문서관리번호	JH-ESG-09
제정일	2024. 10. 01
문서관리자	이재식부장

(주)진 흥 주 물
정보보호 정책

2024. 10. 01

결재	작성자	이 사	전 무	사 장

제1장 정보보호 선언문

미래를 이끄는 (주)진흥주물의 기술력 및 사업 환경에 있어 핵심기술(국가핵심기술 포함) 정보 의 유출 위협은 업무 및 정보 자산에 심각한 영향을 미칠 수 있으므로 정보보호 활동은 필수 불가결한 요소가 되다. 따라서 (주)진흥주물의 임직원은 모든 역량을 동원하여 정보 유출, 해킹 등 각종 정보보안 위협으로부터 안정적이며 신뢰성 높은 안정적 업무 운영을 유지하기 위해 정 보보호 관리체계 수립 및 이행에 최선을 다하여야 하며 이에 다음과 같이 정보보호 정책을 수 립하고 선포한다.

우리의 보호 대상은 다음과 같다.
업무를 위해 자체 생산된 핵심 기술(국가핵심기술 포함) 정보
업무 운영을 통해 수집된 개인정보
업무 운영을 위한 서버/네트워크 등 IT 인프라 설비
회사의 업무 수행을 위해 필요한 중요 사업 정보 및 업무환경 자산
업무 처리를 위한 물리적 장소

우리는 (주)진흥주물의 안전한 정보보호 관리 실현을 위하여 다음과 같은 활동을 수행함으로써 정보보호 목표를 달성하도록 노력한다.

정보, 기술 및 자산을 보호하기 위한 정보보호 관리체계를 수립한다.
정보보호 업무수행을 위한 인적 구성, 시설과 제도 등을 마련한다.
정보, 기술 및 자산에 대한 관리적, 물리적, 기술적 정보보호 지침을 수립하고 실천한다.
정보보호 지침을 실천할 수 있도록 조직 내부에 널리 알리고 관련 교육을 실시한다.
보안사고 관리, 사업 연속성(재해 예방)관리, 법적 준거성 이행을 위한 기본 대책을 수립하고 실천한다.

이를 위해 경영진은 다음과 같이 필요한 자원을 적극 지원한다.
정보보안을 위한 충분한 예산을 확보하여 지원한다.
정보보안을 위해 필요한 조직을 구성하고 충분한 인적자원을 지원한다.
정보보안에 필요한 충분한 내/외부 교육을 지원한다.
정보보안 활동이 지속적으로 이행될 수 있도록 보장하고 지원한다.

외부 업무환경 변화에 따라 본 정책이 지속적으로 유효성을 지닐 수 있도록 전사보안책임자 는 주기적으로 정보보호 정책 및 지침의 유지 변경 작업을 수행하며, 임직원에 대한 정보보호교 육을 수행하여야 한다. 또한 ㈜진흥주물의 전 임직원은 정보보호 정책 및 이에 기반한 지침을 준수하는 데 있어 신의와 성실의 원칙으로 임하며, 정보보호 활동이 지속적으로 유지 및 발전될 수 있도록 맡은 바 소임을 다하여야 한다.

2024년 10월
주식회사 진흥주물

제2장 총칙
제1절 일반사항

제1조【목적】
본 정보보호 정책은 정보보호의 기본이 되는 최상위 문서로서 ㈜진흥주물(이하 '회사' 또는 '당사'라 한다.)의 정보보호 활동에 필요한 기본 방침 결정을 목적으로 한다.

제2조【적용범위】
본 정책은 회사의 국내외 업무 관련 모든 정보, 전산 인프라, 인력을 보호하기 위한 전체 정보보호 업무를 대상으로 한다.
본 정책은 해외법인을 포함한 회사 및 모든 협력업체에 동일하게 적용한다.

제3조【용어 정의】
본 정보보호 정책 내에서 사용되는 용어는 필요한 경우 각 하위 문서에서 별도로 규정하여 사용할 수 있다.
정보보호 선언문: 정보보호에 대한 기본 방향 및 원칙을 정의한 문서
정보보호 조직: 정보보호 관리 수행 체계(조직 및 인원)을 의미함
정보 자산: 정보보호의 대상이 되는 정보, 정보시스템, 시설 등을 의미함
업무 연속성: 재해 재난으로 정상적인 운용이 어려운 데이터 백업과 같은 단순 복구 뿐 아니라, 서비스의 지속적 보장, 핵심업무를 지속적으로 제공할 수 있는 환경 조성 을 의미함

제4조【준용】
본 정책에 따라 회사의 모든 정보보호 업무를 처리하며 이에 명시되지 않은 사항은 관련 법령 및 사규가 정하는 바에 따른다.

제2절 책임 및 권한
제5조【전사보안책임자】
전사보안책임자는 본부장이 담당한다.
전사보안책임자는 정보보호 협의회 위원장직을 겸직한다.
전사보안책임자는 회사 정보보호 업무에 대한 총괄 책임을 가지며 정보보호 업무 수 행을 위한 지시와 감독 권한을 소유한다.
정보보호 관련 제규정(정책, 지침, 절차 등)에 대한 승인 권한을 갖는다.

제6조【정보보호 최고책임자】
정보보호 최고책임자는 정보보호 주관 조직장이 담당한다.
정보보호 최고책임자는 전사보안책임자를 보좌하여 정보보호 업무의 기획, 실행, 평가, 개선에 대한 실무를 관리할 책임을 갖으며, 정보보호협의회 간사직을 겸직한다.

정보보호 업무를 효과적으로 운영하기 위한 지침을 수립하고 시행할 책임을 갖는다.
정보보호 관련 지침의 기준에 따라 자체적으로 정보보호 현황을 점검한다.
정보보호 최고책임자 국내법에서 요구하는 자격 요건을 갖추어야 한다.

① 정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위를 취득한 사람

② 정보보호 또는 정보기술 분야의 국내 또는 외국의 학사학위를 취득한 사람으 로서 정보보호 또는 정보기술 분야의 업무를 3년 이상 수행한 경력(학위 취득 전의 경력을 포함한다)이 있는 사람

③ 정보보호 또는 정보기술 분야의 국내 또는 외국의 전문학사학위를 취득한 사 람으로서 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행한 경력(학위 취득 전의 경력을 포함한다)이 있는 사람

④ 정보보호 또는 정보기술 분야의 업무를 10년 이상 수행한 경력이 있는 사람

⑤ 정보보호 관리체계 인증 심사원의 자격을 취득한 사람

⑥ 정보보호 관련 업무를 담당하는 부서의 장으로 1년 이상 근무한 경력이 있는 사람
정보보호최고책임자는 다음 각 목의 업무를 겸할 수 있으나 이외는 겸할 수 없다.

① 정보보호산업의 진흥에 관한 법률 제13조에 따른 정보보호 공시에 관한 업무
② 정보통신기반 보호법 제5조5항에 따른 정보보호책임자의 업무
③ 전자금융거래법 제21조의2제4항에 따른 정보보호최고책임자의 업무
④ 개인정보보호법 제31조제2항에 따른 개인정보보호책임자의 업무
⑤ 그 밖에 이 법 또는 관계법령에 따라 정보보호를 위하여 필요한 조치의 이행

기타 본 지침에서 언급되지 않은 사항은 국내법 및 정보보호 관련 다른 지침을 따른다.

제7조【전사보안실무자】
정보보호 업무의 분야별 실무를 담당한다.
관리보안담당 실무자: 보안주관부서 관리 보안 실무 담당자
물리보안담당 실무자: 보안주관부서 물리 보안 실무 담당자
기술보안담당 실무자: 보안주관부서 기술 보안 실무 담당자
정보보호 정책 및 지침을 문서화하고 변경사항을 관리할 책임을 갖는다.
부서(팀)의 정보보호 활동을 지원할 책임을 갖는다.
기타 본 지침에서 언급되지 않은 사항은 국내법 및 정보보호 관련 다른 지침을 따른 다.

제8조【지역 보안 책임자】
본사 외 지역 보안 책임자는 근무 지역을 책임지는 임원으로 선임한다.
회사의 모든 정보보호 관련 제규정에 따라 지역의 정보보호 업무를 총괄할 책임을 가진다.

제9조【부서(팀)보안책임자】
부서(팀)보안책임자는 팀(부서)장이 담당한다.
부서(팀)보안책임자는 부서(팀) 정보보호 업무를 총괄할 책임을 갖는다.
부서(팀)보안책임자는 부서(팀)보안담당자를 지정하여 부서(팀) 보안 업무를 이행, 지 시, 감독할 책임을 갖는다.

제10조【부서(팀)보안 담당자】
부서(팀)보안담당자는 부서(팀)의 모든 정보보호 활동을 수행하고 현황을 관리할 책임 을 갖는다.
부서(팀)보안담당자는 부서(팀) 정보보호 활동을 위해 보안실무책임자와 지속적으로 의사소통하고 협조를 구해야 한다.
부서(팀)보안담당자는 정보보호 활동 실행 결과를 부서(팀)보안책임자에게 보고해야 한다.
부서(팀) 보안담당자는 매월 보안의 날 행사를 시행하여 자체 보안점검, 보안교육을 시행하고 결과를 보안 포털에 상신 보고하여야 한다.
부서(팀) 보안담당자는 년1회 정보자산분류를 시행한다.
부서(팀) 보안담당자는 보안 포털의 보안 스티커 관리대장을 최신화 유지하여야 한다.
부서(팀) 보안담당자는 보안점검 결과 취약점을 지속적 개선이행 하여야 한다.

제3장 정보보호 정책
제11조【정보보호 기본원칙】
임직원이 업무상 이용하는 모든 정보 자산은 회사의 자산이며, 회사가 소유권을 가진 다.
모든 정보 자산은 형태 및 중요도에 따라 분류하여 관리한다.
모든 정보 자산은 인가된 사용자에게만 접근을 허용한다.
정보보호담당자는 외부로부터 내부로의 접근은 최소한으로 제한하며, 접속시에는 침해사고에 대비하여 사전에 보안대책을 강구하여야 한다.
구매된 모든 소프트웨어는 회사가 소유권(또는 사용권)을 가지며, 라이센스 계약에 따르지 않고는 불법적으로 복제될 수 없다.
기술 보안 책임자는 각종 재해 및 장애 시 전산망의 안정성 및 신뢰성을 확보하기 위하여 비상계획을 수립하고 그것의 유효성을 지속하기 위하여 주기적으로 테스트한 다.
정보보호 담당 인원은 주기적인 보안 점검 활동을 통해 정보보호 정책 및 지침의 준 수 여부를 확인하고, 필요 시 대책을 수립하고 시행한다.
임직원은 바이러스 및 악성 코드의 유입으로 인한 피해를 예방한다.
모든 임직원은 정보보호의 중요성을 인식하고 정보보호 능력을 배양할 수 있도록 각 자의 직무와 부합하는 정보보호 교육을 받는다

제12조【정보보호 정책의 준수】
임직원이 본 정책 또는 하위 보안규정을 위반하여 회사에 재산상의 손실을 입히거나 이미지를 훼손한 경우에는 관련 사규에 따라 징계할 수 있다.
외부인에 의한 정보 자산 침해 사고는 관계기관과 협조하여 원인을 규명하고, 관련 법에 따라 조치한다.

제13조【정보보호 정책의 운영】
해외법인을 포함한 회사의 모든 임직원 및 제3자, 협력업체 직원은 본 정책을 숙지 및 준수하여야 하며 담당 업무에 적용하여야 한다.
본 정책의 제반 의무 이행에 관한 기록은 유지/보관하여야 한다.
본 정책의 하위 문서인 정보보호 규정은 문서에 정의된 업무 영역에 따라 적용된다.
각 사업장은 본 표준 정책에 기반하여 자체 사업장 실정에 부합되는 관리 세칙을 제정하여 시행한다.

제14조【정보보호 규정 및 프로세스】
본 정보보호 정책의 적용을 위한 상세 내용은 다음 각 호의 정보보호 규정에 별도로 규정한다.
정보보호 관리규정
사용자 보안규정
모바일 보안 규정
인사 보안 규정
사업 연속성 관리 규정
전산 인프라 운영 보안 규정
정보보호시스템 관리규정
물리적 보안규정
개인정보보호관리규정
생산망(OT) 보안규정
방위산업기술 보호규정
산업기술보호지침
정보보호 업무 연속성 관리 지침
클라우드 보안지침
개인정보 안전성 확보 지침
데이터 보안지침
소프트웨어 개발 보안지침

정보보호 정책 및 지침의 사용자 레벨에서 실행 수준을 제고하기 위해 정보보호 프 로세스 및 방법 양식을 별도 문서로 규정한다.
정보보호 프로세스

정보보호 규정 양식

제4장 정보보호 규정
제15조【정보보호 관리규정】
본 규정은 회사의 안전하고 지속적인 업무 운영을 위한 정보보호· 관리체계 수립, 운영, 평가, 개선의 정보보호 업무 규정을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
정보보호 조직구성 및 운영
정보보호 정책 및 규정의 관리
위험관리
보안사고 관리
정보보호 교육
보안 감사

제16조【사용자 보안규정】
본 규정은 회사의 정보자산을 대상으로 인력에 의해 발생될 수 있는 정보 유출, 변조, 오남용, 삭제 등 각종 사고를 최소화하기 위해 사용자가 준수해야 할 정보보호 활동 규정을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
책임 및 권한
사용자 보안 준수사항
외주 인력 보안관리

제17조【모바일 보안규정】
본 규정은 회사의 정보자산을 대상으로 모바일 기기를 통해 발생될 수 있는 정보 유 출, 변조, 오남용, 삭제 등 각종 사고를 최소화하기 위해 사용자가 준수해야 할 정보 보호 활동 규정을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
모바일 업무 보안성 검토절차
모바일 업무 처리기준
모바일 업무 타당성
모바일 기기 활용
모바일 인프라 보호
모바일 앱 보호
회사 지급 모바일 기기 보호

모바일 앱 개발 및 운영 가이드라인
사용자 모바일 보안관리

제18조【인사보안규정】
본 규정은 회사에 근무하는 인력의 채용, 퇴직 및 기타 인사이동에 따른 보안통제, 보 안 위반자의 처리 방안 결정을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
인사 보안 실행
정보보호 정책 위반자의 처리

제19조【사업 연속성 관리 규정】
본 규정은 유사시 회사의 보전과 비상대비 업무의 수행에 필요한 업무처리기준 및 절차를 정한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
비상대응 계획수립
비상대응 모의훈련
비상대응계획 유지관리
비상연락망 관리

제20조【전산 인프라 운영 보안 규정】
본 규정은 회사의 안전하고 지속적인 서비스 제공을 위하여 전산 인프라 운영과정에 서의 정보보호 활동 기준과 원칙 규정을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.

총칙
책임 및 권한
전산 인프라 운영 보안관리
서버 보안관리
네트워크 보안관리
적용 업무 시스템 보안관리
데이터베이스 보안관리
전산 기계실 보안관리

제21조【정보보호시스템 관리규정】
본 규정은 회사의 안전하고 지속적인 서비스 제공을 위하여 정보보호시스템 운영과 정에서의 정보보호 활동 규정을 규정을 목적으로 한다.

본 규정은 다음 각 호의 내용으로 구성된다.
총칙
책임 및 권한
정보보호시스템의 운영관리

제22조【물리적 보안규정】
본 규정은 회사에 대한 출입 권한 획득, 수정, 폐기, 정보 자산 반출이 등 물리적 보 안에 관련한 책임과 역할을 정의하며 비인가 자의 부적절한 행위로부터 당사 근무 인원 및 시설을 안전하게 보호함을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
출입통제
자산 반출입 통제
CCTV운영관리
보안원 운영

제23조【개인정보보호 관리규정】
본 규정은 회사에 모든 개인정보관련 규칙을 세부적으로 정하여, 회사에서 처리하는 개인정보를 체계적이고 안전하게 관리하며, 개인정보의 수집, 유출, 오용, 남용으로부 터 사생활의 비밀 등을 보호함으로써 회사와 임직원 및 고객의 권리와 이익을 증진 하고, 나아가 개인의 존엄과 가치를 구현하기 위함을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
총칙
개인정보보호 조직
개인정보의 관리 및 감독
개인정보보호 준수
개인정보의 처리 제한
개인정보 침해 및 처리
벌칙

제24조【생산망(OT) 보안규정】
본 규정은 회사에 안전하고 지속적인 업무 운영을 위하여 상품 제조를 위한 생산공장 내의 제 조설비, 제조시스템, 네트워크 등으로 구성된 생산망(OT)을 사이버 보안 위협으로부터 보호하기 위해 관리적·기술적 보호조치를 규정하여 안정적인 생산공장 운영을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.
개요
네트워크 보호조치

단위 설비/시스템 보호조치

제25조【방산기술보호규정】
본 규정은 방위산업기술보호지침에 따라 ㈜진흥주물의 방위산업기술(이하 "방산기술" 이라 한다)의 보호에 필요한 사항을 규정함을 목적으로 한다.
본 규정은 다음 각 호의 내용으로 구성된다.

총칙
기술의 식별 및 관리
인원통제 및 시설보호
정보 보호
연구개발 시 방위산업기술 보호
수출 및 국내 이전시 보호

제26조【산업기술보호지침】
이 지침은 『산업기술의 유출방지 및 보호에 관한 법률』(이하 "법" 이라 한다) 제8조(보호지침 의 제정 등) 및 『산업기술의 유출방지 및 보호에 관한 법률 시행령』(이하 "영" 이라 한다) 제10 조(보호지침의 제정)에 따라 국가핵심기술 등 산업기술의 유출을 방지하고 보호하기 위해 필요 한 사항을 규정함을 목적으로 한다.
총칙
기술의 판정 및 등록관리
국가핵심기술의 보호조치
국가핵심기술의 수출
국가핵심기술 보유기관의 해외 인수, 합병, 합작투자 등 외국인 투자
침해신고 및 대응복구
실태조사
보칙

제27조【정보보호 업무 연속성 관리지침】
이 지침은 ㈜진흥주물 (이하 "당사"이라 한다)의 정보시스템을 관리하고 운영하는 데 있어 정 보시스템 장애, 재해 등의 비상사태 발생 시 신속한 대응을 통해 피해를 최소화하고 빠른 시 간 내에 정상 업무를 재개하기 위한 사항을 규정함을 목적으로 한다.

총칙
역할 및 책임
정보보호업무 연속성 계획의 수립
데이터 백업 및 소산 대책
장애 대책

비상대책
재해복구 계획

제28조【클라우드 보안지침】
이 지침은 클라우드의 보안 원칙을 수립함으로써 회사의 영업비밀을 안전하게 보호하고, 정보유출을 예방하는 것을 목적으로 한다.
개요
클라우드 보안성 검토
프라이빗 클라우드 보안
퍼블릭 클라우드 보안

제29조【개인정보 안전성 확보지침】
이 지침은 개인정보 보호법에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보 가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.
목적
정의
안전조치 기준 적용
내부 관리 계획의 수립 시행
접근 권한의 관리
접근통제
개인정보의 암호화
접속 기록의 보관 및 점검
악성프로그램 등 방지
관리용 단말기의 안전조치
물리적 안전조치
재해 재난 대비 안전조치
개인정보의 파기

제30조【데이터 보안지침】
이 지침은 ㈜진흥주물(이하 '회사' 또는 '당사'라 한다.)의 안전하고 지속적인 업무 운영을 위해 정보시스템에서 데이터 생성, 보관, 활용, 폐기에 있어 경영정보 및 기술정보를 안전하게 보호 하고, 국내외 관련 법규사항을 준수하기 위함이다.
데이터 보안
데이터 정의
데이터 라이프사이클 관리

제31조【소프트웨어 개발 보안지침】
이 지침은 ㈜진흥주물(이하 '회사' 또는 '당사'라 한다.)의 안전하고 지속적인 업무 운영을 위해 시스템 구축 시 사이버 보안 위협으로부터 안전한 소프트웨어를 개발하기 위해 기획단계부터 개발완료시까지 전 과정의 보안성 검토 절차(프로세스)를 통해 정보 자산의 기밀성, 무결성, 가 용성 확보를 목적으로 한다.

총칙
소프트웨어 개발 방법론 준수
소프트웨어 개발 보안절차
시큐어 코딩 보안 가이드