	사 규	등록번호: 개정차수: 1차 페 이 지: 3

보완관리규정

	구 분	구 성	검 토	승 인	1차 배포처
결재	직 책	대리	실장	대표이사	
	성 명	유용철	방선호	김광식	
	서 명				
	서명일				
작성부서		정보기획팀	등 록 처	경영기획팀	
협조부서					

	차수	제(개)정일	시행일	주요 개정내용		2차 배포처
개정이력	1차	2017. 7. 1	2017. 7. 1			

보안관리규정

제 1 장 총 칙

제 1 조【목적】

이 규정은 ㈜현대포리텍 (이하 '회사'라 함)의 보안업무를 위한 기반 조직을 구성하고 비인가자의 부적절한 행위로부터 회사의 근무인원 및 시설을 안전하게 보호하며, 전산시스템에 의하여 처리, 저장, 소통되는 자료를 해킹 등의 위협으로부터 보호하고 취약요인을 제거하여 회사의 완전한 보안수준을 달성함을 그 목적으로 한다.

제 2 조【적용범위】

본 규정은 회사의 모든 조직과 임직원, 출입자, 전산장비 및 관련시설을 포함한 모든 부서에 적용한다.

제 3 조【용어의 정의】

1. 관리적 보안: 보안 조직 구성 및 운영, 보안정책 및 절차관리, 보안교육, 보안점검, 보안사고조사 등의 보안활동을 말한다.
2. 물리적 보안: 비인가자로부터 회사의 시설 및 인원을 보호하기 위한 출입통제, 정보자산의 반출입 통제 등의 보안활동을 말한다.
3. 기술적 보안: 정보시스템의 보호 및 정보시스템을 통한 유출을 예방하기 위한 운영관리, 정보시스템 접근통제, 개발 및 유지보수, 침해사고관리 등의 보안활동을 말한다.

제 2 장 본 칙

제 1 절 관리적 보안

제 4 조【조직구성】

회사의 보안업무를 수행하기 위하여 다음과 같이 보안조직을 구성한다.

1. 대표이사
2. CSO (Chief Security Officer)
3. 전사 보안책임자
4. 본부 보안책임자
5. 부문 보안책임자
6. 팀 보안책임자
7. 팀 보안담당자

제 5 조【업무분장】

보안조직 구성에 따른 업무분장을 규정함으로써 보안업무와 관련된 책임한계를 명확하게 한다.

1. 대표이사
   1) 기업비밀의 총책임, 대내외적인 비밀보호 문제에 있어서 기업을 대표
   2) 회사 보안업무의 최종 승인권자

2. CSO (Chief Security Officer)
   1) 회사 보안업무의 총괄적인 조정, 통제
   2) 전사 보안책임자를 지정하여 운영
3. 전사 보안책임자
   1) 보안 규정 및 관련 업무지침 작성
   2) 보안교육, 보안점검 등 회사의 보안업무계획을 수립 및 시행
   3) 분야별 보안담당자 (관리, 물리, 기술)를 지정하여 전문성 있는 업무수행 여건 보장
   4) 보안사고의 조사 보고 및 대응조치
4. 본부 보안책임자
   1) 본부의 보안책임자는 본부장임
   2) 본부의 보안업무 전반에 대한 감독 및 책임
5. 부문 보안책임자
   1) 해당 부문의 장으로 선임
   2) 해당 부문의 보안업무 전반에 대한 감독 및 책임
6. 팀 보안책임자
   1) 팀 보안책임자는 팀장임
   2) 팀의 보안업무를 총괄하며 팀 보안담당자를 지정하여 운영
7. 팀 보안담당자
   1) 비밀의 생산, 보관, 관리 등의 책임
   2) 소속 직원에 대한 비밀유지 교육 및 직원 관리
   3) 비밀의 수 발신 통제, 비밀 안전관리 및 보호조치
   4) 팀내 퇴직자의 관리
   5) 자체 보안 점검

제 6 조【보안규정 수립】

보안 규정은 문서로 작성하여 관리하며 대표이사가 승인한 자료에 한해서 유효성을 인정하며, 다음과 같은 개정 사유 발생 시에 개정하고 개정 시 개정이력을 기록, 유지한다.

1. 보안업무와 관련된 법령 즉, 산업기술의 유출방지 및 보호에 관한 법률, 부정경쟁방지 및 영업비밀의 보호에 관한 법률 등 변경 시
2. 회사 또는 고객사의 보안업무와 관련된 정책 변경 시

제 7 조【정보자산 분류】

정보자산은 그 중요도에 따라서 다음과 같은 분류 기준에 의거하여 분류한다. 대외비 이상의 보안문서는 보안관리규정에 의거하여 관리한다.

구분	내용
극비	회사의 첨단기술정보 또는 중요한 경영전략에 관한 내용으로서 대외적으로 유출 및 공개되어서는 안되며 직접 담당자만 접근이 가능하도록 한다.
비밀	회사의 중요한 기술개발정보 및 전략정보로서 업무 관련자만 접근이 가능하도록 한다.
대외비	일정한 기간동안 대외적으로 공개되어서는 안 될 내용으로서 회사 임직원은 필요시에 소정의 절차에 의하여 접근이 가능하도록 한다.

제 2 절 물리적 보안

제 8 조【보안구역 설정 및 보호】

회사의 영업비밀 및 자산의 보호를 위하여 통제가 요구되는 장소를 보호구역으로 설정하며 설정된 보호구역에 대한 통제대책을 수립하여 시행한다.

제 9 조【출입 통제】

회사는 효율적인 출입통제를 위하여 임직원 또는 외부인에게 출입증 패용 등 육안 식별이 가능한 통제수단을 적용하여 출입통제 업무를 수행한다. 외부인은 회사에 업무적으로 출입이 필요한 경우에만 방문을 요청할 수 있으며 외부인의 방문은 유관부서의 담당자를 통하여 신청하고 승인권자의 승인 후 출입을 허용한다.

제 10 조【반출입 통제】

회사 출입문을 경유하여 반출입되는 모든 물품은 반출입통제 절차에 의거하여 점검 및 확인을 한다. 출입문 근무자는 반출입과 관련되는 모든 이력을 기록, 유지하며 주기적으로 이를 분석한다.

제 11 조【경비인력 운영】

회사의 자산보호와 안전유지를 위하여 경비인력을 운영한다. 경비인력 편성은 용역업체와 기본계약서에 의거하여 편성하되 근무여건을 보장하기 위하여 최소한 2 교대 근무가 가능하도록 편성한다.

제 12 조【CCTV 운영】

외부인의 침입으로부터 회사의 자산을 보호하기 위하여 CCTV 를 설치, 운영한다. CCTV 로 수집할 영상의 범위, 목적, 기간, 운영주체 등이 CCTV 설치계획단계에서 정의되어야 한다. 수집된 영상물은 판독이 가능한 상태를 유지하도록 관리한다.

제 3 절 기술적 보안

제 13 조【시스템 운영기준】

시스템 운영기준을 적용함에 있어서 <모두 차단 후 필요 시 허용>을 기본정책으로 설정한다. ACL (Access Control List, 접근통제목록)은 보안의 영향도를 고려하여 최소의 필수 인원에게만 허용하는 정책을 유지한다. 기술 보안담당자만이 시스템에 접근할 수 있어야 하며 유지보수 등 접근권한에 변동 발생 시 전사 보안책임자에게 보고 후 변경한다.

제 14 조【사용자 보안】

PC 에 대한 보안책임은 각자에게 있다. 표준 OS (Operating System, 운영체제)를 명확하게 정의하고 OS 별로 비밀번호 설정방법 등 개인조치사항을 공지한다. 회사에서 지정한 정품 소프트웨어 외에 임의로 소프트웨어 설치를 금지한다.

제 15 조【네트워크 보안】

네트워크 보안을 위하여 침입차단시스템 (방화벽, Firewall)을 설치하여야 하며 침입차단시스템이 차단에 실패한 경우 피해를 최소화하기 위하여 침입탐지시스템을 운영한다. 네트워크 장비에 대한 접근권한을 주기적으로 점검한다. 설치되는 장비의 시간을 동기화하여 무결성을 보장한다.

제 16 조【서버 보안】

1. 서버시스템은 서버, 저장장치 등의 하드웨어와 응용시스템, 데이터베이스 등의 소프트웨어를 총칭하며, 영업비밀은 암호화 (Encoding)하여 서버에 저장하고 열람

시는 복호화 (Decoding)한다.

2. 서버시스템은 물리적 보안대책이 강조되어있는 통제구역에 설치한다. 서버시스템의 처리속도 및 용량을 주기적으로 점검한다. 시스템 장애 시 신속한 업무 복구를 위하여 OS 및 데이터베이스에 대한 백업을 주기적으로 수행한다. 영업비밀에 대한 열람 및 반출 로그를 기록, 유지한다.

부 칙

제 1 조【시행일】

이 규정은 2017년 7월 1일부터 시행한다.

제 2 조【경과규정】

이 규정이 시행되기 이전에 회사에서 시행한 것은 이 규정에 의한 것으로 본다.
