다.

유형	정의	비고
위험 수용	■ 위험을 받아들이고 비용을 감수함	■ 실질적 조치 보류
위험 감소	■ 위험을 감소시킬 수 있는 대책을 채택하여 구현함	■ 대부분의 실질적 위험 조치가 이에 해당
위험 회피	■ 위험이 존재하는 프로세스나 사업을 포기함	■ 가장 근본적인 조치 방안이나, 현실적으로 불가한 경우 많음
위험 전가	■ 잠재적 비용을 제 3 자에게 이전하거나 할당함	■ 보험, 소송, 페널티 등

3) 위험조치 난이도 평가

위험조치 과제의 후보를 식별한 후, 해당 과제의 난이도를 판단하기 위해 다음 3가지 관점을 고려한다.

① 복잡도

등급	기준	비고
3	■ 서비스 운영 상 영향이 적어 간단히 수행할 수 있는 경우	■ 타 시스템, 조직 간 연관성 없거나 낮음
2	■ 서비스 운영 상 영향이 예상되어 별도 계획 하에 수행해야 하는 경우	■ 타 시스템, 조직 간 연관성 존재
1	■ 서비스 운영 상 큰 영향이 예상되어 세부적인 계획 하에 수행해야 하는 경우	■ 타 시스템, 조직 간 연관성 복잡

. ② 발생가능성

등급	기준
3	■ 1 개월 이내 (Quick-fix)
2	■ 3 개월 이내
1	■ 3 개월 초과

③ 예상 비용

등급	기준
3	■ 1 천만원 이하
2	■ 5 천만원 이하
1	■ 5 천만원 초과

4) 위험조치 과제 선정
IT보안담당자는 위험조치 과제 선정 시 해당 위험의 위험도, 발생가능성, 해당 과제의 적용 난이도 · 소요기간 · 예상비용 등 5가지 항목을 종합적으로 고려한다.
① 5가지 항목 수치의 총합이 높은 순서대로 선정
② 또는, 5가지 항목 중 일부 특정 항목 위주로 고려하여 선정

5) 위험 수용
IT보안담당자는 특정 위험에 대한 조치 없이 위험 수용 시 그 사유를 명시한다. 위험 수용 사유의 예는 다음과 같다.
① 수치 총합이 특정 수치 이하인 과제
② 위험도가 낮은 과제
③ 적용 난이도가 높은 과제
④ 소요기간이 긴 과제
⑤ 예상비용이 높은 과제

3.3.7 산출물

산출물명	형태/위치	보존기한
위험평가 보고서	파일	5 년
위험조치 계획서	파일	5 년
위험조치 결과서	파일	5 년

3.4 보안사고 관리

3.4.1 프로세스 목표
보안 이슈 또는 사고 징후 발견 시 즉각 대응하기 위한 보고체계를 수립한다.
보안 이슈 및 사고의 원인을 분석 · 조치하고 추후 유사 사고 재발 가능성을 최소화한다.
보안 이슈 또는 사고에 대해 신속히 대응한다.

3.4.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 16.1 보안사고 관리 ■ 16.2 보안사고 처리

3.4.3 적용 대상
6) 표준 적용 대상
본 규정의 적용 범위와 동일
7) 실제 적용 대상
N/A
8) 제외 가능 대상
N/A

3.4.4 필요 자원

정보	인프라·업무환경
■ 보안사고 발생 정보 ■ 보안사고 최초 보고자 ■ 보안사고 피해 현황	■ 방화벽, IPS, NAC ■ 네트워 트래픽 모니터링 ■ 기타 보안시스템

3.4.5 표준 통제요건

1) 보안사고 등급

① 보안책임자는 보안사고를 의심할 수 있는 유형을 정의하여, 일반 임직원이 보안사고 여부를 판단하는 데에 활용하도록 한다.

② 보안책임자는 보안사고 심각도에 따른 등급을 정의한다.

2) 보안사고 대응 조직

보안책임자는 보안사고 발생 시 기존 보안 조직도를 활용한 보안사고 대응 조직 임시 구성안을 정의한다.

3) 보안사고 보고 절차

보안책임자는 보안사고 의심 상황 발생 시 이를 신속히 인지할 수 있는 보고 절차를 수립·운영한다.

4) 보안사고 대응 절차

보안책임자는 보안사고 인지 후 사고 등급에 따른 대응을 위한 절차를 수립·운영한다.

5) 보안사고 원인 분석·평가

보안책임자는 보안사고 대응 종료 후 원인 분석·평가를 위한 절차를 수립·운영한다.

6) 보안사고 원인 제공자 징계

보안사고 원인 제공자에 대한 징계는 인사규정에 따른다.

▶ HS-GP-HR08(상벌)

3.4.6 세부 통제요건

1) 보안사고 등급

① 보안사고 의심 정황

IT보안담당자는 다음과 같은 상황을 보안사고 의심 정황으로 정의한다.

A. 도면 등 중요정보 도난, 분실, 유출, 위변조
B. 시스템 또는 PC 로그인 해킹
C. PC 파일 접근 불가
D. 시스템 또는 PC 악성코드 감염
E. 서버, DBMS 등 전산장비의 특이한 장애
F. 기타 보안 취약점, 소프트웨어 오동작, 시스템 오류 등

② 보안사고 등급

IT보안담당자는 보안사고의 심각도에 따라 4개 등급으로 구분한다.

등급	구분	정의
1 등급 (심각)	기준	모든 네트워크와 서비스 장비에 심각한 영향을 주어 고객 서비스 전체에 심각한 위험을 초래하는 취약점 및 사고
	사례	■ 주요 서비스 중단 사례 - 주요 시스템 정지 또는 불안정 - 공장 라인 운영에 영향을 미치는 사태 - 감염 PC에서 다량의 트래픽을 발생시키는 경우(DDoS 공격 등) ■ 비즈니스 사례 - 시스템 다운 타임이 12 시간 이상 - 시스템 피해 금액이 500 만원 이상 - 파트너 고객사의 신뢰성 상실 사태 - 전면적인 생산 중단 사태

㈜화신 정보보안관리

등급	구분	정의
2 등급 (경계)	기준	일부 또는 개별 서비스에 심각한 영향을 주는 취약점
	사례	■ 주요 서비스 중단 사례 - 개별 시스템 장애 발생 - 생산성에 영향을 미치는 시스템 중지 사태 ■ 비즈니스 사례 - 일부 수입 손실의 발생 사태 - 파트너 고객사의 신뢰성 저하 사태 - 문제 해결에 일부 영업 손실을 초래하는 사태
3 등급 (주의)	기준	서비스에 중대한 영향을 미치지는 않지만, 지속적으로 발생하거나 특정 부분에서 발생될 경우 위험을 초래할 수 있는 잠재적인 위험성이 존재하는 취약점 및 사고
	사례	■ 주요 서비스 기능의 중단 사례 - 이중화된 시스템의 개별 장애 발생 - 일부 노드 및 지역 장애 발생 - 일반적으로 알려진 악성코드에 의한 공격 ■ 비즈니스 사례 - 일부 서비스 속도 지연 사태 - 공정 라인 속도 지연 사태
4 등급 (정상)	기준	서비스에 직접적인 영향을 주지 않는 일반적인 인터넷상의 보안 위협 취약점 및 사고
	사례	■ 주요 서비스 기능의 중단 사례 - 시스템 기능성이나 공정 라인에 영향이 미미한 상황 - 업무 PC 또는 공정 PC 일부 감염 ■ 비즈니스 사례 - 네트워 트래픽 일부 점유

2) 보안사고 보고 체계

① 모든 임직원은 보안사고가 의심되는 상황 인지 시, IT보안담당자 또는 총무보안담당자에게 통보한다.

② IT보안담당자 및 총무보안담당자는 보안사고 여부 및 등급을 판단하여 IT운영부서장 또는 보안책임자에게 보고한다.

③ 보안사고 발생 시 IT보안담당자 및 총무보안담당자는 보안책임자에게 세부적인 사고 상황을 보고하고, 사고 원인 및 대처방안을 분석한다.

3) 보안사고 대응 조직

① 2등급 이상의 보안사고 발생 시, 보안책임자는 대표이사 승인 하에 기존 보안조직을 다음과 같이 임시 재편한다.

A. 보안책임자
대표이사 직속으로서, 보안사고 대응 총괄 책임을 담당한다.

B. IT운영부서장
보안책임자의 지시에 따라, 보안사고 대응에 필요한 IT 관련 제반 사항을 지원한다.

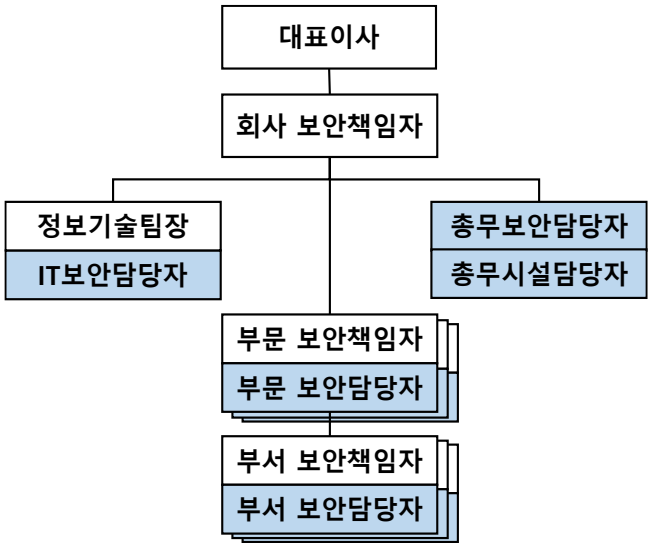
C. 총무보안담당자
보안책임자의 지시에 따라, 관리 · 물리 영역 관련 대응을 수행한다.

D. 총무시설담당자
보안책임자의 지시에 따라, 방재시설 관련 대응을 수행한다.

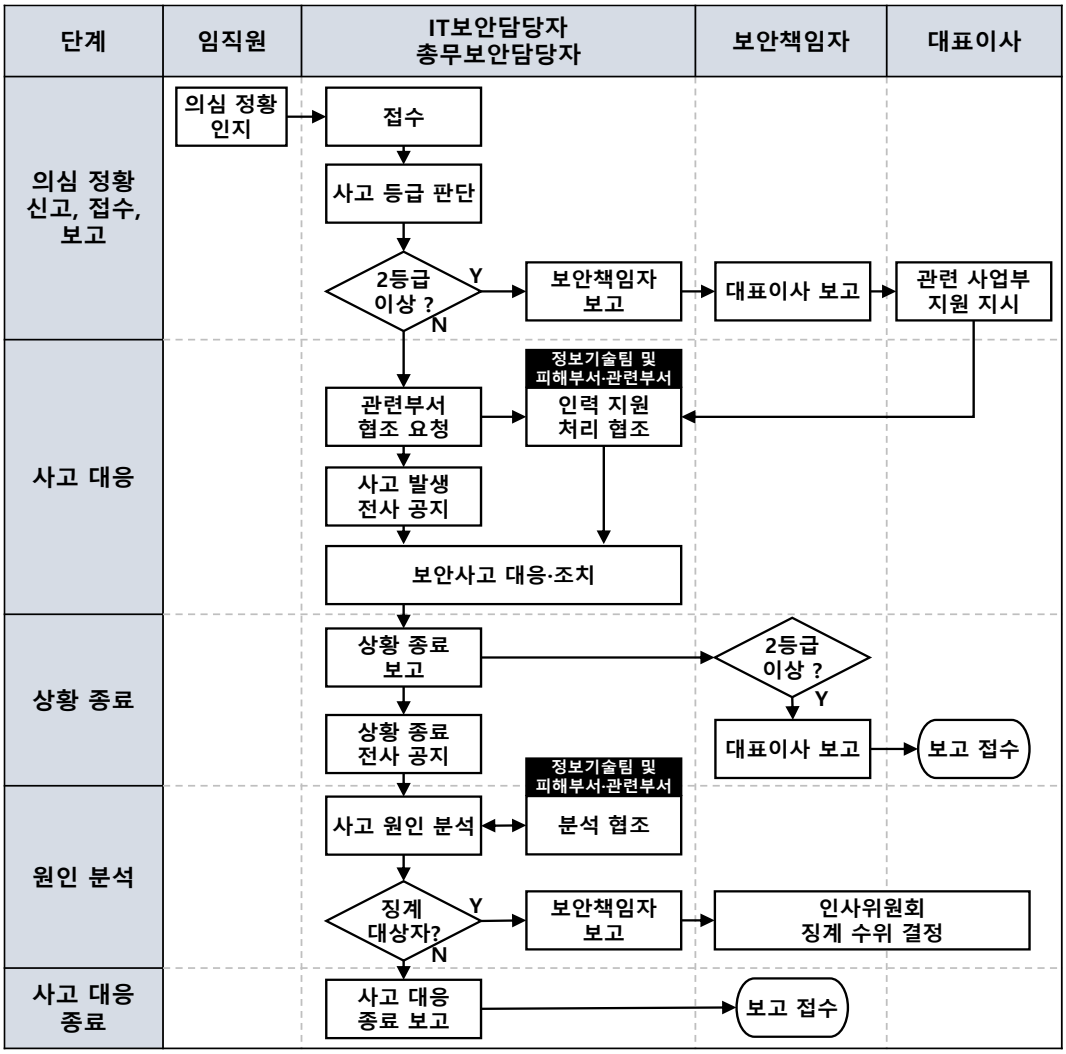
E. 부문 보안책임자, 부서 보안책임자
보안책임자, IT운영부서장, 총무보안 · 시설담당자가 전달하는 대응 사항을 책임 부문 · 부서 내 임직원이 준수하도록 전파한다.

㈜화신 정보보안관리

② 보안사고 대응을 위해 임시 재편된 보안 조직도는 다음과 같이 구성한다



4) 보안사고 대응 절차



5) 보안사고 원인 분석 · 평가
① IT보안담당자 및 총무보안담당자는 보안사고 대응 이후 피해 상황을 파악한다.
② IT보안담당자 및 총무보안담당자는 보안사고 관련 증거를 확보 및 보존한다.
③ 사고 처리 완료 후, 보안책임자는 보안사고 보고서를 작성하여 대표이사에게 보고한다.
④ 보안사고 보고서는 다음 사항을 포함한다.
A. 보안사고 유형 · 등급
B. 사고 발생 일시
C. 조치 완료 시각
D. 사고 대상 자산
E. 사고 영향 범위
F. 사고 내용(현상)
G. 사고 원인과 조치 내용
H. 사후 대책
I. 기타 사고와 관련된 다양한 증적 등
6) 관련 파트너 고지
IT보안담당자는 보안사고 등급에 따라 피해 고객 또는 파트너에게 피해 사실을 고지한다.

3.4.7 산출물

산출물명	형태/위치	보존기한
보안사고 보고서	KMS	5 년
관련 파트너 고지 이력	메일	5 년

3.5 BCM 보안

3.5.1 프로세스 목표
정상적인 업무 수행이 불가한 비상 상황에서도 최소한의 ISMS 수준을 유지하도록 필수 요건과 대체 요건을 정의하고, 비상 대응 절차를 수립한다.

3.5.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 17.1 BCM 보안

3.5.3 적용 대상
1) 표준 적용 대상
본 규정의 적용 범위와 동일
2) 실제 적용 대상
N/A
3) 제외 가능 대상
N/A

3.5.4 필요 자원

정보	인프라·업무환경
■ 필수 응용시스템 리스트 ■ 필수 장비 리스트	■ N/A

㈜화신 정보보안관리

3.5.5 표준 통제요건

1) 대상 시스템 정의
IT보안담당자는 BCM 대상 시스템을 정의한다.

2) 시스템 fail over 계획 수립
IT보안담당자는 BCM 대상 시스템 각각에 대해 fail over 계획을 수립한다.

3) Fail over 상황의 최소 보안 요건
IT보안담당자는 fail over 상황에서 준수해야 할 최소 보안 요건을 정의한다.

4) BCM 정기 검토
IT보안담당자는 fail over 계획을 정기 검토한다.

3.5.6 세부 통제요건

1) 대상 시스템 정의
① IT보안담당자는 BCM 대상 시스템의 fail over 기준을 다음과 같이 구분한다.
A. Mirror site: 시스템 중요도 5
B. Hot site: 시스템 중요도 3
C. Warm site: 시스템 중요도 2
D. Cold site: 시스템 중요도 1

2) Fail over 상황의 최소 보안 요건
① IT보안담당자는 시스템 fail over 상황에서 준수해야 할 최소 보안 프로세스를 다음과 같이 정의한다.
A. 사용자 인증
B. 사용자 등록
C. 사용자 권한 관리
D. 네트웍 보안
② 최소 보안 프로세스의 세부사항은 해당 프로세스를 참조한다.

3) BCM 정기 검토
IT보안담당자는 fail over 계획을 다음과 같이 정기 검토하여 필요 시 개정한다.
① 검토 시기: 연 1회 (매년 12월 중)
② 검토자: IT운영부서장
③ 검토 공유: 해당 부문 보안책임자
④ 검토 승인: 대표이사

3.5.7 산출물

산출물명	형태/위치	보존기한
시스템 fail over 계획	파일	5 년

3.6 보안 감사

3.6.1 프로세스 목표

정보보호 정책 준수 여부를 점검하기 위한 보안감사 수행 절차를 수립한다
ISMS 범위 내 정보, 조직, 사업장, 시스템에 대해 정책 · 지침의 모든 조항에 대한 준수 여부를 감사한다.
이해관계가 배제된 외부 독립조직에 의한 보안감사 수행 절차를 수립한다.

3.6.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 18.3 ISMS 독립 감사 ■ 18.4 보안 감사

㈜화신 정보보안관리

3.6.3 적용 대상

1) 표준 적용 대상
본 규정의 적용 범위와 동일

2) 실제 적용 대상
N/A

3) 제외 가능 대상
N/A

3.6.4 필요 자원

정보	인프라·업무환경
■ 각 프로세스별 산출물·증적	■ 고객사 보안감사 수검 ■ 외부 전문업체 보안감사 계약

3.6.5 표준 통제요건

1) 보안감사 수행
보안책임자는 본 규정의 준거성 평가를 위한 보안감사를 정기 수행한다.

2) 보안감사 계획 수립
보안책임자는 보안감사를 위한 계획, 범위, 항목을 수립한다.

3) 보안감사 결과 및 조치
① 보안책임자는 부적합사항에 대한 시정 조치를 수행하고 그 결과를 확인한다.
② 보안책임자는 점검 결과를 기록하여 유지한다.
③ 보안책임자는 점검 결과를 대표이사에게 보고한다.

3.6.6 세부 통제요건

1) 보안감사 수행
① 보안감사 수행 시기는 다음과 같이 정한다.
A. 정기: 격년 1회 (시기 무관)
B. 비정기: 보안책임자가 필요하다고 판단 시
② 보안감사 대상은 본 규정의 적용범위 전체를 대상으로 한다.

2) 보안감사 계획 수립
보안감사 범위는 본 규정의 적용범위 내에서 정하여 수행한다. 이 때, 다음 사항을 반영한다.
① 지난 보안감사 범위와의 중복성을 고려하여, 팀별 범위의 공평함을 유지할 것.
② 보안 위규 가능성이 높다고 판단되는 범위를 주요 대상으로 고려할 것.
③ 감사 당시의 사회적 보안이슈, 정보보호 관련 법률 · 비즈니스적 관심사항을 주요 대상으로 고려할 것.

3) 외부 보안감사
고객사 보안감사, 외부 전문업체 컨설팅 수행 시 보안감사를 갈음할 수 있다.
① 현대차 · 모비스 정기 보안점검
② 정기 회계 감사 시 IT감사
③ 국내외 인증 대비 외부 전문업체 컨설팅 결과

3.6.7 산출물

산출물명	형태/위치	보존기한
현대차·모비스 보안감사 계획서	파일	5 년
현대차·모비스 보안점검 결과서	파일	5 년
TISAX self-assessment report	파일	5 년

㈜화신 정보보안관리

4. 영역별 프로세스 : 관리 영역

4.1 임직원 보안서약

4.1.1 프로세스 목표

임직원 및 장기 출입 외부인력에 대한 보안서약 관련 요건을 정의한다.

4.1.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 7.1 임직원 보안서약

4.1.3 적용 대상

1) 표준 적용 대상
당사 임직원 전체
2) 실제 적용 대상
N/A
3) 제외 가능 대상
N/A

4.1.4 필요 자원

정보	인프라·업무환경
■ 임직원 명단 ■ 장기 출입 외부인력 명단	■ 없음

4.1.3 적용 대상

1) 표준 적용 대상
당사 임직원 전체
2) 실제 적용 대상
N/A
3) 제외 가능 대상
N/A

4.1.4 필요 자원

정보	인프라·업무환경
■ 임직원 명단 ■ 장기 출입 외부인력 명단	■ 없음

4.1.5 표준 통제요건

1) 임직원 보안서약서 징구
총무보안담당자는 임직원에 대해 비밀유지 및 당사 보안정책 준수 의무를 공지하고 문서를 통한 서약을 받는다
2) 임직원 보안서약 내용
총무보안담당자는 보안서약 내용에 구체적인 준수사항, 보안정책 위반 시 처벌 관련사항을 포함한다.

㈜화신 정보보안관리

4.1.6 세부 통제요건

1) 임직원 보안서약서 징구
총무보안담당자는 모든 임직원에 대해, 고용계약시 고용계약서와 별개의 문서로 보안서약서를 징구한다.

2) 임직원 보안서약 내용
총무보안 담당자는 보안서약서에 명시할 사항을 다음과 같이 정의한다.
① 회사 보안정책을 준수할 것.
② 회사 보안정책 위반 시 불이익을 받을 수 있음을 명시할 것.
③ 민감정보 취급팀에 대해, 관련 사항을 추가 명시할 것. (개인정보, 도면 등)

4.1.7 산출물

산출물명	형태/위치	보존기한
임직원 보안서약서	파일	5 년

4.2 임직원 보안교육

4.2.1 프로세스 목표
보안교육 내용, 대상, 시기, 방법 등 보안교육 관련 요건을 정의한다.

4.2.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 7.2 임직원 보안교육

4.2.3 적용 대상

1) 표준 적용 대상
당사 임직원 전체

2) 실제 적용 대상
N/A

3) 제외 가능 대상
N/A

4.2.4 필요 자원

정보	인프라·업무환경
■ 부서 보안담당자 명단 ■ 보안교육 반영할 기반 자료	■ 없음

4.2.5. 표준 통제요건

1) 임직원 보안교육
총무보안담당자는 임직원 대상 보안교육 프로그램을 계획 · 운영한다.

2) 보안교육 자료
① 총무보안담당자는 보안교육용 자료를 작성하여 배포한다.
② 보안책임자는 보안교육 내용을 승인하고, 교육에 필요한 자원을 지원한다.

3) 보안교육 참석 관리

4.2.6 세부 통제요건

1) 임직원 보안교육

① 총무보안담당자는 보안교육을 다음과 같이 수행한다.

A. 교육 시기: 반기 1회 또는 특별 사항 발생 시

B. 교육 수행: 총무보안담당자

C. 교육 대상: 부서 보안담당자

② 팀내 임직원에 대한 자체 보안교육은 팀내 보안담당자의 재량으로 수행한다.

2) 보안교육 자료

총무보안담당자는 보안교육 내용에 다음 사항을 포함한다. 각 교육 내용은 회차별 주제를 별도로 정하여 수행할 수 있다.

① 보안 위험 일반사항

② 당사 정보보안 규정 변경 사항

③ 부서 보안담당자 준수사항, 일반사용자 준수사항

④ 개인정보 보호

⑤ 일반사용자 해킹 방지

⑥ 악성코드 주의 이슈

3) 보안교육 참석 관리

① 총무보안담당자는 보안교육 수행 시마다 대상자의 참석 여부를 기록한다.

② 보안교육에 대한 KPI를 다음과 같이 정의한다.

A. 교육 이수율 = 교육 참가자 / 교육 대상자

B. KPI 목표: 교육 이수율 90% 이상

4.2.7 산출물

산출물명	형태/위치	보존기한
보안교육 자료	파일	5 년
보안교육 참석자 명단	파일	5 년

4.3 프로젝트 보안

4.3.1 프로세스 목표

외부 프로젝트 사업 수행 시, 해당 프로젝트의 특성에 따라 본 규정이 정의한 프로세스 적용 방법에 관한 요건을 정의한다.

4.3.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 6.2 프로젝트 보안

4.3.3 적용 대상

1) 표준 적용 대상

보호대상 정보자산 관련 상주 외부 프로젝트

2) 실제 적용 대상

보호대상 정보자산 관련 상주 외부 프로젝트

3) 제외 가능 대상

내부 TF 프로젝트

㈜화신 정보보안관리

4.3.4 필요 지원

정보	인프라·업무환경
■ 외부 프로젝트 정보 ■ 프로젝트 팀원에게 제공되는 민감정보 ■ 프로젝트 팀원에게 제공되는 시스템 권한	■ 프로젝트 관련 응용시스템·서버·DBMS ■ 소스관리 시스템 ■ 배포관리 시스템

4.3.5 표준 통제요건

1) 프로젝트 유형 정의

IT보안담당자는 외부 프로젝트의 보안요건 관련 특성에 따라 프로젝트 유형을 정의한다.

2) 프로젝트 보안 점검

IT보안담당자는 프로젝트 유형에 따른 보안요건의 준수 여부에 대한 점검 절차를 수립·운영한다.

4.3.6 세부 통제요건

1) 프로젝트 유형 정의

IT보안담당자는 외부 프로젝트의 특성에 따라 해당되는 프로세스 및 적용할 보안요건을 정의한다.

해당 케이스	해당 프로세스	해당 요건
공통	협력업체 보안	■ NDA 체결 ■ 투입인력 보안서약서 징구
상주 개발	개발 보안	■ 전용 개발서버 사용 ■ 전용 소스관리시스템 사용 ■ 전용 배포관리시스템 사용
내부 네트워 연결	네트워 보안	■ 네트워 사용 제한
인프라 접속	사용자 인증	■ Hiware 접속

2) 프로젝트 보안 점검

IT보안담당자는 프로젝트 보안 점검을 다음과 같이 수행하고 필요한 사항을 조치한다. 해당 보안 점검은 위험평가의 성격으로 간주한다.

① 점검 시기

A. 최초 점검: 프로젝트 계약 또는 인력 투입 후 1주 이내

B. 프로젝트 계약 기간 중 매월 마지막 주 (단, 계약 후 3주 미만 경과 시 생략 가능)

② 점검 방식: 별도 체크리스트

③ 점검자: 프로젝트 담당자

④ 확인자: IT보안담당자

▶ [별첨]프로젝트 보안점검 체크리스트

4.3.7 산출물

산출물명	형태/위치	보존기한
프로젝트 보안 점검 결과	파일	5 년

㈜화신 정보보안관리

4.4 협력업체 보안

4.4.1 프로세스 목표

외부조직과의 협업으로 인한 정보 교류가 존재할 경우, 정보 유출 방지를 위한 조직 간 NDA 체결 관련 요건을 정의한다.
외부조직에 의한 정보 유출 가능성을 최소화하고, 유출사고 발생시 책임소재를 명시한다.

4.4.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 13.5 정보 공유 NDA ■ 15.1 협력업체 위험관리

4.4.3 적용 대상

1) 표준 적용 대상
보호대상 정보를 제공받거나, 보호대상 정보자산의 접속 권한을 제공받는 외부 협력업체
2) 실제 적용 대상
PLM 접속 권한 제공받는 외부 협력업체
3) 제외 가능 대상
N/A

4.4.4 필요 지원

정보	인프라·업무환경
■ 협력업체 리스트 ■ 협력업체와의 교류 정보	■ PLM

4.4.5 표준 통제요건

1) NDA 체결
① IT보안담당자는 협력업체와 계약 시 NDA를 체결한다.
② 계약서 내 비밀유지 관련 조항을 구체적으로 명시하는 방식으로 NDA를 갈음할 수 있다.
2) NDA 표준 내용
① IT보안담당자는 NDA에 다음 사항을 포함한다.
A. NDA 제목
B. 책임자 회사명/소속팀/직급/성명
C. NDA 유효기간 (계약 만료일자 명시, 만료 후 3년)
D. 비밀유지 대상 정보 내역
E. 양측의 책임사항
F. 계약 외 정보에 대한 사용 금지 문구
② NDA를 통해 합의된 사항은 해당 협력업체의 재하도급 업체에 대해서도 동일하게 적용한다.
3) NDA 법적 검토
IT보안담당자는 NDA 표준 양식에 대해 법적 검토를 득한다.
4) NDA 요건 검토
IT보안담당자는 해당 업체와의 재계약시, NDA에 명시된 요건을 검토하여 필요 시 갱신한다.
5) NDA 연장
해당 협력업체 계약 주관팀은 계약 연장 시 이를 IT보안담당자에게 통보한다.

4.4.6 세부 통제요건

1) NDA 법적 검토

NDA 조항이 계약서에 포함 시, 계약서에 대한 법적 검토를 득하여 이를 갈음할 수 있다.

2) NDA 연장

① 해당 협력업체 계약 주관팀은 계약 연장 시 다음 사항을 IT보안담당자에게 통보한다.

A. 책임자 회사명/소속팀/직급/성명 (변경 시)

B. 계약 만료일자

C. 비밀유지 대상 정보 내역 (변경 시)

② IT보안담당자는 계약 연장 시 통보된 내역을 PLM 운영자에 전달한다.

4.4.7 산출물

산출물명	형태/위치	보존기한
협력업체 계약서	KMS	5 년
협력업체 계약서 법적 검토 이력	파일	5 년
투입인력 보안서약서	파일	5 년

5. 영역별 프로세스 : IT 영역

5.1 사용자 인증

5.1.1 프로세스 목표

관리대상 정보자산에 대해, 사용자가 시스템 접속 시 사용자측이 직간접적으로 입력하는 각종 정보를 기준으로 접속 인증 여부를 결정하게 되며, 이러한 인증에 관련된 요건을 정의한다.

관리대상 정보자산에 대해, 비인가 사용자의 무단 접속을 방지한다.

5.1.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 9.1 사용자 인증 ■ 9.4 인증정보 기밀성

5.1.3 적용 대상

1) 표준 적용 대상

2) 실제 적용 대상

3) 제외 가능 대상

5.1.4 필요 자원

정보	인프라·업무환경
■ 사용자 계정 정보 ■ 시스템 리스트	■ 대상 시스템이 사용자 인증 관련 기능 지원 ■ 대상 시스템 내 패스워드 정책 강제 설정 기능 ■ 외부자용 OTP 기능

㈜화신 정보보안관리

5.1.5 표준 통제요건

1) 인증방식 개요

IT보안담당자는 ID/PW 방식을 기본으로 시스템별 사용자 인증을 구현하도록 조치한다.

2) 패스워드 정책

① IT보안담당자는 시스템별 패스워드 정책을 수립·적용한다.

② IT보안담당자는 모든 시스템에 대해 디폴트 패스워드 사용을 금지한다.

3) 패스워드 발급

각 시스템 운영자는 일반사용자에게 패스워드 최초 발급 또는 재발급 시, 발급 과정에서 노출되지 않도록 안전한 발급 방식을 정의한다.

4) 인증 추가 조치

IT보안담당자는 시스템의 중요도 및 위험도에 따라 인증수준 강화를 위한 추가 조치를 검토한다.

5) 인증수준 차등 적용

IT보안담당자는 시스템별 중요도 및 위험평가 결과에 따라 인증 수준을 차등 적용한다.

5.1.6 세부 통제요건

1) 인증방식 개요

① IT보안담당자는 시스템 접속 시 인증방식을 케이스별로 다음과 같이 구분한다.

A. 일반 정보시스템: ID/PW

B. 중요 정보시스템: OTP 추가 (Hiware, PLM)

C. PLC 프로그램: password only

② 웹기반 응용시스템의 경우, 로그인 화면 우회를 방지하기 위해 모든 페이지에 인증 로직을 구현한다.

③ OTP 사용 시, OTP넘버의 사용기한을 설정한다. 이때, 외부접속의 경우 최대 24시간을 초과하지 않도록 한다.

2) 패스워드 정책

응용시스템 운영자는 사용자의 디폴트 패스워드 사용을 실질적으로 금지하기 위해, 사용자 최초 로그인 후 강제 변경을 적용한다.

3) 패스워드 발급

① 응용시스템 운영자는 내부 임직원 및 외부 협력업체 계정의 패스워드에 대해, 임시 패스워드 최초 발급 후 최초 로그인 시 패스워드를 강제 변경하도록 구현한다.

② 응용시스템 운영자는 패스워드 강제 변경 구현이 불가한 경우, 다음 사항을 준수한다.

A. 임시 패스워드 생성 시 랜덤값으로 설정할 것

B. 내부 임직원 및 외부 협력업체에 최초 전달 시 즉시 변경해야 함을 강조할 것

4) 인증 추가 조치

시스템의 중요도 및 위험도에 따라 다음 사항을 추가 적용한다.

① 로그인 실패 횟수: 패스워드 무작위 입력(brute force) 공격의 위험이 있다고 판단되는 경우, 로그인 실패 횟수를 설정한다.

② 프로토콜: 원격 접속 경로에 보안 위험 존재 시, 암호화 프로토콜을 적용한다.

A. 인터넷을 경유한 외부에서의 접속 (해외 법인의 접속 포함)

B. 기타 접속 경로에 보안 위험 존재 시

③ 디폴트 포트 금지: 원격 접속 경로에 보안 위험 존재 시, 디폴트 포트를 추측이 어려운 포트로 변경한다.

④ 세션 타임아웃: 원격 접속 경로에 보안 위험 존재 시, 세션 타임아웃을 각각의 기준에 따라 적용한다.

5) 인증수준 차등 적용

① IT보안담당자는 다음 사항을 반영한 시스템별 세부 인증 규칙을 수립한다.

② 시스템 케이스 구분 (자산 중요도, 자산 환경에 따른 위험도 고려)

③ 고위험 여부

④ 인증방식

⑤ 패스워드 정책: 최소길이, 복잡도, 변경주기

⑥ 원격 접속 시, 암호화 여부

⑦ 원격 접속 시, 디폴트 포트 변경 여부

⑧ 로그인 실패 횟수

⑨ 세션 타임아웃

㈜화신 정보보안관리

⑨ 허용 IP주소 설정

5.1.7 산출물

산출물명	형태/위치	보존기한
시스템 인증 규칙	파일	5 년

5.2 사용자 계정 · 권한 관리

5.2.1 프로세스 목표

관리대상 정보자산에 대해, 사용자 계정 · 권한의 할당 · 변경 · 회수 · 삭제에 관한 요건을 정의한다.
관리대상 정보자산에 대해, 정식 절차를 통해 계정 · 권한을 등록한다.
유휴 계정 · 권한을 최소화한다.

5.2.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 9.2 사용자 등록 ■ 9.3 특권사용자 계정 ■ 9.5 정보·응용시스템 접근

5.2.3 적용 대상

1) 표준 적용 대상
보호대상 정보자산 중 응용시스템, 주요 전산장비
2) 실제 적용 대상
보호대상 정보자산 중 응용시스템, 코어 영역 전산장비
3) 제외 가능 대상
보호대상 정보자산 중 소영역 전산장비 (L2 스위치, 무선 AP, 무선 공유기 등)

5.2.4 필요 자원

정보	인프라·업무환경
■ 임직원 사번 ■ 사용자 계정 생성 규칙	■ 계정 승인 이력 관리 시스템 ■ 계정 발급 방법 ■ 계정 자동 추출 기능 ■ 퇴사자 계정 자동 비활성화

5.2.5 표준 통제요건

1) 개별/공용계정 사용 대상
IT보안담당자는 시스템별 개별/공용계정 사용 대상을 정의한다.
2) 특권계정 문서화
IT보안담당자는 각 시스템별 특권계정을 문서화한다.
3) 일반사용자 계정 · 권한 할당
각 시스템 운영자는 일반사용자 계정 · 권한 할당 시 신청 · 승인 하에 할당한다.
4) 특권계정 · 권한 할당
각 시스템 운영자는 자신의 계정을 포함하여, 특권 계정 · 권한 할당 시 신청 · 승인 하에 할당한다.
5) 일반사용자 계정 디폴트 권한
응용시스템 운영자는 일반사용자 계정 최초 발급시, 최소 권한이 설정된 role 또는 그룹을 할당한다.
6) 사용자 계정 · 권한 정기 검토
각 시스템 운영자는 사용자 최소 권한 원칙을 유지하기 위해, 사용자 계정 · 권한에 대한 정기 검토를 수행한다.

㈜화신 정보보안관리

5.2.6 세부 통제요건

1) 개별/공용계정 사용 대상
   ① 공용계정 허용 케이스는 다음 사항으로 제한하고, 이 외에는 공용계정 사용을 불허한다.
      A. PLM 외부업체 계정: 업체 단위 발급
      B. Hiware 외부업체 계정: 업체 단위 발급
      C. 공장 라인 내 PC: 팀 단위 사용
      D. PLC 프로그램: 팀 단위 사용
   ② 특권계정에 대해, 공용계정 사용을 금지한다.
   ③ 공용계정 허용 시, 개인 추적이 가능하도록 다음 사항을 적용한다.
      A. IP주소를 로깅할 것.
      B. 계정-IP주소를 매핑하여 로깅할 것.

2) 특권계정 문서화
   특권계정은 다음 계정을 포함한다.
   ① 최고관리자 계정: Admin, Administrator, root, superuser
   ② 외부업체 유지보수 계정
   ③ 시스템 연동용 계정: WAS의 DB 접속용 계정, EAI 연동 계정, 대외서버용 계정 등

3) 일반사용자 계정 · 권한 할당
   ① 계정 · 권한 신청권자는 사용자의 팀장으로 정한다.
   ② 계정 · 권한 승인권자는 시스템 운영자로 정한다.
   ③ 응용시스템 운영자는 일반사용자 계정 · 권한 할당 시 다음 원칙을 적용한다.
      A 신청 기반 승인 원칙
      B. Role-based 권한 할당
      C. Role별 최소 메뉴 할당
   ④ 도면 사용 시스템의 경우, 다음 사항에 대해 일반사용자의 소속팀장이 도면의 관리 책임을 담당한다.
      이 때, 소속팀장은 팀원의 신청에 따라 다음 사항을 직접 승인할 수 있다.
      A. 도면 암호화 해제
      B. 도면에 적용된 DRM 정책의 변경
      C. 도면의 외부 반출

4) 특권계정 · 권한 할당
   ① 특권계정 · 권한 신청권자는 시스템 운영자로 정한다.
   ② 특권계정 · 권한 신청권자는 정보화 부서장으로 정한다.
   ③ 각 시스템 운영자는 특권계정 · 권한 할당 시, 사용 필요 원칙에 따른다.
   ④ 각 시스템 운영자는 특권계정 사용자의 직무영역 변경 시 즉시 반영을 원칙으로 한다.

5) 일반사용자 계정 디폴트 권한
   응용시스템 운영자는 일반사용자 계정에 권한 할당 시, 다음 원칙을 적용한다.
   ① 최초 발급 시 부서별 기본 권한 할당
   ② 타 부서 소유의 메뉴에 대한 접근권한이 필요한 경우, 별도 신청 · 승인 하에 할당

6) 사용자 계정 · 권한 정기 검토
   사용자 계정 정기 검토는 다음 방침에 따라 수행한다.
   ① 검토 시기
      A. 정기: 정기적으로 점검
      B. 비정기: 이슈 발생 시 점검
   ② 검토 대상 시스템: e-HR, KMS, SAP, PLM
   ③ 검토 대상 계정 유형: 일반사용자, 특권계정
   ④ 검토 항목
      A. 유휴 계정 여부 (퇴사자, 계약만료 등)
      B. 유휴 권한 여부
      C. 과다 발급 계정 · 권한 여부 (부서 이동, 직무영역 변경 등)
      D. 낮은 사용실적 여부

㈜화신 정보보안관리

5.2.7 산출물

산출물명	형태/위치	보존기한
일반사용자 계정·권한 신청·승인 이력	파일	5 년
특권계정·권한 신청·승인 이력	파일	5 년
일반사용자 계정·권한 정기 검토 결과	파일	5 년
특권계정·권한 정기 검토 결과	파일	5 년

5.3 도면 암호화

5.3.1 프로세스 목표

핵심 중요정보에 대해, 암호화 대상, 알고리즘, 키 관리 등 암호화 관련 요건을 정의한다.
중요정보 유출 시에도 기밀성을 보장한다.
암호화 키 유출을 방지한다.

5.3.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 10.1 암호화

5.3.3 적용 대상

1) 표준 적용 대상
보호대상으로 지정한 문서의 파일 포맷
2) 실제 적용 대상
도면 문서 파일: CAD, iCAD, MODView, Catia 포맷
3) 제외 가능 대상
N/A

5.3.4 필요 자원

정보	인프라·업무환경
■ 암호화 대상 도면 파일 포맷 ■ 암호화 시점	■ 도면 DRM ■ 정책 관리 서버

5.3.5 표준 통제요건

1) 암호화 알고리즘
IT보안담당자는 국내외 공인 인증을 획득한 암호화 모듈을 사용한다.
2) 암호키 관리
① IT보안담당자는 다음 사항을 포함한 암호키 관리 방안을 수립한다.
A. 암호키 관리주체
B. 암호키 생성 · 변경 주기
C. 암호키 적용 경로
D. 암호키 폐기 방식
E. 암호키 복구 절차
② IT보안담당자는 국정원 보안적합성 평가 인증을 획득한 DRM 모듈을 사용할 경우, 암호키 관리를 생략할 수 있다.

5.3.6 세부 통제 요건

1) 도면 DRM 적용

① IT보안담당자는 적용 대상 도면의 파일 포맷에 대해 DRM을 적용한다.

② DRM 정책은 다음 항목을 포함한다.

A. 평문 파일로 복사&붙여넣기 금지

B. 화면 캡처 금지

C. 보조 저장매체로 쓰기 금지

2) 도면 DRM 정책 변경

① IT보안담당자는 도면 사용팀장에게 도면 DRM 정책의 변경 권한을 할당할 수 있다.

② 도면 사용팀장은 도면 사용자의 신청에 근거하여 다음과 같이 정책을 변경한다.

A. 도면 DRM 복호화 (해제)

B. 도면 DRM 정책 완화

C. 도면 반출

3) 도면 반출

① 도면 사용팀장은 도면 반출 시 도면 사용자의 신청에 근거하여 반출한다.

② DRM 해제 상태로 도면 반출 시, 도면에 파일암호를 적용하여 반출한다.

5.3.7 산출물

산출물명	형태/위치	보존기한
도면 DRM 적용 상태	PLM	5 년
도면 DRM 정책 변경 이력	PLM	5 년
도면 반출 이력	PLM	5 년

5.4 네트웍 보안

5.4.1 프로세스 목표

관리대상 정보자산이 구축된 네트웍에 대해, 네트웍 연결 통제, 인터넷 접점구간 통제, 중요 네트웍 내 행위 감시를 비롯한 각종 네트웍 보안 조치에 대한 요건을 정의한다.

네트웍 내 각 서브넷별 중요도 · 위험도를 고려한 분리 요건을 정의한다.

임직원의 외부 접속, 원격지에 위치한 국내외 법인망과의 연결에 필요한 보안 요건을 정의한다.

5.4.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 13.1 네트웍 관리 ■ 13.2 네트웍 보안 요건 ■ 13.3 네트웍 분리 ■ 13.4 전자정보 공유

5.4.3 적용 대상

1) 표준 적용 대상

보호대상 정보자산 중, 정보기술팀 책임 하에 운영하는 네트웍 장비, 서버 및 기타 인프라 장비로 구성된 네트웍 영역

2) 실제 적용 대상

① 내부 서버망

② 내부 OA망

③ 내부 FA망

3) 제외 가능 대상

내부 서버망 및 OA망과 분리된 별도의 폐쇄망 영역

㈜화신 정보보안관리

5.4.4 필요 자원

정보	인프라·업무환경
■ 네트웍 구성도	■ 네트웍 장비 ■ 방화벽 및 기타 네트웍 보안시스템

5.4.5 표준 통제요건

1) 인터넷 접점구간 보안
네트웍 운영자는 내부 네트웍의 인터넷 접점구간에 대해 방화벽을 포함한 네트웍 보안을 적용한다.

2) 네트웍 사용 제한
네트웍 운영자는 내외부 인력의 PC를 내부망 연결 시, 사전 승인 하에 통신을 허용한다.
IT보안담당자는 공개서비스 허용/차단 대상을 정의하여 네트웍 운영자를 통해 적용한다.

3) 인터넷 경유 구간 암호화
네트웍 운영자는 인터넷을 경유하는 국내외 법인망에 대해 VPN을 적용한다.
메일서버 운영자는 이메일에 전송 암호화를 적용한다.

4) 네트웍 트래픽 모니터링
네트웍 운영자는 인터넷 접점구간 또는 백본 영역의 네트웍 트래픽을 모니터링한다.

5) 네트웍 이중화
네트웍 운영자는 무중단 서비스가 필요한 구간에 대해 네트웍 이중화를 적용한다.

6) 네트웍 분리
네트웍 운영자는 내부망 내 상호 통신을 불허할 서브넷에 대해 네트웍 분리를 적용한다.

5.4.6 세부 통제요건

1) 인터넷 접점구간 보안
① 네트웍 운영자는 인터넷 접점구간에 대해 다음과 같은 네트웍 보안시스템을 적용한다.
A. 방화벽
B. IPS
C. 웹방화벽
D. 스팸필터 서버
E. 네트웍 VPN
F. SSL VPN

2) 네트웍 사용 제한
① 네트웍 운영자는 PC의 내부 네트웍 임의 연결을 통한 고정 IP를 운영한다.
② NAC 운영자는 내부 네트웍에 연결된 PC의 NAC 에이전트 미설치 시, 고정 IP 할당과 별개로 해당 PC의 네트웍 사용을 차단한다.
③ IT보안담당자는 내부망에 연결된 PC를 통한 공개서비스의 사용에 대해 다음 정책을 적용하고, 네트웍 운영자는 이를 보안시스템에 적용한다.
A. 차단: 외부 주요 포털 메일서비스, 유해사이트
B. 허용: 일반 웹 접속 (메신저 포함)

3) 인터넷 경유 구간 암호화
메일서버 운영자는 메일서버에 SSL 또는 TLS 암호화를 적용한다.

4) 네트웍 이중화
네트웍 운영자는 다음 기준에 따라 이중화를 적용한다.
① 백본 구간: 경로 이중화 (Active-active)
② 인터넷 접점구간 방화벽: 경로 이중화 (Active-Standby)

5) 네트웍 분리
네트웍 운영자는 다음 기준에 따라 네트웍을 VLAN으로 분리한다.
① 인터넷 DMZ 망
② 내부 서버팜
③ 내부 OA망
A. 언하동 사업장 사무동 / 현장 / 연구소
B. 봉동 사업장 사무동 / 현장
C. 해외 법인사업장별 네트웍
④ 내부 FA망

5.4.7 산출물

산출물명	형태/위치	보존기한
네트웍 구성도	파일	5 년
일일 보고▶네트웍 모니터링	파일	5 년

5.5 개발 보안

5.5.1 프로세스 목표
응용시스템 도입 시 필요한 보안요건을 정의한다.
응용시스템 개발 시 분석-설계-구현-테스트-유지보수로 구분되는 각 개발 단계별로 필요한 요건을 정의한다.
개발작업 시 테스트 목적의 실데이터 사용을 최대한 억제하고, 실데이터를 사용한 테스트가 불가피할 경우 개발서버 내 실데이터의 저장기간 최소화를 위한 요건을 정의한다.

5.5.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 12.2 개발·운영환경 분리 ■ 14.1 시스템 도입 보안 ■ 14.2 SDLC 보안 ■ 14.3 테스트 데이터 관리

5.5.3 적용 대상
6) 표준 적용 대상
보호대상 정보 관련 응용시스템 (자체 개발/위탁 개발 포함)
7) 실제 적용 대상
도면을 사용하는 응용시스템 (자체 개발/위탁 개발 포함)
8) 제외 가능 대상
도면 사용과 무관한 시스템

5.5.4 필요 자원

정보	인프라·업무환경
■ KISA 시큐어코딩 가이드	■ 웹방화벽

㈜화신 정보보안관리

5.5.5 표준 통제요건

9) 개발 요건 정의
① IT보안담당자는 응용시스템 신규 개발·기능 확대 시 적용해야 할 보안요건을 정의한다.
② 해당 보안요건은 SDLC 각 단계에서의 점검 사항에 포함한다.

10) 개발·운영 환경 분리
① IT보안담당자는 운영환경과 분리된 개발환경을 별도로 구축한다.
② 운영시스템 내 불필요한 개발 도구 및 시스템 도구의 설치를 금지한다.

11) 개발·테스트 서버 인증
① 개발·테스트 서버의 인증수준은 운영서버와 동일한 수준으로 구현한다.
② 개발·테스트 서버와 운영서버 간 사용자 인증정보를 서로 다르게 설정하는 것을 원칙으로 한다.
단, 동일한 운영자가 개발·테스트 서버 및 운영서버를 담당할 경우, 본 요건은 생략할 수 있다.

12) SDLC 단계별 점검사항
IT보안담당자는 SDLC 단계별 보안요건 적용 여부 점검 시점을 정의한다.
이 때, 다음 단계에서는 보안요건 적용 여부를 필수 점검한다.
① 설계 단계
② 최종 승인 단계

13) 보안코딩 기준
① IT보안담당자는 응용시스템 개발 시 보안코딩을 위한 가이드를 적용한다.
② KISA에서 배포한 각 개발언어별 시큐어코딩 가이드를 활용할 수 있다.

14) 개발자 자격 요건
IT보안담당자는 개발자의 보안코딩 이해도를 보장하기 위해 개발자의 자격 요건을 정한다.

15) 소스 관리
IT보안담당자는 소스 관리를 위한 시스템을 구축하여 버전을 관리한다.

16) 배포 관리
IT보안담당자는 소스 배포 시스템을 구축하여 배포 과정을 관리한다.

17) 테스트 데이터 관리
① 사용 여부를 통제할 테스트 데이터는 도면 암호화 대상 파일로 정의한다.
: 도면 문서 파일: CAD, iCAD, MDView, Catia 포맷
② IT보안담당자는 해당 데이터에 대해, 응용시스템 개발 과정에서 테스트 목적의 실데이터 사용 금지 원칙을 적용한다.
③ 응용시스템 운영자는 테스트 데이터 사용 시, 더미 파일을 생성하여 사용한다.
④ 응용시스템 운영자는 운영서버의 도면 데이터를 테스트용으로 추출 시, IT보안담당자의 사전 승인을 득한다.
⑤ 응용시스템 운영자는 테스트 완료 즉시 테스트에 사용한 데이터를 개발서버에서 삭제한다.

5.5.6 세부 통제요건

18) 개발 요건 정의
IT보안담당자는 개발 요건에 다음 프로세스에서 정의한 보안 요건을 반영한다.
① 사용자 인증
② 사용자 계정·권한 관리
③ 도면 암호화
④ 특권계정 행위 점검

19) 개발·운영 환경 분리
① IT보안담당자는 개발·테스트 서버와 운영서버를 각각 전용 서버로 구축한다.
② 운영서버 내 설치할 수 있는 개발 도구 및 시스템 도구는 다음에 해당하는 것 외에 모두 금지한다.
A. OS 설치 시 기본 설치되는 built-in 도구
B. 시스템 구동에 필수적인 개발 프레임웍 (JDK 등)
C. 시스템 운영에 필수적인 시스템 도구

19) 개발 · 운영 환경 분리
① IT보안담당자는 개발 · 테스트 서버와 운영서버를 각각 전용 서버로 구축한다.
② 운영서버 내 설치할 수 있는 개발 도구 및 시스템 도구는 다음에 해당하는 것 외에 모두 금지한다.
A. OS 설치 시 기본 설치되는 built-in 도구
B. 시스템 구동에 필수적인 개발 프레임웍 (JDK 등)
C. 시스템 운영에 필수적인 시스템 도구

20) 개발자 자격 요건
IT보안담당자는 개발자의 자격 요건을 다음과 같이 정한다.
① 개발 PM: 다음 중 한가지를 충족할 것.
A. 해당 시스템 구축 경험 3회 이상
B. 해당 시스템 언어의 개발 경력 5년 이상
C. 소프트웨어 기술등급 고급 이상
② 개발 팀원: 다음 중 한가지를 충족할 것.
A. 해당 시스템 언어의 개발 경력 1년 이상
B. 소프트웨어 기술등급 중급 이상

21) 배포 관리
① 응용시스템 운영자는 개발 완료 후 배포관리자에게 배포 요청한다.
② 배포관리자는 배포할 소스에 대해 보안코딩 분석 후 배포한다. 단, 배포 대상 시스템이 웹방화벽에 의한 보호 대상에 포함되는 경우 보안코딩 분석을 생략할 수 있다.

5.5.7 산출물

산출물명	형태/위치	보존기한
PLM 보안요건 리스트	파일	5 년
배포관리 이력	배포관리시스템	5 년

5.6 특권계정 행위 점검

5.6.1 프로세스 목표
관리대상 정보자산에 대해, 보안 취약점을 유발할 수 있는 ISMS의 중요 변경 행위를 정의하고, 각 변경 행위를 통제하기 위한 요건을 정의한다.
관리자를 비롯한 특권 사용자의 행위를 통제하기 위한 요건을 정의한다.
특권 사용자의 임의적 행위를 점검한다.

5.6.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 12.1 변경 관리 ■ 12.5 이벤트 로깅 ■ 12.6 관리자 행위 로깅

5.6.3 적용 대상
1) 표준 적용 대상
① 특권계정의 행위 중 임의 변경 시 보안 영향도가 있는 작업을 대상으로 행위 점검을 수행한다.
② 점검대상 행위 기준은 다음 기준에 따른다.
A. 시스템 운영자
a. 계정 · 권한 임의 할당 여부
b. 보안정책 임의 변경 여부
B. 배포관리자: 소스 임의 배포 여부
C. 일반사용자 중 특권사용자: 부여된 권한의 임의 사용 여부

㈜화신 정보보안관리

2) 실제 적용 대상
① PLM 시스템 운영자: 계정 · 권한 임의 할당 여부
② PLM 배포관리자: 소스 임의 배포 여부
③ 도면 사용팀 팀장
A. 도면 DRM 암호화 해제
B. 도면 DRM 정책 변경
C. 도면 임의 반출
3) 제외 가능 대상
① 서버 운영자의 서버 내 보안설정 변경
② 네트웍 운영자의 네트웍 설정 변경
③ 보안시스템 운영자의 보안시스템 정책 변경
④ 도면 사용팀장의 도면 DRM 복호화 및 반출

5.6.4 필요 자원

정보	인프라·업무환경
■ 관리대상 시스템별 중요 기능 내역	■ 신청·승인 이력 기록용 시스템 ■ 관리대상 시스템별 행위 로그 ■ 특권계정 행위 점검 툴

5.6.5 표준 통제요건
1) 변경작업 승인 · 기록
해당 특권계정 사용자는 지정된 작업 수행 시 신청 · 승인 절차를 거친다.
2) 변경작업 로깅 · 작업기록
IT보안담당자는 임의 변경작업에 대한 사후 점검을 위해 변경작업을 로깅한다.
3) 임의 변경 점검 · 조치
① IT보안담당자는 특권계정의 임의 행위 발견 시, 이에 대한 조치방안을 정한다.

5.6.6 세부 통제요건
1) 변경작업 승인 · 기록
① 신청 · 승인 절차는 다음 기준에 따른다.

행위 구분	신청자	승인자
시스템 변경	시스템 운영자	정보화 부서장
PLM 도면 암호화 해제 PLM 도면 암호화 정책 변경 도면 반출	사용팀원	사용팀장

② 시스템 운영자의 경우, 원활한 업무를 위해 사전 승인을 생략할 수 있다. 단, 작업내역을 그룹웨어에 저장한다.
2) 변경작업 로깅 · 작업기록
① 로깅 세부사항은 다음 기준에 따른다.
A. 로깅 · 작업기록 방법
a. 로깅: 특권계정 사용자의 행위를 시스템에서 자동 로깅
b. 작업기록: 특권계정 사용자의 작업내역 직접 입력 또는 작업 승인 신청내역 직접 입력
B. 로깅 · 작업기록 데이터 보호
a. 특권계정 사용자 - 그룹웨어 운영자 분리
b. 특권계정 사용자 - 로그 저장 DB 직접 접근 금지
c. 5년 이상 보존
② IT보안담당자는 로깅 작업을 외부업체에 위탁할 경우, 해당 요건을 계약서에 명시한다.

3) 임의 변경 점검 · 조치
① 임의 행위 발견 시 조치방안은 다음 기준에 따른다.
A. 해당 특권계정 사용자에게 소명 요구
B. 필요 시 변경작업 복원
② IT보안담당자는 다음 기준에 따라 임의 변경 점검을 수행한다.
A. 수행 주기: 월 1회 (매월 마지막주)
B. 특권계정 사용자가 기록한 작업내역과 실제 작업로그 간 일치 여부 확인
C. 불일치 발견 시 임의 행위로 간주, 소명 요구
D. 소명되지 않은 작업로그에 대해, 보안위험을 판단하여 보안책임자에 보고

5.6.7 산출물

산출물명	형태/위치	보존기한
시스템 변경작업 작업 이력	그룹웨어	5 년
PLM 도면 암호화 변경 이력	PLM	5 년
특권계정 행위점검 기록	파일	5 년

5.7 백업 관리

5.7.1 프로세스 목표

관리대상 정보자산 중 핵심시스템에 대해, 시스템 장애, 데이터 손실 등의 장애 상황 시 신속한 복구를 위해 필요한 백업 요건을 정의한다.

5.7.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 12.4 백업

5.7.3 적용 대상

1) 표준 적용 대상
서버 OS, DBMS, 코어 네트웍 장비 설정, 보안시스템 정책
2) 실제 적용 대상
① 서버 OS
② DBMS
3) 제외 가능 대상
① 네트웍 장비 설정
② 보안시스템 정책

5.7.4 필요 자원

정보	인프라·업무환경
■ 장비 리스트	■ 백업관리 시스템

5.7.5 표준 통제요건

1) 기본 백업 정책
IT보안담당자는 다음 사항을 포함하는 백업 요건을 정의한다.
① 백업 대상 시스템
② 대상별 백업 주기
③ 대상별 백업데이터 저장 · 운반 매체

2) 백업 데이터 보호
① 백업시스템 운영자는 백업 데이터에 대해 접근제어를 적용한다.
② 백업시스템 운영자는 백업 데이터를 타 건물로 소산 보관한다.
3) 백업 확인
백업시스템 운영자는 백업 성공 여부를 정기적으로 확인한다.

5.7.6 세부 통제요건
1) 기본 백업 정책
백업시스템 운영자는 다음 기준에 따라 자동 백업시스템을 운영한다.

백업 대상	백업 방식	백업 주기	백업 데이터 저장 위치
Windows 서버	Full 백업 최신 이미지 유지	매일	백업시스템
DBMS	Full, incremental 최신 이미지 유지	매일	백업시스템

2) 백업 데이터 보호
① 백업시스템 운영자는 백업시스템의 특권계정을 운영자 전용으로 사용한다.
② 백업시스템 운영자는 백업 데이터 소산을 위해, 백업대상 시스템과 백업시스템의 위치를 서로 다른 사업장으로 분리하여 운영한다.
3) 백업 확인
백업시스템 운영자는 다음 기준에 따라 백업 확인작업을 수행한다.

5.7.7 산출물

산출물명	형태/위치	보존기한
백업 데이터	백업시스템	5 년
일일보고▶백업 확인 결과	파일	5 년

5.8 악성코드 통제

5.8.1 프로세스 목표
관리대상 정보자산 중 악성코드 감염 가능성이 있는 시스템에 대해, 인터넷 경로, 물리적 인터페이스 등을 통해 유입되는 악성코드를 통제하기 위한 요건을 정의한다.
악성코드 감염 가능성을 최소화한다.

5.8.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 12.3 악성코드 통제

5.8.3 적용 대상
1) 표준 적용 대상
인프라 시스템: 서버, 네트웍 장비, 보안시스템
2) 실제 적용 대상
① 업무용 Windows PC
② 내부망에 연결된 외부인력의 Windows PC
③ Windows 서버

3) 제외 가능 대상
IT보안담당자는 다음에 해당하는 PC · 서버에 대해, 백신 설치를 제외할 수 있다.
① Unix, Linux 설치 시스템
② 전용 어플라이언스 시스템
③ 네트웍 인터페이스 비활성화 상태 시스템
④ 내부 네트웍과 분리된 폐쇄망에 연결된 시스템

5.8.4 필요 자원

정보	인프라·업무환경
■ Windows PC 리스트 ■ Windows 서버 리스트	■ PC 백신 ■ Windows서버 백신

5.8.5 표준 통제요건
1) 백신 설치 및 기본 설정
IT보안담당자는 다음 기준에 따라 백신을 설치하고 기본 설정을 적용한다.
① Windows PC 및 서버에 백신 설치
② 백신 소프트웨어 정기 자동 업데이트 설정
2) 인터넷 접점구간 스팸메일 차단 서버 설치
IT보안담당자는 인터넷 접점구간을 통한 악성코드 유입을 차단하기 위해 스팸메일 차단 서버를 설치한다.
3) 사용자 백신 조작 차단
IT보안담당자는 백신 설치된 PC의 사용자가 임의로 백신의 작동을 조작할 수 없도록 조치한다.
4) 실시간 감시
IT보안담당자는 백신 소프트웨어의 실시간 감시를 활성화하고, 실시간 감시를 위한 기준을 수립 · 운영한다.
5) 디스크 전체 검사
IT보안담당자는 백신 설치된 PC · 서버 디스크 정기 전체 검사를 위한 기준을 수립 · 운영한다.

5.8.6 세부 통제요건
1) 사용자 백신 조작 차단
IT보안담당자는 다음 기준에 따라 사용자의 임의적인 백신 조작을 차단한다.
① 백신 설치된 PC의 사용자에 대해, administrator 권한 사용 금지
② PC 사용자에 의한 백신 강제 종료 불가한 제품 사용
2) 실시간 감시
백신시스템 운영자는 Windows PC · 서버에 대해, 다음 인터페이스를 대상으로 실시간 감시를 적용한다.
① 네트웍 인터페이스: 이더넷, 무선, 블루투스
② 입력장치
A. USB, IEEE1394, (micro) SD, ODD 드라이버
B. 기타 보조저장매체 연결 가능한 모든 입력장치
3) 디스크 전체 검사
백신시스템 운영자는 Windows PC · 서버의 디스크에 대해 다음과 같이 자동 전체 검사를 적용한다.
① Windows PC: 일 1회 주간 시간대(12:00~1:00) 자동 전체 검사
② Windows 서버: 일 1회 야간 시간대(17:00~08:00) 자동 전체 검사

5.8.7 산출물

산출물명	형태/위치	보존기한
Windows PC·서버 백신 설치 상태	백신 관리 서버	5 년

㈜화신 정보보안관리

5.9 패치 관리

5.9.1 프로세스 목표

관리대상 정보자산 시스템에 대해, 각 시스템의 코어 영역에 존재하는 취약점 제거를 위해서는 벤더가 제공하는 보안 패치가 필수적이므로, 이를 위한 요건을 정의한다.
모든 패치 대상 시스템에 대해 최신 보안 패치를 유지한다.

5.9.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 12.7 패치 관리

5.9.3 적용 대상

1) 표준 적용 대상
모든 시스템 자산: 서버, 응용시스템, DBMS, 네트웍 장비, 보안시스템, PLC 펌웨어
2) 실제 적용 대상
① Windows PC
② Windows 서버
3) 제외 가능 대상
IT보안담당자는 다음 시스템에 대해 패치를 제외할 수 있다.
① Unix/Linux 서버
② DBMS
③ 네트웍 장비
④ 보안시스템
⑤ PLC 펌웨어

5.9.4 필요 자원

정보	인프라·업무환경
■ N/A	■ Windows서버 업데이트 ■ NAC: PC Windows 강제 업데이트

5.9.5. 표준 통제요건

1) 취약점 정보 평가
PC · 서버 운영자는 Windows PC · 서버의 버전에 따른 기술 취약점 정보를 수집 · 평가한다. 단, 벤더의 공식 업데이트 서버를 통한 패치 적용 시 생략할 수 있다.
2) 패치 적용 방식
PC · 서버 운영자는 Windows PC · 서버에 대해, 자동 · 수동 패치 업데이트를 적용한다.
3) 패치 적용 시간
PC · 서버 운영자는 패치 적용으로 인한 업무 영향도를 고려하여, 패치 적용 시간대를 선정한다.

5.9.6 세부 통제요건

1) 패치 적용 방식 및 시간
① Windows PC
A. NAC 운영자는 Windows PC에 대해 자동 패치를 적용한다.
B. 패치 주기는 다음과 같이 설정한다.
일 1회 주간 시간대(12:00~1:00) 자동 업데이트
② Windows 서버 패치
A. Windows서버 운영자는 패치를 수동 적용한다.
B. 패치 주기는 다음과 같이 정한다.
a. 정기: 월 1회 수동 업데이트
b. 비정기: 긴급 패치 발견 시 수동 업데이트

2) 패치 소스 및 경로
① 패치 소스는 벤더의 공식 업데이트 서버를 통한다.
② 패치 경로는 네트웍을 활용할 수 있다.

5.9.7 산출물

산출물명	형태/위치	보존기한
패치 이력	패치 대상 PC 패치 대상 서버	5 년

5.10 보안 취약점 분석

5.10.1 프로세스 목표

관리대상 정보자산 중 핵심시스템에 대해, 시스템 인프라 진단, 웹 진단, 모바일 진단 등 시스템 보안 취약점 분석에 관한 요건을 정의한다.

5.10.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 12.8 보안 취약점 분석

5.10.3 적용 대상

3) 표준 적용 대상
모든 시스템 자산: 서버, 응용시스템, DBMS, 네트웍 장비, 보안시스템, PLC 펌웨어

4) 실제 적용 대상
① Windows, Unix, Linux 서버
② 웹기반 응용시스템
③ DBMS

5) 제외 가능 대상
① 네트웍 장비
② 보안시스템
③ PLC 펌웨어

5.10.4 필요 자원

정보	인프라·업무환경
■ 주요정보통신기반시설 취약점 분석·평가 상세 가이드	■ 모의해킹 도구 ■ 시스템 인프라 진단 도구

5.10.5 표준 통제요건

1) 취약점 분석 수행
① 취약점 분석 대상 선정 시, 해당 시스템 운영자와 협의 하에 선정한다.
② IT보안담당자는 취약점 분석을 위한 체크리스트를 정의한다.

2) 분석 수행인력
보안 취약점 분석 시, 전문성을 확보하기 위해 외부 전문업체에 의뢰하여 수행할 수 있다.

3) 분석 결과 보고 및 조치
① IT보안담당자는 점검 결과를 문서화하고 보안책임자에게 보고한다.
② 점검 결과 필요한 조치사항을 도출한다.

㈜화신 정보보안관리

5.10.6 세부 통제요건

1) 취약점 분석 수행

① 보안 취약점 분석 수행 주기는 다음과 같이 정한다.

A.정기 수행: 연 1회 이상 (시기 무관)

B. 비정기 수행: 보안 이슈 발생 시, 이슈와 관련된 범위에 대해 수행할 수 있다.

a.사회적으로 보안 취약점 이슈 발생 시

b. 회사 내부에서 시스템 보안 취약점에 의한 보안사고 발생 시

② IT보안담당자는 취약점 분석 시 <주요 정보통신기반시설 취약점 분석 · 평가 상세 가이드> 기반 수행을 원칙으로 한다.

2) 분석 대상

취약점 분석 대상을 다음 중 선택하여 수행한다.

① 모의해킹: 내부 웹 기반 업무시스템 (KMS, e-HR, PLM 등)

② 시스템 인프라 진단

A. 서버: Windows서버, Unix서버, Linux서버 (물리 서버, 가상 서버 무관)

B. DBMS

C. 네트웍 장비: 코어 영역 장비

D. 보안시스템

3) 분석 결과 보고 및 조치

① IT보안담당자는 분석 완료 후 1주일 내에 분석 결과를 보안책임자에게 서면 보고한다.

② IT보안담당자는 분석 결과 식별된 취약점에 대해 해당 시스템 담당자에게 통보하여 조치한다.

③ IT보안담당자는 조치 완료 후 조치 결과를 보안책임자에게 서면 보고한다.

5.10.7 산출물

산출물명	형태/위치	보존기한
보안 점검 결과 보고서	파일	5 년
보안 점검 결과 조치 보고서	파일	5 년

5.11 사용자 역할

5.11.1 프로세스 목표

IT보안담당자와 총무보안담당자가 조치해야 할 보안요건 외에, 사용자의 적극 참여가 필수적인 사항에 대한 요건을 정의한다.

5.11.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 9.4 인증정보 기밀성

5.11.3 적용 대상

1) 표준 적용 대상

보호대상 정보자산을 사용하는 내부 임직원 및 외부 협력업체 인력

2) 실제 적용 대상

보호대상 정보자산을 사용하는 내부 임직원 및 외부 협력업체 인력

3) 제외 가능 대상

N/A

5.11.4 필요 자원

N/A

5.11.5 표준 통제요건

IT보안담당자는 사용자 참여가 필요한 사항을 다음과 같이 정의한다.

1) 인증정보 노출 주의
2) 패스워드 정책
3) 저작권 보호

5.11.6 세부 통제요건

1) 인증정보 노출 주의

사용자는 본인 부주의에 의한 패스워드, OTP넘버 등의 인증정보의 노출을 방지하기 위해 다음 사항을 준수한다.

① 수기 메모 금지
② 개인 계정 패스워드 제3자에게 공유 금지
③ 공용PC 내 개인 계정 패스워드 저장 금지
④ OTP넘버 공유 금지
⑤ 사적 계정과 회사 계정에 대해 동일 패스워드 사용 금지

2) 패스워드 정책

① 사용자는 규정에 명시된 패스워드 정책을 기준 이상의 강화된 패스워드를 사용한다.
② 사용자가 숙지해야 할 패스워드 정책의 기본사항은 다음과 같다.

A. 최소길이: 최소 10자리 이상 사용 권장.
B. 복잡도: 영대문자, 영소문자, 숫자, 특수문자 중 3가지 이상의 조합 권장.
C. 변경주기: 90일마다 변경 권장. 패스워드 노출 의심 시 즉시 변경.

3) 저작권 보호

① 사용자는 회사 소유 PC에서 불법 소프트웨어를 설치·사용하지 않는다.
② 사용자는 회사 소유 PC에서 불법으로 획득한 컨텐츠를 사용하지 않는다.

5.11.7 산출물

N/A

6. 영역별 프로세스 : 물리 영역

6.1 보안구역 관리

6.1.1 프로세스 목표

관리대상 정보자산이 위치한 사업장에 대해, 각 업무 공간의 중요도에 따른 물리적 보안조치를 차별화하기 위한 보안구역 통제 관련 요건을 정의한다.
비인가자의 보안구역 출입을 방지한다.

6.1.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 6.3 모바일 기기 ■ 11.1 보안구역 ■ 11.3 딜리버리 영역

㈜화신 정보보안관리

6.1.3 적용 대상

1) 표준 적용 대상
ISMS 적용범위 사업장 전체

2) 실제 적용 대상
ISMS 적용범위 사업장 전체

3) 제외 가능 대상
없음

6.1.4 필요 자원

정보	인프라·업무환경
■ 사업장 배치도 ■ 사무실 배치도 ■ 전산실 배치도	■ 출입통제시스템 ■ CCTV ■ DVR시스템
■ 방문자 기본 신상정보 ■ 방문 목적 ■ 담당자 정보	■ 방문자관리시스템

6.1.5 표준 통제요건

4) 보안구역 정의
총무보안담당자는 다음과 같이 보안구역의 레벨을 구분한다.
① 제한지역
② 제한구역
③ 통제구역

5) 보안구역 지정
총무보안담당자는 각 업무공간별 중요도에 따라 보안구역을 지정하고, 필요한 보안조치를 구현한다.

6) 딜리버리 구역 지정
총무보안담당자는 외부와 거래하는 각종 장비, 시설, 물품, 자재 등을 발송·하역하기 위한 구역을 보안구역에 포함하여 정의하고, 필요시 보안조치를 적용한다.

7) 방문자 관리
총무보안담당자는 방문자 관리 시스템을 운영한다.

8) CCTV 운영
총무보안담당자는 전 사업장의 외곽 경비 및 공정 내 시설관리를 위해 CCTV를 운영한다.

6.1.6 세부 통제요건

9) 보안구역 지정
총무보안담당자는 다음 기준에 따라 통제구역을 지정하고 통제수단을 적용한다.

사업장	보안구역 구분	대상 업무공간	출입 허용 대상	통제 수단
언하동	제한구역	■ 사무동	■ 전 임직원	■ RF 출입키
		■ 경비동	■ 총무팀 ■ 경비인력	■ 경비인력 24 시간 상주
	통제구역	■ 사무동 2 층 전산실	■ 정보기술팀	■ RF 출입키
		■ 사무동 2 층 통신실	■ 총무팀	■ RF 출입키
		■ 공장동 PILOT동	■ 개발팀 ■ 생산팀	■ RF 출입키
		■ 기술연구소	■ 기술연구소	■ RF 출입키
	자재구역	■ 공장동 자재창고	■ 자재관리팀	■ 24 시간 상주/순찰
	납품구역	■ 공장동 물류창고	■ 물류관리팀	■ 24 시간 상주/순찰

㈜화신 정보보안관리

사업장	보안구역 구분	대상 업무공간	출입 허용 대상	통제 수단
봉동	제한구역	■ 사무동 층별 사무실	■ 전 임직원	■ RF 출입키
		■ 경비동	■ 총무팀 ■ 경비인력	■ 경비인력 24 시간 상주
	통제구역	■ 사무동 2 층 전산실	■ 정보기술팀	■ RF 출입키
		■ 사무동 2 층 통신실	■ 총무팀	■ RF 출입키
		■ 공장동 PILOT동	■ 개발팀 ■ 생산팀	■ RF 출입키
	자재구역	■ 공장동 자재창고	■ 자재관리팀	■ 24 시간 상주/순찰
	납품구역	■ 공장동 물류창고	■ 물류관리팀	■ 24 시간 상주/순찰

10) 방문자 관리

총무보안담당자는 방문자 출입 시 내부 촬영을 차단하기 위해 다음 사항을 조치한다.

① 방문자 입장 시

A. 경비 담당자는 방문자의 스마트 기기에 봉인 테이프를 부착한다.

B. 경비 담당자는 방문자 관리시스템에 봉인 테이프 부착 여부를 기록한다.

② 방문자 퇴장 시

A. 경비 담당자는 방문자 스마트 기기의 봉인 테이프 상태를 확인한다.

B. 경비 담당자는 방문자 관리시스템에 봉인 테이프 상태를 기록한다.

C. 경비 담당자는 방문자 스마트 기기의 봉인 테이프가 해제되어 있거나 해제되었던 흔적이 있는 경우, 총무보안담당자에게 통보한다.

D. 총무보안담당자는 해당 방문자의 담당자에게 통보하여 소명을 요구한다.

E. 경비 담당자는 방문자 관리시스템에 봉인 테이프 해제 소명 결과를 기록한다.

11) 기타

보안구역에 대한 기타 세부 통제요건은 다음 문서를 참조한다.

▶ HS-GP-GA04(보안관리규정)

6.1.7 산출물

표

산출물명	형태/위치	보존기한
언하동·봉동 보안구역 배치도	파일	5 년
신규입사자 업무연락서	KMS	5 년
방문자 출입기록 방문자 봉인 테이프 적용 기록	방문자 관리시스템	5 년

6.2 자산 반출입

6.2.1 프로세스 목표

내부 시스템의 외부 반출입 또는 폐기 시 시스템 저장장치 내 중요 데이터 유출 방지를 위한 요건을 정의한다.

6.2.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 11.4 장비 사용

㈜화신 정보보안관리

6.2.3 적용 대상

1) 표준 적용 대상

저장장치가 있는 장착된 전산장비 중, 저장된 정보 유출 시 보안위험이 예상되는 전산장비

2) 실제 적용 대상

① 서버 장비
② 퇴사자 PC
③ 타 사업장 전배자 PC
④ 외부인력 PC
A. 장기 상주 외부인력 (RF 출입키 발급)
B. 장기 상주 여부와 별개로, 민감한 정보를 취급한 것으로 IT보안담당자가 판단한 외부인력

3) 제외 가능 대상

① 네트웍 장비
② 보안시스템
③ 방문자 PC
④ 내부 인력 PC
⑤ 공장 라인 PC

6.2.4 필요 자원

정보	인프라·업무환경
■ 파기 대상 서버 정보 ■ 퇴사자 PC 정보 ■ 타 사업장 전배자 PC 정보 ■ 외부인력 정보	■ 디스크 파기 장치 ■ 디스크 소거 장치

6.2.5 표준 통제요건

1) 자산 반출입 기준

IT보안담당자는 자산 반출입 적용 대상을 식별하고, 반출입 시 보안요건을 정의한다.

2) 디스크 파기

IT보안담당자는 서버 장비에 대해 디스크 파기 절차를 수립 · 적용한다.

3) 디스크 소거

IT보안담당자는 디스크 소거 절차를 수립 · 적용한다.

6.2.6 세부 통제요건

1) 자산 반출입 기준

① IT보안담당자는 서버 최초 반입 후 반출을 불허함을 원칙으로 한다.
② 서버 유지보수는 외부인력의 방문을 통해 수행한다.
③ 서버 운영자는 방문 유지보수 시 유지보수용 PC를 지급하여 수행하도록 한다.

2) 디스크 파기

서버 운영자는 서버 폐기 시 디스크를 천공 후 이력을 기록한다.

3) 디스크 소거

① PC 관리자는 다음에 해당되는 경우 PC 재사용으로 인한 정보 유출을 방지하기 위해 디스크 소거 조치 후 결과를 기록한다.
A. 퇴사자, 타 사업장 전배자 PC 재사용
B. 내부인력 PC 회수 후 재사용
C. 상주 외부인력의 철수
② PC 관리자는 디스크 소거를 위한 전용 장비를 사용하여 소거한다.

6.2.7 산출물

산출물명	형태/위치	보존기한
서버/PC 디스크 파기 이력 서버/PC 디스크 소거 이력	파일	5 년

6.3 방재시설 관리

6.3.1 프로세스 목표

관리대상 정보자산이 위치한 사업장에 대해, 보안구역 내 중요 시스템 · 시설 영역에 대한 방재 관련 요건을 정의한다.
각종 재해 · 재난 상황 시 신속 대응하여 복구한다.

6.3.2 국내외 인증기준 관련성

구분	관련 프로세스
TISAX	■ 11.2 방재시설

6.3.3 적용 대상

1) 표준 적용 대상
ISMS 적용범위 사업장 전체
2) 실제 적용 대상
ISMS 적용범위 사업장 전체
3) 제외 가능 대상
없음

6.3.4 필요 자원

정보	인프라·업무환경
■ 각종 재해 위협 정보	■ 소방시설 ■ 발전시설, UPS ■ 공조시설

6.3.5 표준 통제요건

1) 재난 위협 식별
총무시설담당자는 천재지변, 공장 내 안전사고 등에 의해 발생할 수 있는 각종 재난 위협 상황을 식별한다.
2) 위협 대상 자산 식별
총무시설담당자는 각종 재난 위협에 영향받을 수 있는 전산장비 등 각종 자산을 식별한다.
3) 방재 설비 운영
총무시설담당자는 위협 대상 자산을 보호하기 위한 방재 설비를 구축하고, 비상 설비를 추가 운영한다.
4) 비상사태 대응 시나리오
총무시설담당자는 각종 비상사태 대응 시나리오에 재난 상황을 포함한다.

6.3.6 세부 통제요건

1) 재난 위협 식별
총무시설담당자는 재해 관련한 재난 위협을 다음과 같이 식별하고, 각 위협에 대응하기 위한 책임부서 및 관련부서를 지정한다.

㈜화신 정보보안관리

가상 비상사태 상황	개요
천재지변(운송사고 및 전염병) 발생	■ 외주자재 운송중 사고발생 ■ 전염병 발생
지진으로 인한 도장라인 화재	■ 자연재해(지진) 발생으로 도장라인 화재 ■ 화재로 인한 건조로, 보일러 훼손
프레스 라인 정지	■ 천재지변 및 사고로 인한 핫스탬핑 라인 파손/전복
도장라인 고장/사고 발생	■ 도장라인 화재발생으로 장비 고장 및 비가동 발생
설비 환경유해 발생	■ 설비 오작동으로 환경 유해 요소의 발생(GAS 누출, 유류 누출)

2) 방재 설비 운영
① 총무시설담당자는 정전 시 대응 절차를 수립 · 운영한다.
② 화재 세부 대응 절차는 다음 매뉴얼을 따른다.
▶ 화재 및 재난 대응 매뉴얼
▶ 18 지구대 조직 및 대응절차
3) 비상사태 대응 시나리오
① 총무시설담당자는 각종 비상사태 대응을 위한 비상계획의 작성을 관리한다.
② 총무시설담당자는 비상사태 상황별 책임부서를 지정하고, 책임부서가 작성한 상황별 비상대책서를 취합 관리한다.
③ 총무시설담당자는 비상사태 대응 시나리오를 연 1회 이상 검토하여 부사장 승인을 득한다.

6.3.7 산출물

산출물명	형태/위치	보존기한
2020 년 비상사태 대응 대책서	파일	5 년

㈜화신 안전 · 환경보건 경영방침

당사는 자동차용 Chassis 및 Body를 생산하는 자동차 부품 생산 전문 기업으로
제품의 설계 및 개발, 생산, 사용, 폐기에 따른 ESH 리스크 평가 결과를 통한
환경 및 안전보건에 미치는 영향을 최소화 하기 위하여
다음과 같은 방침을 개발하고 이행한다.

1. 환경/안전보건 관련 법규를 비롯한 제반 준수의무 사항을 철저히 준수한다.

2. 모든 활동, 제품, 서비스 분야에 대한 조직상황 분석 및 ESH영향을 파악하여 관련된 RISK를 최소화하기 위한 ESH경영목표를 수립, 지속적 개선활동을 실시한다.

3. 원부자재 LOSS의 최소화 및 재활용, 재사용, 폐기물 감량화 등을 추진하여 환경개선과 오염방지 활동을 지속적으로 전개한다.

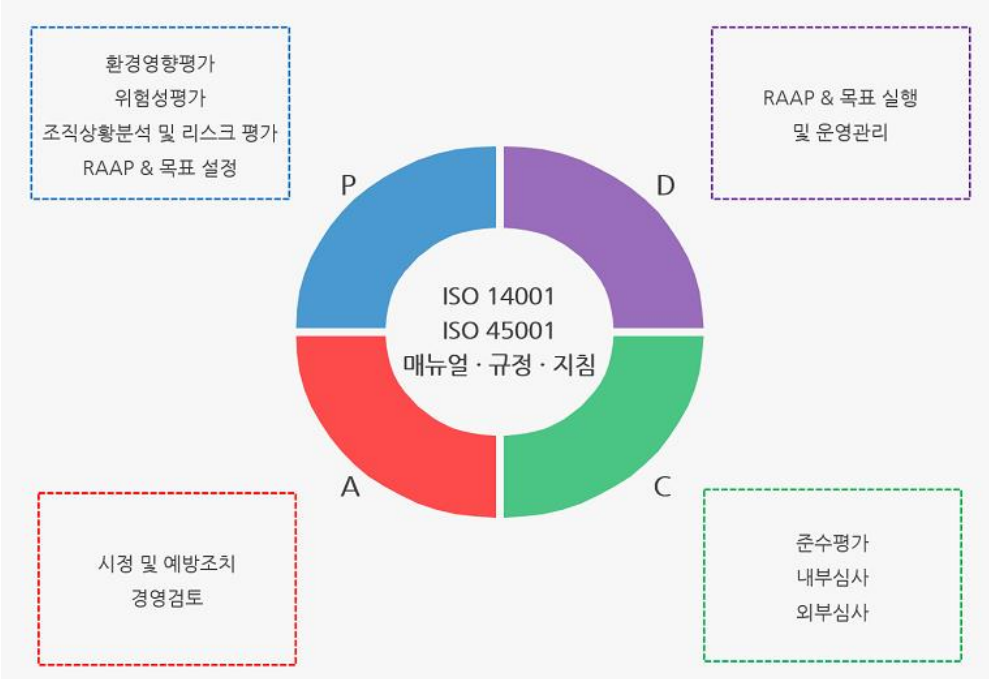
4. ESH경영에 관한 의식을 높이기 위하여 노사 간의 협력과 참여를 보장하고 임직원에 대해 교육, 훈련을 실시하고 당사의 ESH방침과 개선성과를 공표한다.

5. 안전보건 사건사고의 예방과 환경영향을 최소화하는 지속적 개선 활동을 수립, 실행, 유지한다.

ESH방침은 회사 내의 전 직원에게 전달되고 수행되어야 하며
계속적으로 효과가 있는지 검증되기 위해 정기적인 검토를 지속적으로 실행한다.
ESH 방침을 이해관계자에게 공개함으로써 개선 의지에 대한 우리의 결의를 밝힌다.

P.D.C.A 사이클이란?

P(Plan,계획), D(Do,실행), C(Check,평가), A(Act,개선) 반복을 통해 업무를 지속적으로 개선해 나가는 방법



㈜화신 환경관리

1. 목 적

본 규정은 당사 환경관리에 관한 기준을 설정하여 업무수행 중 예상되는 대기, 수질, 폐기물, 소음진동 및 천연자원사용 등 환경오염을 예방하고 오염물질 배출을 최소화하여 근로자에게 쾌적한 작업환경을 제공하고, 자연 및 생활환경을 지속적으로 보전하는데 그 목적이 있다.

2. 적용범위

당사에서 발생되는 환경오염에 대하여 관련규정을 근거로 관리하고 저감 시키는 업무에 적용한다.

3. 용어의 정의

3.1 담당임원

환경관리부서 담당중역으로 한다.

3.2 모니터링(측정 및 점검)

회사의 업무활동, 제품 및 서비스 수행 시 환경에 영향을 미칠 수 있는 특성들을 주기적으로 점검하고 측정함으로써 환경오염을 사전에 예방하기 위한 활동을 말한다.

3.3 오염물질

당사의 업무활동, 제품, 서비스 전반에 걸쳐 발생되는 대기 및 수질 오염물질, 폐기물 등을 말한다.

3.4 위탁 측정업체

당사에서 측정, 분석할 수 없는 측정 대상물질을 측정, 분석하는 외부 전문기관을 말한다.

3.5 대기오염물질

대기오염의 원인이 되는 가스, 입자상 물질 또는 악취 등의 환경오염 물질을 말한다.

3.6 특정 대기유해물질

사람의 건강, 재산이나 동·식물의 생육에 직접 또는 간접으로 유해를 줄 우려가 있는 대기오염물질을 말한다.

3.7 대기오염 물질 배출시설

대기오염물질을 배출하는 시설물, 기계, 기구를 말한다.

3.8 대기오염 방지시설

대기오염물질 배출시설로부터 배출되는 오염물질을 제거하거나 감소시키는 시설을 말한다.

3.9 수질오염물질

수질오염의 원인이 되는 물질로써 환경부령에서 정하는 것을 말한다.

3.10 폐수

물에 액체성 또는 고체성의 수질오염물질이 유입되어 그대로 사용할 수 없는 물을 말한다.

3.11 폐수 배출시설

수질오염물질을 배출하는 시설물, 기계, 기구를 말한다.

3.12 수질오염 방지시설

폐수 배출시설로부터 배출되는 오염물질을 제거하거나 감소시키는 시설을 말한다.

3.13 폐기물

회사의 활동 및 제품생산에 발생되는 물질로서 생산활동에서 더 이상 사용되지 아니하며, 대기중으로 배출되거나 오·폐수 관으로 유입되지 아니하는 고상 또는 액상물질을 말하며 생활폐기물과 사업장폐기물로 구분된다.

3.14 사업장 폐기물

3.14.1 지정폐기물

사업장폐기물 중 폐 전구, 폐 유리, 폐 비철금속, 폐유, 기름걸레, 폐 페인트 등 주변환경에 중대한 위험이 있는 물질로서 대통령이 정하는 폐기물을 말한다.

3.14.2 일반폐기물

사업장폐기물 중 지정폐기물을 제외한 폐기물을 말한다.

3.14.3 환경관리 계획

환경관리부서장이 연간 사업계획을 통하여 수립한 환경관리를 위한 연간 계획을 말한다.

㈜화신 환경관리

4. 책임과 권한

4.1 담당임원

1) 환경관리계획을 승인한다.
2) 배출시설 및 방지시설의 인·허가 신청을 승인한다.

4.2 환경관리부서장

1) 환경관리 운영계획을 수립한다.
2) 환경관련 교육훈련계획을 수립한다.
3) 배출시설에 대한 방지시설을 설치 및 정상 운영 되는지 지도 점검하여야 한다.
4) 신규 및 변경 유해물질에 대한 사용여부를 판단 검토하여야 한다.
5) 폐기물 위탁처리 업체를 선정 및 위탁처리 한다.
6) 폐기물 보관장소 유지 관리한다.
7) 환경목표, 세부목표 및 환경경영추진계획의 적절성과 이행성을 모니터링 한다.
8) 대 관청 업무를 수행한다.
9) 주기적으로 준수평가를 실시한다.
10) 조직상황분석 및 리스크평가 결과에 따른 운영관리기준의 변경관리
11) 환경 관련 협력업체 등록 및 관리

4.3 관련 부서장

1) 환경관련 설비구입 및 변경 전 환경관리부서장에게 검토를 요청하여야 한다.
2) 관련부서장은 사용중인 유해물질의 신규 또는 변경 시 환경관리부서장의 검토 및 합의를 받아야 한다.
3) 환경관리부서장의 요청 시 준수평가를 성실히 수행하여야 한다.
4) 조직상황분석 및 리스크평가 결과에 따른 부서 내 운영관리 기준의 제.개정

5. 업무절차

5.1 조직상황분석 및 RISK 평가

전 부서장은 환경관련 분야에 대한 조직상황분석 및 RISK평가를 실시하여 지속적 개선을 위한 운영관리 기준의 개선 및 EMS경영목표를 실행하여야 한다.

5.2 환경관리 계획수립

환경관리부서는 다음의 사항에 근거하여 사업계획수립 및 관리 규정에 의거하여 환경관리 계획을 수립한다.

5.2.1 환경방침 및 환경관리방향
5.2.2 전사 환경오염에 대한 실태파악과 대책
5.2.3 방지시설 설치에 대한 사항
5.2.4 중대한 환경문제
5.2.5 환경관련 교육훈련 내용
5.2.6 조직상황분석 및 RISK 평가 결과
5.2.7 기타 환경에 대한 중요사항

5.3 배출시설 및 방지시설의 설치 및 관리

5.3.1 배출시설 및 방지시설의 설치

1) 기존설비
① 환경관리부서는 기존 배출시설 및 방지시설의 환경기준치 준수유무를 지도 점검한다.
② 배출시설 및 방지시설 관리부서는 기존 배출시설 및 방지시설에 대하여 설비관리 규정에 따라 관리한다.
③ 관련부서는 배출시설 및 방지시설을 설비관리 규정에 따라 관리한다.

2) 신규설비 및 설비 변경
① 관련부서는 신규설비 설치 및 설비 변경 전 환경관리부서에 환경성 검토를 의뢰 한다.
② 환경관리부서는 신규설비 설치 및 설비 변경 시 법적 요건과 환경성 검토를 실시 하고 신규설비가 배출시설에 해당될 경우 관련부서와 협의하여 대표이사의 승인 후 관련 법규에 따라 인허가를 득하고 방지시설을 설치한다.

㈜화신 환경관리

5.3.2 배출시설 및 방지시설의 관리

1) 해당부서는 배출시설 및 방지시설에 대하여 적정하게 운전관리 될 수 있도록 배출시설 및 방지시설 설비유지 및 관리를 위한 지침을 제조설비관리 규정에 따라 작성 및 유지한다.
2) 해당부서는 배출시설을 적정 관리하여 오염발생을 최소화하여야 하며, 지속적인 공정 및 설비 개선을 위해 노력한다.
3) 해당부서는 배출시설 가동 시 해당 방지시설의 적정운전 여부를 확인 후 설비를 가동하고 배출시설 및 방지시설 운영기록부에 운영에 대한 기록 관리를 한다.
4) 해당부서는 배출되는 오염물질이 배출허용 기준 내에서 배출될 수 있도록 방지 시설을 정상 운영하여야 하며 설비 이상 발생 시 즉각 시정조치 하여야 한다.
5) 관련부서장은 배출시설 및 방지시설 이상 발생에 대하여 시정조치가 안되고 배출 시설 가동을 중지할 필요가 있을 경우에는 환경관리부서장에게 통보하고 관련 배출 시설 가동을 중지한 후 설비보전을 실시한다.
6) 해당부서는 배출시설 및 방지시설 수리가 완료된 후 이상이 없음을 확인한 후 환경관리 부서장에게 통보 후 배출시설 및 방지시설을 가동한다.
7) 설비관리는 설비관리 규정에 따른다.

5.4 폐기물 관리

5.4.1 폐기물 수집

1) 해당부서는 발생되는 폐기물을 성상별로 분리하여 수집, 운반하여 이를 지정된 장소에 보관한다.
2) 기름걸레 발생부서는 분리수거 후 마대자루 담은 후 지정된 저장소에 보관하여야 한다.
3) 절삭유 및 폐유액상이 발생하는 팀은 공드럼에 담은 후 누출되지 않게 밀폐하여 지정된 보관장소에 보관하여야 한다.
4) 폐유는 운반 전 폐기물 발생신고서를 작성하여 환경관리부서에 통보 후 누유 되지 않도록 조치 후 지정된 폐기물 보관장에 보관한다.

5.4.2 폐기물 운반

1) 발생되는 폐기물은 발생부서에서 보관장까지 운반 분리수거 한다.
2) 절삭유 및 폐유액상 발생부서는 운반도중에 흘려서는 안되며, 안전하게 운반 관리한다.
3) 중량 폐기물은 차량 및 기타 운반도구로 폐기물 보관장까지 운반한다.
4) 폐기물 운반 시 분리가 안된 폐기물에 대해서는 환경관리부서에서 폐기물 발생부서에 통보하여 시정조치를 하도록 한다.

5.4.3 보관

1) 폐기물은 지정 폐기물과 일반 폐기물로 구분하여 보관하며, 보관방법은 폐기물 관리법에 따른다.
2) 폐기물 보관장소는 집수통을 설치하여 누출수로 인한 제 2 차 오염을 예방한다.
3) 지정 폐기물 보관장소는 폐기물 관리법에 따라 폐기물량, 종류, 보관기간 등을 기재한 표지판을 설치하며, 드럼 등의 보관용기에 보관할 경우에는 용기 별로 보관 표지를 부착한다.
4) 폐기물 보관장의 설치 및 보관방법은 폐기물관리법에 따른다.
5) 재활용 폐기물은 분리 수거하여 정량 관리한다.
6) 환경관리부서는 폐기물 적치장 유지관리 상태를 점검하고, 발생되는 부적합 사항은 시정 및 예방 조치업무 규정에 따라 처리한다.

5.4.4 처리 업체 선정 및 위탁처리

1) 환경관리부서는 위탁처리업체 선정은 대관청 등록업체로 폐기물관리법에 따라 적법유무를 판단하여 선정한다.
2) 환경관리부서는 폐기물관리법에 따라 적법하게 위탁 처리한다.
3) 환경관리부서는 폐기물 위탁처리 시 중량을 계량하고, 폐기물적법시스템(올바로 시스템)을 사용하여 기록한다.
4) 환경관리부서는 폐기물 처리업체를 관리하며 부적합 시 시정하도록 통보한다.
5) 생활폐기물은 해당부서에서 분리수거 후 환경관리부서에 통보 처리한다.

5.4.5 지속적 관리

1) 환경관리부서는 연도별 폐기물 발생량을 비교 분석한다.
2) 폐기물 발생부서는 폐기물의 지속적인 감소를 위해 노력한다.

㈜화신 환경관리

5.5 모니터링 (측정 및 점검)

1) 배출시설 및 방지시설 운영부서는 배출된 오염물질이 배출 기준 내로 배출되고 있는지 정기적인 자가 측정을 실시하면 이를 환경관리부서에 통보한다. 자가측정 횟수와 방법은 환경법에 따른다.

2) 자가측정은 자체 또는 위탁측정업체에 의뢰하며, 결과를 자가측정 기록부에 기록하고 배출허용기준 초과 시는 시정 및 예방조치업무 규정에 따른다.

3) 배출시설 및 방지시설 운영부서는 자가측정에 따른 측정치가 기준치 보다 이상 일시 환경관리부서와 협의 후 배출시설 및 방지시설을 보완한다.

4) 측정 및 기록자료는 환경법 및 기록관리 규정에 따라 관리한다.

5) 환경담당자는 1 일 1 회이상 환경점검을 실시하며 그 내용을 "환경안전업무일지" 에 기록한다.

5.5.6 환경관리부서는 년 1 회이상 준수평가를 실시하다. 단, 법개정 및 대외적 환경변화에 따라 환경관리부서장이 필요하다고 판단 시 실시 할 수 있다.

5.6 폐기물 인계사항 기록 보존

환경관리부서는 환경법에 의해 폐기물적법시스템을 운영관리 한다.

5.7 대관청 업무

환경관리부서는 환경법에 따라 대관청 업무를 수행한다.

5.8 협력업체 관리

1) 평가방법

부품업체 평가규정(HSGP-0015)에 의거하여 평가한다.

2) 평가 예외사항

관공서의 허가를 받았거나 정부 지정업체인 경우 평가대상에서 제외한다.

6. 문서화 정보의 관리

환경관리 기록은 법적 서식을 기준으로 사용하며 그 보존연한은 법적 기준에 준하여 보존한다.

번호	기 록 명	최소보존기간	보관책임자
1	배출시설 및 방지시설 운영일지(수질)	3년	관련팀
2	배출시설 및 방지시설 운영일지(대기)	3년	관련팀
3	자가측정기록부	3년	관련팀
4	폐기물목록형관리	3년	관련팀
5	폐기물중간처리시설 운영관리대장	3년	관련팀
6	폐기물관리대장	3년	관련팀

7. 문서화 정보

1) 교육훈련 규정(HS-QP-HR02)
2) 시정 및 예방조치 규정(HS-QP-QA03)
3) 조직상황분석 및 리스크평가 규정(HS-ESH-GA13)
4) 유해물질 관리 지침(HS-EI-GA04)
5) 부품업체평가 규정(HSGP-0015)

8. 첨부

1) 배출시설 및 방지시설 운영일지(수질)(HS-EP-GA04-01)
2) 배출시설 및 방지시설 운영일지(대기) (HS-EP-GA04-02)
3) 폐기물목록형관리대장(HS-EP-GA04-03)
4) 폐기물중간처리시설 운영관리대장(HS-EP-GA04-04)
5) 폐기물관리대장(HS-EP-GA04-05)

㈜화신 생물다양성 정책

화신은 경영 활동 전반에서 발생 가능한 생태계 파괴를 예방하고 관련된 리스크를 최소화함과 동시에, 지역사회의 생물다양성을 보전하기 위해 본 정책을 선언한다.

본 정책은 국제사회의 생물다양성 협약 (Convention on Biological Diversity), 멸종위기에 처한 야생동식물종의 국제거래에 관한 협약(Convention on International Trade in Endangered Species of Wild Fauna and Flora) 등의 가이드라인을 참고하여 제정하였으며, 이에 따라 생물다양성 보전을 위한 국제 사회의 노력에 동참한다.

1. 목적

최근 환경오염, 지구온난화 등이 가속화됨에 따라 생태계는 급속도로 파괴되고 있으며, 많은 생물, 야생동식물이 멸종 위기에 놓여져 있습니다. 따라서 본 정책은 화신이 생물다양성 보전을 기후변화와 관련된 중요한 환경 문제로 인식하여 생물다양성의 보전 뿐만 아니라 생물다양성 증진, 야생 동식물, 관리 자원의 지속가능한 이용 실현 등을 위해 노력하며 생물다양성 보존에 대한 의무와 책임을 다하기 위해 제정하였습니다.

2. 적용범위

1) 화신의 모든 국내/외 임직원은 본 정책을 준수할 의무가 있습니다.
2) 협력사 등 거래관계에 있는 내·외부 이해관계자에게도 본 정책을 준수하도록 권장하겠습니다.
3) 본 정책에서 권장하고 있는 행위는 해당 국가의 법을 준수하여 적용하도록 하겠습니다.

3. 생물다양성 정책

1) 화신은 신규 거점 진출 및 사업장 확대 등을 수행함에 있어 생물 다양성을 위협하는 요소와 요인을 파악 및 예방하고 필요 시 조치를 취하겠습니다.
2) 화신은 모든 사업장에서 해당 국가와 지역의 법적 요건을 준수하여 중장기적으로는 생물다양성 저해와 손실 없는 사업 운영을 위해 노력하겠습니다.
3) 화신은 사업장 부지를 포함한 주변 지역과 지역사회의 생물다양성 보전·복원·확대, 서식지 보존 등과 같은 긍정적인 영향을 증진할 수 있는 위한 활동을 계획하고 추진하겠습니다.
3) 화신은 멸종 위기에 놓인 희귀종 및 고유종의 보호를 최우선으로 생각하여, 생물 다양성 보호 문제에 대한 이해를 높이기 위해 임직원 및 이해관계자들에게 관련 정보를 제공하도록 하겠습니다.
4) 화신은 지속가능한 자원 활용을 고려하고, 환경 친화적인 기술과 제품을 개발하도록 노력하겠습니다.

4. 실행방안

1) 경영활동에 관련된 의사결정 과정에서 중·장기적인 리스크 등을 분석하여 생물다양성 보전을 위한 절차와 거버넌스 체계를 구축하도록 하겠습니다.
2) 생물다양성 보존과 관련한 기준과 목표를 수립하여 실행될 수 있도록 모니터링 하겠습니다.

㈜화신 기업지배구조헌장

화신(이하 "회사")은 기업 본연의 지속 가능한 성장을 추구함과 동시에 이러한 노력이 고객의 만족, 구성원과 협력사의 성장, 주주이익의 극대화, 사회의 행복, 그리고 국가 경제 및 인류의 발전으로 이어질 수 있도록 진취적이며 균형적인 경영활동을 도모한다.

회사는 이러한 경영목표와 철학의 실현에 있어 보다 건전하고 투명한 지배구조의 구축이 그 기초가 됨을 인지하고, 「화신 기업지배구조 헌장」을 다음과 같이 제정함으로써 이를 회사 경영의 일반 원칙으로 한다. 다음과 같은 방침을 개발하고 이행한다.

회사는 본 헌장을 기초로 전문적이고 독립적인 이사회의 구성과 활동을 지원하고 이사회를 통해 경영진의 책임경영을 감독함으로써, 기업과 주주가치의 영속적인 발전을 추구하고 궁극적으로는 이해관계자의 신뢰와 존경을 받을 수 있는 기업이 되도록 한다.

제 1장 주주

제 1조 주주의 권리

① 주주는 주식회사 화신(이하 "회사" 라 한다)의 소유자로서 상법 등 관련 법령에서 정하는 다음의 기본 권리를 갖는다.
- 이익 분배 참여권
- 주주총회 참석 및 의결권
- 주주권 행사에 필요한 정보를 정기적이고 시의적절하게 제공받을 권리 등

② 정관의 변경, 합병, 영업양수도, 분할, 해산, 자본의 감소, 주식의 포괄적 교환 및 이전 등 회사의 존립과 주주권에 중대한 변화를 가져오는 주요 사항들은 주주총회에서 주주의 권리를 최대한 보장하기 위한 적법한 절차를 통해 결정된다.

③ 회사는 주주총회 사전에 모든 주주에게 의안 등에 대한 정보를 충분히 제공함으로써 주주가 충분한 기간을 갖고 검토할 수 있도록 하고, 주주총회 일정 및 장소 관련 주주권의 행사가 용이하게 이루어질 수 있도록 배려한다.

④ 주주는 상법 등 관련 법령에 따라 주주총회의 의안을 제안할 수 있으며, 주주총회에서 의안에 대하여 질의하고 설명을 요구할 수 있다.

제 2조 주주의 공평한 대우

① 주주는 보통 주 1주마다 1개의 의결권을 가지며, 회사는 상법 및 관련 법령이 정하는 기준에 따라 주주의 본질적 권리가 침해되지 않도록 공평하게 대우한다. 단, 특정 주주에 대한 의결권 제한은 법률이 정하는 바에 따라 이루어질 수 있다.

② 회사는 관련 법령에 따라 주주에게 필요한 정보를 적시에 충분하고 공평하게 제공한다. 또한 공시 의무가 없는 정보를 공개할 경우에도 모든 주주에게 공평하게 제공하여야 한다.

③ 회사는 위법한 내부거래 및 자기거래로부터 주주를 보호하며, 적절한 내부통제장치를 갖추어 관리한다.

제 3조 주주의 책임

① 주주는 자신의 의결권 행사가 기업 경영에 영향을 미칠 수 있음을 인식하고 회사의 발전과 이익을 위하여 적극적으로 의결권을 행사하여야 한다.

② 회사의 경영에 영향력을 행사하는 지배주주는 기업과 모든 주주의 이익을 위해 행동하고, 이에 반하는 행동으로 기업과 다른 주주에게 손해가 발생하지 않도록 노력해야 한다.

㈜화신 기업지배구조헌장

제 2장 이사회

제 4조 이사회의 기능

① 이사회는 관련 법령의 범위 내에서 회사 경영에 관한 포괄적인 권한과 책임을 가지며, 회사와 주주의 이익을 위해 주요 경영의사결정과 경영감독 기능을 수행하여야 한다.

② 이사회는 대표이사 또는 이사회 내 위원회에 권한을 위임할 수 있다. 다만, 법령 · 정관, 이사회 규정에서 정하는 주요한 사항은 제외한다.

제 6조 이사의 자격

① 이사는 관련 법령에서 정한 자격기준에 부합할 뿐만 아니라, 모든 주주와 이해관계자의 권익을 균형 있게 대변할 수 있는 자이어야 한다.

② 사내이사는 회사를 경영하는 고위 경영진으로서 회사의 사업과 관련된 풍부한 경험과 전문지식을 보유하고 직무 수행에 충분한 시간을 할애할 수 있어야 한다.

③ 사외이사는 금융, 회계, 법률, 경제, 지배구조 등 분야에 관한 전문지식이나 실무적 경험이 풍부한 자로서 회사와 중대한 이해관계가 없으며, 경영진과 특정주주로부터 독립적인 의사결정을 할 수 있어야 한다.

제 7조 이사회의 운영

① 이사회는 정기적으로 개최하는 것을 원칙으로 하되, 긴급한 의안이 있는 경우 임시 이사회를 개최한다. 이사회의 원활한 운영을 위하여 이사회의 권한과 책임, 운영절차 등을 구체적으로 규정한 이사회 규정을 제정 · 운영한다.

② 이사회는 의사진행에 관하여 안건, 경과 요령, 그 결과, 반대하는 자와 그 반대 이유를 기재한 의사록을 작성하고 이를 보관하여야 한다.

③ 이사회는 관련 법령에서 정하는 방식 및 범위에 따라 개별 이사의 이사회 참석 여부와 안건에 대한 찬반 여부 등 활동 내역을 공개한다.

제 8조 이사회 내 위원회

① 이사회는 업무수행의 전문성과 운영의 효율성을 높이기 위하여 정관이 정하는 바에 따라 이사회 내 위원회를 설치 · 운영할 수 있다.

② 위원회의 조직, 운영 및 권한 등에 관한 사항은 명문화된 규정에 따른다.

③ 이사회로부터 위임된 사항에 대한 위원회의 결의는 이사회 결의와 동일한 효력을 가지며, 위원회는 결의한 사항을 이사회에 보고하여야 한다.

④ 만약, 위원회가 결의한 사항에 중대한 문제가 발견될 경우, 이사회가 이를 충분히 논의하고 다시 결의할 수 있다.

제 9조 사외이사의 역할

① 사외이사는 이사회의 구성원으로서 회사의 중요한 경영 의사결정에 참여하고, 경영진의 업무를 감독하는 동시에 적절한 조언을 통해 경영진을 지원한다.

② 사외이사는 직무수행을 위해 충분한 시간을 투여하고, 이사회가 개최될 때에는 사전에 관련 자료를 충분히 검토한 후 참석하여야 한다.

③ 회사는 이사회 개최 전 사외이사의 직무수행에 필요한 정보를 충분히 제공하여야 한다.

④ 사외이사는 직무수행에 필요한 정보의 제공을 회사에 요청할 수 있고, 필요한 경우 정해진 절차에 따라 회사의 비용으로 임직원이나 외부 전문가 등의 지원을 받을 수 있다.

⑤ 사외이사는 충실한 직무 수행을 위해 과도한 겸직을 지양한다.

㈜화신 기업지배구조헌장

제 2장 이사회

제 10조 이사의 의무 및 책임

① 이사는 선량한 관리자로서 주의의무와 충실의무를 다하여 직무를 수행하며, 충분한 정보와 노력을 바탕으로 합리적 의사결정을 하여야 한다.

② 이사는 자기 또는 제3자의 이익을 위하여 그 권한을 행사하여서는 안 되고, 회사의 발전과 주주의 이익을 최우선으로 직무를 수행한다.

③ 이사는 직무수행상 얻어진 회사의 정보를 외부에 유출하거나, 자기 또는 제3자의 이익을 위하여 이용해서는 안된다.

④ 이사가 법령 또는 정관을 위반하거나 그 임무를 소홀히 한 때에는 회사에 대하여 법령에 따른 손해배상책임을 지며, 이사에게 악의나 중과실이 있는 때에는 제3자에 대하여서도 손해배상 책임을 진다.

⑤ 이사가 경영판단을 하는 과정에 있어 충분한 정보를 바탕으로 합리적인 판단에 의해 회사에 최선의 이익이라고 생각되는 방법으로 성실하게 직무를 수행하였다면, 그러한 이사의 경영판단은 존중되어야 한다.

⑥ 회사는 유능한 인사를 이사로 영입하기 위해 회사의 비용으로 이사를 위한 손해배상책임보험에 가입할 수 있다.

제 11조 평가 및 보상

① 이사회의 경영활동 내용은 공정하게 평가되어야 하며, 그 결과를 보수에 적정하게 반영하여야 한다.

② 이사의 보수는 주주총회에서 승인된 범위 내에서 집행된다.

③ 회사는 법령에 따라 주요 경영진의 보수 및 보수 지급 기준 등을 공시한다.

제 3장 감사기구

제 12조 감사위원회

① 감사위원회는 3인 이상 이사로 주주총회에서 선임하고, 독립성을 유지하기 위해 위원의 3분의 2 이상은 사외이사로 구성한다. 또한, 전문성의 유지를 위해 위원 중 1인은 회계, 재무 등 감사업무에 관한 전문적 식견을 갖춘 자로 임명한다.

② 감사위원회는 이사와 경영진 업무집행의 적법성, 기업재무활동의 건전성과 타당성, 재무보고의 정확성, 회계처리 기준의 타당성 등을 검토하며, 외부감사인의 선임 및 해임에 대한 승인과 주주총회에서의 보고 등을 수행한다.

③ 감사위원회는 감사업무에 필요한 정보에 자유롭게 접근할 수 있으며, 필요한 경우 외부기관 및 전문가 등에게 회사의 비용으로 자문을 요청할 수 있다.

④ 감사위원회는 정기위원회와 임시위원회로 하며, 필요한 경우 경영진, 재무담당 임원, 감사부서 임원에 보고를 요구하거나 외부감사인이 참석하도록 할 수 있다.

⑤ 감사위원회는 매 회의에 대한 의사록을 작성한다.

제 13조 외부감사인

① 외부감사인은 회사와 경영진 및 특정 주주 등으로부터 법적, 실질적으로 독립성을 유지하여야 한다.

② 외부감사인은 감사위원회에서 선임되며, 외부감사 활동 중에 확인한 중요사항 등을 감사위원회에 보고하여야 한다.

③ 외부감사인은 주주총회에 참석하여 감사보고서에 관한 주주의 질문이 있는 경우 이를 성실히 설명하여야 한다.

④ 외부감사인은 주식회사의 외부감사에 관한 법률 등 관련 법규에서 요구하는 바에 따라 회사의 존속가능성에 대해 고려하여야 한다. 외부감사인은 부주의한 회계감사로 인해 회사 및 정보이용자에게 발생한 손해를 배상할 책임이 있다. 외부감사인은 주주총회에 참석하여 감사보고서에 관한 주주의 질문이 있는 경우 이를 성실히 설명하여야 한다.

㈜화신 기업지배구조헌장

제 4장 이해관계자

제 14조 이해관계자의 권리보호

① 회사는 고객과 직원, 주주, 채권자, 협력사, 지역사회 등 다양한 이해관계자에 대한 기업의 사회적 책임을 다하기 위해 노력한다.

② 회사는 법령이나 계약에 의한 이해관계자의 권리를 보호하며, 근로기준법 등 노동관계법령을 성실히 준수함으로써 근로조건의 유지 · 개선에 노력한다.

③ 회사는 법령에서 요구되는 범위 내에서 이해관계자의 권리보호에 필요한 정보를 제공한다.

④ 회사는 공정거래 관련 법률의 준수를 통해 공정한 시장 질서의 확립을 촉진하며 국민 경제의 균형 있는 발전을 도모해야 한다.

⑤ 회사는 채권자의 지위에 중대한 영향을 미치는 합병, 감자, 분할 등의 사항에 대해 채권자 보호 절차를 준수한다.

제 5장 공시

제 15조 공시

① 회사는 정기적으로 사업보고서, 반기보고서 및 분기보고서 등을 작성하여 공시하며, 정기 공시 외에도 법적 의무사항 및 주주와 이해관계자에게 중대한 영향을 미칠 수 있는 중요 현안은 가능한 신속하고 정확하게 공시한다.

② 회사는 공시정보 이용자들에게 공평한 기회를 제공하기 위하여 이용자들이 동시에 동일한 정보에 접근할 수 있도록 공시한다.

③ 회사는 공시책임자를 지정하여 회사의 중요한 정보가 공시책임자에게 신속하게 전달될 수 있도록 내부 체계를 갖추어야 한다.

㈜화신 이사회 규정

2021.12.31 개정

제 1장 총칙

제 1조 [목적]

이 규정은 회사의 이사회 구성과 운영에 관하여 필요한 사항을 규정함을 목적으로 한다.

제 2조 [기능]

① 이사회는 법령 또는 정관에 정하여진 사항, 주주총회로부터 위임 받은 사항, 회사 경영의 기본방침 및 업무집행에 관한 중요사항을 의결한다.

② 이사회는 이사 직무 집행의 적법성 여부를 감독한다.

③ 이사회는 각 이사가 직무를 수행함에 있어 법령 또는 정관에 위반하거나 현저히 부당한 방법으로 처리하거나 할 염려가 있다고 인정한 때에는 그 이사에 대하여 관련 자료의 제출, 조사 및 설명을 요구할 수 있다.

④ 제3항의 경우에는 이사회는 그 사안에 대하여 그 집행의 중지 또는 변경을 요구할 수 있다.

⑤ 이사회는 그 결의로 이사회에서 결정된 사항의 집행을 위한 구체적인 사항의 결정을 대표이사에게 위임할 수 있다.

제 3조 [구성]

① 이사회는 대표이사를 포함한 주주총회에서 선임된 이사 전원으로 구성된다.

② 회사는 이사회 내에 감사위원회를 둔다.

제 2장 이사회 소집

제 5조 [소집]

① 이사회는 이사회 의장 또는 대표이사가 필요 또는 타당하다고 인정할 때 또는 1인 이상 이사의 청구가 있고 그 청구가 정당한 이유가 있다고 인정될 때, 이사회 의장 또는 대표이사가 이를 소집한다.

② 상법 제393조 제4항에 따라 정기 이사회는 매 분기 1회 개최를 원칙으로 하며, 필요에 따라 수시로 임시 이사회를 개최할 수 있다.

제 6조 [소집통지]

① 이사회 소집통지는 이사회 의장, 대표이사 또는 이사회 의장이 지명한 이사의 지시에 따라 이사회 간사가 회의일자, 장소, 목적사항을 이사회 심의에 필요한 정보 및 자료와 함께, 회의일보다 적어도 1일 전에 각 이사에게 통지한다.

② 전항의 소집통지는 각 이사에게 문서, 전자문서 또는 구두로써 할 수 있다.

③ 이사회는 본 조 제1항의 목적사항에 관하여서만 의결을 할 수 있다.

④ 이사회는 사전 또는 사후에 이사 전원의 서면 동의가 있을 때에는 본 조 제1항의 절차를 따르지 않고 개최될 수 있다.

㈜화신 이사회 규정

2021.12.31 개정

제 3장 이사회 결의사항

제 7조 [주주총회, 이사회 및 기타 경영지배구조 관련 사항]

① 주주총회의 소집 및 부의 안건 채택(전자적 방법에 의한 의결권의 행사 허용)

② 주주명부의 폐쇄 및 기준일 지정

③ 주주제안에 대한 심의 및 주주총회 부의 여부에 대한 결정

④ 대표이사, 각자 대표이사 또는 공동 대표이사의 선임

⑤ 대표이사에게 그 직무를 수행하지 못할 사정이 있을 경우, 이사회, 주주총회를 주재할 이사의 순위 결정

⑥ 이사회의 연기 및 속행의 결의

⑦ 사외이사 제도에 관한 사항

⑧ 지배인의 선임 또는 해임

⑨ 명의개서대리인의 선임

⑩ 주주대표소송에 있어서 소송 참가

⑪ 지점의 설치, 이전 또는 폐지

⑫ 정관의 변경

⑬ 이사회규정의 제·개정 및 폐지

⑭ 이사에 대한 전문가 조력의 결정

⑮ 이 규정 전문에서 정한 경영기본이념의 실행을 위한 회사 경영관리체계의 정립 및 수정

⑯ 내부회계관리규정 제·개정

⑰ 임원관리규정의 제·개정

⑱ 간이 주식교환, 간이 합병, 간이 분할합병, 소규모 주식교환, 소규모 합병 및 소규모 분할합병 등의 결정

제 8조 [투자 및 기획관리 사항]

① 당사가 발행주식 총 수의 50%를 초과하여 지분을 보유하는 회사로서, 출자액의 규모가 자기자본의 100분의 5 이상의 회사의 설립, 합병, 분할, 해산, 주권 상장 및 코스닥 상장

② 자기자본의 100분의 5 이상의 타 법인에 대한 출자 및 출자지분의 처분

③ 자산총액의 100분의 5 이상의 자산의 취득

④ 자기자본의 100분의 10 이상의 신규 시설 투자, 시설 증설 또는 별도 공장의 신설

⑤ 회사의 합병/분할 등에 관한 사항

⑥ 회사의 해산 및 회사의 계속

⑦ 자기자본의 100분의 10에 해당하는 금액을 초과하는 영업의 양수 또는 양도. 단, 다음 각 항목 중 1에 해당하는 사항에 대해서는 출석 이사의 3분의 2 이상의 찬성이 있어야 한다.

1. 양수 또는 양도하고자 하는 영업부문의 자산액이 최근 사업연도 회사 자산총액의 100분의 10 이상인 영업의 양수 또는 양도
2. 양수 또는 양도하고자 하는 영업부문의 매출액이 최근 사업연도 회사 매출액의 100분의 10 이상인 영업의 양수 또는 양도
3. 영업의 양수로 인하여 인수할 부채액이 최근 사업연도 회사 부채총액의 100분의 10 이상인 영업의 양수
4. 영업 전부의 양수
5. 영업 전부의 임대 또는 경영위임, 타인과 영업의 손익 전부를 같이 하기로 하는 계약 및 기타 이에 준하는 계약의 체결, 변경 또는 해약

㈜화신 이사회 규정

2021.12.31 개정

제 3장 이사회 결의사항

제 9조 [회계 및 재무관리 사항]

① 재무제표(연결재무제표 포함) 및 영업보고서 그 밖에 회사의 재무상태와 경영성과를 표시하는 것으로서 상법 시행령에서 정하는 서류의 승인

② 중간배당, 주식배당

③ 준비금의 자본전입

④ 신주의 발행

⑤ 정관에 따른 주주 이외의 자에 대한 신주 발행에 관한 사항

⑥ 실권주 및 단주의 처리

⑦ 자본 감소

⑧ 주식의 액면분할 및 병합

⑨ 자기주식의 취득 및 처분 또는 이를 목적으로 하는 신탁계약 등의 체결 및 해지

⑩ 주식의 포괄적 교환, 주식의 포괄적 이전

⑪ 사채의 발행 (대표이사에게 사채의 금액 및 종류를 정하여 1년을 초과하지 아니하는 기간 내에 사채를 발행할 것을 위임할 수 있음)

⑫ 전환사채, 신주인수권부사채, 이익참가부사채, 교환사채 등 특수 사채의 발행사항 결정

⑬ 10억원을 초과하는 증여 또는 기부. 단, 태풍, 홍수, 화재, 지진 등 천재지변으로 인한 긴급 구호 제공과 “사회복지공동모금회법” 에 따른 기부는 선 집행 후 사후 보고할 수 있다.

⑭ 회사 주요 자산의 담보제공 또는 처분. 단, 회사 주요 자산이라 함은 장부가액 또는 감정가액이 자기자본의 100분의 5를 초과하는 자산을 말한다.

⑮ 자기자본의 100분의 5를 초과하는 국내외 차입계약(1년 이내의 단기차입 제외) 및 자기자본의 100분의 5를 초과하는 타인을 위한 채무보증

⑯ 이익배당한도 내의 주식소각

⑰ 대규모의 자금도입 및 보증행위

⑱ 중요한 재산에 대한 저당권, 질권의 설정

제 10조 [인력 및 조직관리 사항]

① 주식매수선택권의 부여 및 부여의 취소

② 상법 제398조(이사 등과 회사 간의 거래)의 이사회 승인

③ 이사의 경업거래의 승인 및 승인 없는 경업거래에 대한 개입권 행사

④ 상법 제397조의 2(회사의 기회 및 자산의 유용 금지)의 이사회 승인

⑤ 임원배상책임보험 가입 및 기타 임원의 책임 부담에 대한 구제 제도의 도입

⑥ 이사 해임 안 제출

⑦ 공정거래자율준수관리자의 선임 또는 해임

⑧ 상법 제542조의 13(준법통제기준 및 준법지원인)에 따른 준법지원인의 임면, 준법통제 기준의 제정 및 변경

⑨ 이사와 감사위원회의 보수는 주주총회에서 이사 전원에 대한 보수 총액 또는 그 상한을 정하고, 개별 이사의 보수 결정을 그 범위 내에서 이사회에 위임한 경우 개별 이사에 대한 보수액 결정을 포함한다.

㈜화신 이사회 규정

2021.12.31 개정

제 3장 이사회 결의사항

제 11조 [기타 주요 경영사항]

① 독점규제 및 공정거래에 관한 법률 제11조의2(대규모내부거래의 이사회 의결 및 공시)에서 이사회 의결사항으로 정한 사항

② 상법 제542조의 9(주요주주 등 이해관계자와의 거래)에서 이사회의 승인사항으로 정한 사항

③ 기타 법령 및 정관에 정하여진 사항, 주주총회에서 특별히 위임 받은 사항 및 대표이사가 필요하다고 인정하는 중요 사항

제 12조 [결의사항의 위임 및 보고사항]

① 이사회는 법령 및 정관에 위반되지 않는 범위 내에서 본 장에 명시된 이사회 결의사항 중 일부를 각 위원회에서 정하도록 할 수 있다.

② 본 장에 명시되지 않은 일체의 사항에 관하여는 대표이사가 이 규정에 의하여 위임되고 부여된 권한 하에서 이를 결정·집행한다.

③ 대표이사는 이사회가 정하는 바에 따라 다음 각 호의 사항에 대한 권한과 책임을 갖는다.

6. 이사회에 의하여 의결된 사항의 달성, 시행 및 집행
7. 이사회의 의결을 요하는 사항 이외의 제반 사항 결정 및 집행
8. 회사의 전반적인 업무집행에 관한 조치를 취하고 계약 체결을 위한 서명 또는 기명날인을 하며, 회사를 대표하여 약정을 하는 행위
9. 임직원에 대한 순차적인 권한의 재위임
10. 하기 사항에 관한 이사회 보고
    1) 연간 경영계획
    2) 분기 경영실적
    3) 정기 임원인사 및 조직개편
    4) 자기자본의 100분의 5를 초과하는 타법인 출자 및 출자지분의 처분, 자산의 취득, 신규 시설투자, 시설 증설에 대한 분기별 실적
    5) 이사회가 대표이사에게 사채발행을 위임한 경우 그 집행 결과
    6) 기타 대표이사가 필요하다고 판단하는 사항

④ 대표이사 또는 대표이사로부터 위임을 받은 내부회계관리자는 내부회계관리제도의 운영실태를 이사회 및 감사위원회에 연 1회 보고하고, 감사위원회는 내부회계관리제도의 운영실태를 평가하여 이사회에 연 1회 보고한다.

⑤ 공정거래자율준수관리자는 공정거래자율준수프로그램의 운영실적 및 계획을 이사회에 반기 1회 보고한다.

⑥ 준법지원인은 준법통제기준의 준수여부를 점검하여 그 결과를 연 1회 이사회에 보고하여야 한다.

제 4장 이사회 심의 의결

제 13조 [관계인의 출석]

이사회는 안건 심의와 관련하여 필요할 경우 이사회의 구성원이 아닌 임직원, 외부인사 등을 출석시켜 안건에 대한 설명이나 의견을 청취할 수 있다.

제 14조 [의결의 채택]

① 이사회 업무를 처리함에 있어 이사 전원의 과반수를 회의 정족수로 한다.

② 이사회의 결의는 이사 과반수의 출석과 출석이사 과반수로 한다. 다만, 상법 제397조의2 및 제398조에 해당하는 사안에 대한 이사회 결의는 이사 3분의 2 이상의 수로 한다.

③ 상법 제391조, 제368조 제3항, 제371조 제2항, 제415조의2 제3항에 의거하여 제1항의 정수는 정관으로 그 비율을 더 높게 규정하여 강화할 수 있다.

㈜화신 이사회 규정

2021.12.31 개정

제 4장 이사회 심의 의결

제 15조 [의사록]

① 이사회의 의사에 관하여는 의사록을 작성한다.

② 의사록에는 의사의 안건, 경과요령, 그 결과, 반대하는 이사와 그 반대이유를 기재하고 출석한 이사가 기명날인 또는 서명한다.

③ 주주는 영업시간 내에 이사회 의사록의 열람 또는 등사를 청구할 수 있다.

④ 회사는 정당한 이유가 있는 경우 제3항의 청구에 대하여 이유를 붙여 이를 거절 할 수 있다. 이 경우 주주는 법원의 허가를 얻어 이사회 의사록을 열람 또는 등사할 수 있다.

제 5장 이사

제 16조 [이사의 의무]

① 이사는 법령 및 정관에 의거하여 신의성실의 원칙에 따라 선량한 관리자의 주의로 업무를 수행하여야 한다.

② 이사는 전항과 관련하여 회사 내 담당 임직원이 작성 또는 제출한 품의서, 통보서, 보고서 및 각종 회계자료 등과 회계사, 감정평가사, 변호사 등 외부의 관련 전문가들이 제출한 보고서 등 그리고 회사 내 각종 전문위원회의 의견 등을 신뢰하고 이에 의존하여 업무를 수행할 수 있다.

③ 이사는 이사회의 사전 승인이 없으면 자기 또는 제3자의 계산으로 회사의 영업부류에 속한 거래를 하지 못한다. 만약, 이사가 이에 위반하여 자기 또는 제3자의 계산으로 회사의 영업 부류에 속한 거래를 한 경우, 이사회는 그 이사의 거래가 자기의 계산으로 한 것인 때에는 이를 회사의 계산으로 한 것으로 볼 수 있고, 제3자의 계산으로 한 것 인 때에는 그 이사에 대하여 이로 인한 이득의 양도를 청구할 수 있다.

④ 이사는 이사회의 사전 승인이 없으면 동종 영업을 목적으로 하는 다른 회사의 무한책임사원이나 이사가 되지 못하며, 동종 영업을 목적으로 하는 다른 회사의 무한책임사원이나 이사가 회사의 이사로 선임된 경우, 이사회는 당해 이사로 하여금 다른 회사의 무한책임사원이나 이사의 직을 사임토록 요구할 수 있다.

⑤ 이사는 이사회의 사전 승인이 없으면 자기 또는 제3자의 계산으로 회사와 거래 할 수 없다.

⑥ 이사는 재임 중에는 물론 퇴임 후에도 업무 수행과 관련하여 알게 된 회사의 비밀을 최선의 주의를 다하여 관리하여야 하며, 회사의 비밀을 이용하여 자기 또는 제3자의 이익을 도모하여서는 아니 된다.

⑦ 이사는 업무와의 관련 여부를 불문하고 회사의 명예나 위신을 실추시키지 않도록 품위를 유지하여야 한다.

⑧ 이사가 본 조에 규정된 의무를 이행하지 않은 경우, 회사는 당해 이사에 대하여 손해배상을 청구하거나 당해 이사를 해임할 수 있다.

⑨ 이사는 이사회의 사전 승인이 없으면, 직무를 수행하는 과정에서 알게 되거나 회사의 정보를 이용한 사업기회 또는 회사가 수행하고 있거나 수행할 사업과 밀접한 관계가 있는 사업 기회를 자기 또는 제 3자의 이익을 위하여 이용하여서는 아니 된다.

⑩ 이사는 필요 시 회사의 비용으로 외부 전문인력의 도움을 구할 수 있다.

부칙

제 1조 [시행일]

이 규정은 2019년 12월 31일부터 시행한다.