

문서관리번호	2026-S-11
최초제정일	2018. 4. 2
최종개정일	2026. 2. 1
문서관리부서	전산부

유성기업 표준보안관리

2026.02.01



■ 총칙

○ 목적

본 지침은 유성기업 주식회사(이하 "당사"라 한다)의 정보보호 활동을 위한 기반 조직을 구성하고, 비 인가자의 부적절한 행위로부터 당사 근무인원 및 시설을 안전하게 보호하고 정보시스템에 의하여 처리, 저장, 소통되는 자료를 바이러스, 해킹 등의 위협으로부터 보호하고 취약요인을 제거하여 당사의 정보가 안전하게 보호되어 당사가 경쟁력을 확보하고 지속성장 발전되도록 하는데 그 목적이 있다.

○ 적용범위

지침은 당사의 모든 조직과 임직원, 출입자, 전산장비 및 관련시설 또한 협력사보안 위반 제제규정을 포함한 모든 정보자산에 대한 정보보호활동 업무에 적용된다.

■ 준수 의무

1. 책임과 권한

1.1 임직원

- 1.1.1 본 지침의 보안정책을 준수해야 한다.
- 1.1.2 보안교육에 참석할 의무가 있고, 자체 점검 등 회사 보안활동에 적극 협조해야 한다.
- 1.1.3 회사의 정보자산 반출 시 정해진 절차에 따라야 하며, 임의 판단으로 반출할 수 없다.
- 1.1.4 출입증은 항상 패용해야 하며 출입증을 타인에 대여, 공유하지 않는다.
- 1.1.5 보안사고를 발견하였을 경우 팀(부문)별 보안책임자 또는 보안담당조직에 즉각 해당 사실을 알려야 한다.
- 1.1.6 회사의 보안규정을 위반하는 경우 다음과 같은 인원에 책임이 있다.
 - 1) 임직원이 보안규정 위반: 위반자 및 소속 팀(부문)장
 - 2) 방문자가 보안규정 위반: 출입허가를 요청한 임직원
- 1.1.7 정품소프트웨어 사용을 원칙으로 하며, 불법소프트웨어 사용상 문제발생 시 본인의 책임에 있다.

1.2 방문자

1.2.1 출입증을 소속회사의 직원이나, 타인에 대여, 공유하는 행위를 해서는 안 된다.

1.2.2 카메라 또는 카메라폰과 같은 영상 기록장치를 이용한 임의 촬영을 금지한다.

1.2.3 당사에서 제공된 자료 외 어떤 자료도 취득, 사용해서는 안 된다.

1.2.4 기타 당사에서 요구하는 보호조치를 준수해야 하며 위반 시 아래와 같은 책임을 진다.

1) 출입증을 대여하거나 본 목적과 다르게 사용하는 등 오.남용 적발 시 해당자의 출입증을 회수하고 출입금지 조치하며, 해당 회사에는 재발방지 대책을 요구한다.

2) 보호구역내에서는 당사의 통제를 따라야 하며 이를 위반 시 강제 퇴실 또는 퇴장된다.

3) 당사 자료를 무단으로 활용하거나 유출을 시도하는 경우에 민형사상 책임을 진다

1.3 보조기억매체

1.3.1 보조기억매체사용

1) 각 부서는 보조기억매체를 등록한 후 사용하여야 한다.

2) 보조기억매체의 등록방법은 승인할 매체의 S/N번호를 확인하여 전산 부문에 메일로 승인요청 하는 것을 말한다.

3) 보조기억매체 사용제한

(1) 각 부서는 등록된 보조기억매체만 사용할 수 있으며 업무목적 이외 사적인 용도로 사용할 수 없다.



(2) 각 부서팀(부문)장은 팀원들에게 공지,교육을 통하여 보조기억매체의 임의 사용을 제한하여야 하고 주기적으로 확인 해야한다.

4) 각 팀(부문)장의 역할

(1) 각팀(부문)장은 소속직원이 미등록 보조기억매체를 사용하거나 업무적인 목적 이외 사적인 용도로 사용하지 않도록 감독하여야 하며, 이를 위반한 사실을 발견 또는 확인하는 즉시 전산부문장에 통지하여야 한다.

5) 전산부문장의 책무

(1) 전산부문장은 각 부서에서 사용하는 보조기억매체 등록 현황(목록)을 DLP시스템에서 수시확인 관리한다.

(2) 전산부문장은 보조기억매체를 일괄 구입하여 필요한 부서에 보급할 수도 있다.

(3) 전산부문장은 비밀 유출이 우려되거나 유출 징후가 있는 경우에는 지체 없이 대표이사에게 보안사고 조사를 승인받아야 한다.

1.4 자료접근권한 및 패스워드 관리

1.4.1 해당부문

1) 중요 전산업무 사항의 자료접근권한 부여 요청.

1.4.2 전산부문장

1) 자료접근 권한에 대한 검토/설정 관리

2) (1회/3개월) 서버장비 및 네트워크장비의 패스워드 관리

1.5 협력사 보안위반 제재 및 관리

1.5.1 협력사의 임직원은 회사로 부터 취득한 모든 자료를 임의사용, 유출하지 않고 보호할 의무를 가진다

1.5.2 협력사는 회사의 보안규정, 사규규정, 거래계약서의 내용을 충실히 이행



하여 신뢰성 있는 협력관계를 유지할 수 있도록 노력해야 한다.

1.5.3 협력사는 회사에서 받은 각종 영업비밀 관련 자료(도면, 각종 정보파일 등) 및 정보를 웹사이트 등에 공개 및 업로드 하여서는 아니된다

1.5.4 협력사는 회사에 바이러스 유포 및 해킹 등의 위협을 가해 재산상의 손실을 입혀서는 아니된다

1.5.5 협력사 직원의 과실은 곧 협력사의 과실이며 이로 인해 발생하는 회사의 손해에 대해서는 전적으로 협력사에서 책임이 있다.

2. 관리적 보안

2.1 보안조직구성 및 관리주체

2.1.1. 보안업무와 관련된 전사보안조직의 구성 및 관리는 전산부문에서 주관한다.

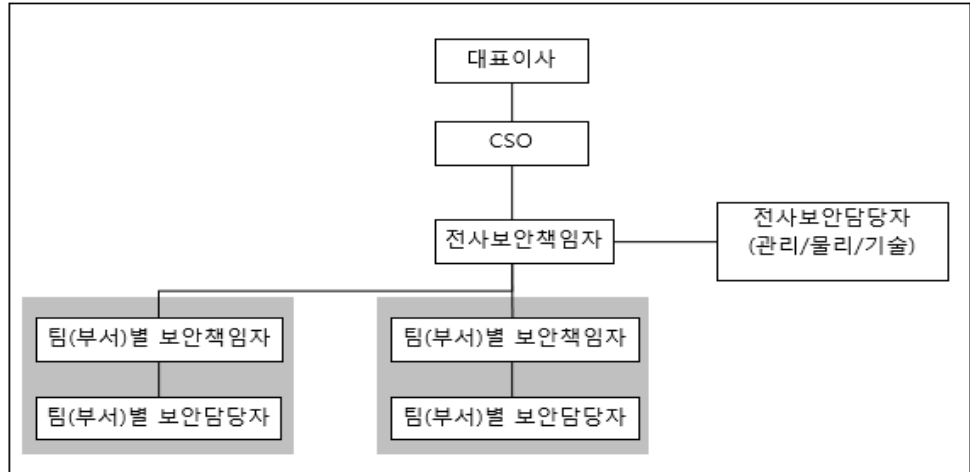
2.1.2 보안조직 구성 및 운영에 관한 절차를 마련하고 CSO의 승인을 득한 후 등록 관리한다.

2.2 보안협의체 운영

2.2.1 보안에 대한 주요 사항의 결정 및 사내 하부조직까지의 원활한 정책 전달 및 이행을 위해 CSO, 보안책임자, 보안담당자를 구성원으로 하는 협의체를 구성하고 정기적으로 운영해야 한다.

2.3 보안조직도

2.3.1 담당자의 팀, 성명, 연락처를 포함한 조직도를 아래와 같이 작성하여 규정 내에 포함한다.



2.4 보안조직 업무분장 (책임과 역할) (1. 업무분장 기준 참조)

2.4.1 CSO

- 1) 대표이사 또는 대표이사의 권한을 위임받은 임원으로 한다.
- 2) 보안총괄책임자로서 보안에 관련한 모든 정책을 결정한다.
- 3) 전사보안책임자 와 전사보안담당자를 선임한다.
- 4) 보안업무를 기획, 시행하도록 전사보안책임자에 지시하고 시행 상황을 관리감독 한다.

2.4.2 전사보안책임자

- 1) 전사보안책임자는 CSO가 선임한 자로 한다.
- 2) 보안업무를 CSO에 보고, 승인 후 시행한다.
- 3) 회사의 보안규정을 수립하고 교육, 공지 등을 활용하여 적용한다.
- 4) 보안관련 법령 및 관련사의 보안정책 변경 등 외부환경 변화에 따른 회사의 보안정책을 재 검토하고 필요 시 보안규정에 반영하거나 보안교육, 점검, 감사 등의 조치를 시행한다.
- 5) 보안의식 제고를 위해 매월 특정일을 '보안의 날'로 지정하여 자체점검을 시행한다. (공장/팀 보안책임자, 담당자에게 자체점검 결과를 요구할 수 있다)

- 6) 보안교육 및 홍보를 실시한다.
- 7) 보안사고 발생 시 외부 수사기관과의 연계여부를 판단하고 대책 수립 및 징계를 시행한다.
- 8) 정보자산의 정기적인 점검을 통해 취약성 조사 및 대응방법을 마련하여 보안사고를 사전에 예방한다.
- 9) 회사 정보보호실태를 분기별로 CSO에게 보고한다.
- 10) 정보보호 활동 계획 및 예산에 대한 운영 및 승인을 시행한다.
- 11) 분기 1회 이상 정기적으로 팀 보안 책임/담당자 회의를 개최하여 보안 정책의 하부조직 전파에 노력한다.

2.4.3 전사보안담당자

- 1) 전사보안담당자는 물리보안담당자, 관리보안담당자, 기술보안담당자로 역할을 구분하고, 규정에서 정한 보안업무를 수행한다.
- 2) 물리보안담당자
 - (1) 각 팀(부문)에서 요청하는 보안구역설정을 검토, 승인하고, 그 결과를 요청부서에 회신하고 이를 현황으로 관리해야 한다.
 - (2) 물리보안시스템을 운영하며 관련된 절차를 수립, 그 절차에 따라 운영 현황을 관리하며 필요시 전사보안책임자담당자에 보고, 조치한다.
- 3) 관리보안담당자
 - (1) 교육계획을 수립 및 시행하고, 각종 보안 이벤트 시행, 모니터링, 정보 자산에 대한 정기적인 점검 등을 통한 보안사고 예방활동을 수행한다.
 - (2) 보안사고 발생 시 이에 대한 조사, 조치활동을 담당한다.
- 4) 기술보안담당자
 - (1) 정보기술 관련한 전 부문의 보안업무를 총괄하여 수립 및 시행한다.
 - (2) 정보기술 보안운영계획 및 보안감사계획을 수립하고 시행한다.
 - (3) 정보기술 보안에 관련한 별도의 세부 지침을 마련하여 시행한다.
 - (4) 정보기술 보안시스템의 관리 및 성과분석을 실시한다.
 - (5) 전산자산의 안정적 운영 및 보안대책을 마련하고 실시한다.
 - (6) 정보기술(IT) 업무를 수행하는 자로 전사보안책임자가 지명한 직원으로

한다.

- (7) '기술적보안'에 규정된 내용을 계획하고 시행한다.
- (8) 전산자산의 취약점이 발견되면 전산담당자에게 개선을 요청해야 하며, 패치를 실시한다.
- (9) 내.외부 전산장비에 대한 보안점검을 실시한다.
- (10) 보안규정 상의 보안업무 수행사항을 적용 및 실행한다.
- (11) 보안사고 발생 시 기술적인 조사, 조치 등을 지원한다.
- (12) 위 각 호에 대한 결과를 보안책임자에게 보고한다.

2.4.4 팀(부문)보안책임자

- 1) 각 팀의 팀(부문)장으로 해당 팀(부문)내 보안업무를 수행, 조정, 감독한다.
- 2) 팀(부문)내 각종 기업비밀의 보안성 검토 및 보안문서 여부를 결정한다.
- 3) 팀(부문)내 자체 보안점검이 정상적으로 이행되고 있는지 확인하고 감독한다.
- 4) 팀(부문)내 시건장치 등이 적절히 사용, 관리되고 있는지 확인하고 감독한다.
- 5) 팀(부문)원 보안교육 실시를 주관한다.
- 6) 팀(부문)보안담당자를 임명한다.
- 7) 팀(부문)내 보안사고 발생시 또는 발생할 우려가 있는 경우 전사보안책임자에게 통보한다.
- 8) 팀(부문)의 업무와 관련 있는 장소가 보안상 출입을 제한할 필요가 있는 경우 물리보안담당자에 보호구역 설정을 요청한다.
- 9) 회사의 보안정책이 효과적으로 이행될 수 있도록 적극 지원한다.
- 10) 팀(부문)별 보안담당자
 - (1) 팀(부문)별 보안책임자가 임명한 자로 해당 팀(부문)의 전반적인 보안의 무관리를 담당하며 보안관리부서와 긴밀한 협조체계를 구축하여 정보보호 활동에 있어서 부서간 이견 발생시 협의체 역할을 수행한다.
 - (2) 보안 담당자 회의는 회사의 보안방향 및 정책에 대한 사항의 실무협의, 보완대책 등을 강구하고 임직원에게 전파하는 업무를 수행한다.

2.4.5 보안서약서



1) 영업비밀의 법적인 보호와 임직원의 보안인식제고를 위해 '영업비밀 및 정보보호서약서'를 작성하여 제출토록 한다.

2) 임직원

(1) 임직원은 입사시 정보보안에 대한 중요성을 숙지하여 '영업비밀 및 정보보호서약서'를 작성 후 채용담당자에게 제출한다.

(2) '영업비밀 및 정보보호서약서'는 관련 법령 및 정보의 기밀사항 및 자산 관리에 관하여 지켜야 할 사항을 명시해야 한다.

(3) '영업비밀 및 정보보호서약서'의 법적 유효성을 보장받기 위해 3년 마다 1회 이상 징구해야 한다.

(4) 임직원은 퇴사시 본인이 보호해야 할 영업비밀의 내용과 보호기간, 부정경쟁방지 등에 관한 법령 준수 및 법적 책임 등이 포함된 '퇴직자영업비밀유지서약서'를 작성 제출해야 한다.

(5) 정보보호를 위해 '퇴직자영업비밀유지서약서'는 '영업비밀 및 정보보호서약서'로 통일한다.(퇴직시 기 징구한 서약서 내용을 한번더 숙지하게 하고 별도로 징구하지 않는다.)(퇴직시 서약서를 출력하여 퇴직서류에 첨부한다.)

(6) '영업비밀 및 정보보호서약서'는 ERP시스템에 있는 전자승인 시스템을 통해 승인해야한다.(효력은 서면과 동일함)

3) 제3자(일반용역, 외주인원)

(1) 일반용역을 포함한 외주인원은 계약시 '외주인원 및 업무수행자 정보보호서약서'를 작성하여 관리(주관)부서에 제출한다.

(2) 계약서는 회사에서 정한 표준계약서를 사용해야 하며, 표준계약서에는 회사의 보안규정을 준수할 것과 외주인원 및 외주인원의 소속사에 보안책임이 있음을 공지하는 내용이 포함되어야 한다.

(3) 기술용역 또는 기술자료 교환이 있는 계약의 경우 회사의 정보자산보호/관리를 위해 당사의 보안점검에 외주인원 소속사도 포함이 되어 있



음을 고지하는 문구를 포함한 계약서를 사용해야 한다.

4) 중요업무 수행자

- (1) 중요 프로젝트를 수행하는 임직원 및 외부인원은 프로젝트의 존재 사실 및 프로젝트를 수행하는 동안 알게 된 일체의 영업비밀에 대한 비밀유지를 서약하는 '외주인원 및 업무수행자 정보보호서약서'를 작성해야 한다.
- (2) '외주인원 및 업무수행자 정보보호서약서'는 프로젝트명, 수행기간, 본인의 업무 등이 명기되어야 한다.

2.4.6 보안교육

1) 전사보안책임자

- (1) 전 임직원에게 대해 연2회 이상 보안교육을 실시해야 하며 필요한 경우 대표이사의 입회를 요구할 수 있다.
- (2) 신입사원 입사 시 관리, 물리, 기술 각 영역에 대해 교육을 실시해야 한다.
- (3) 보안정책 변경 등 사유 발생 시 팀(부문)보안담당자에게 공지 및 소집 교육 등을 통해 교육을 실시해야 한다.

2) 팀(부문)보안책임자

- (1) 내/외부 보안사고 발생 등 보안상 필요하다고 판단하는 경우 팀원에 대한 보안교육을 실시할 수 있다.
- (2) 사내 규정 변경 등의 전달사항이 있는 경우 팀(부문)보안담당자가 팀 내 전달교육을 시행하도록 한다.
- (3) 팀내 해외 주재원 근무대상자가 발생하는 경우 명령 발령일 2주 이내에 팀(부문)보안책임자는 해외근무 시 필요한 보안조치에 대해 보안교육을 실시해야 한다.

2.4.7 퇴직자 관리

1) 인사담당부서

- (1) 퇴직자에 대해 '영업비밀 및 정보 보호 서약서'를 퇴직서류에 포함하여 징구해야한다.
- (2) 인사담당부서는 퇴직 후 동종업계로 전직한 사실을 인지 한경우 당사에서 취득한 영업비밀이 제공되었는지를 확인하고 위반사항을 확인하는 경우 법적 조치를 취한다.

2) 팀(부문)보안책임자

- (1) 팀 내 퇴직이 예정되거나, 퇴직명령이 발령된 직원에 대해 재직기간 동안 습득한 모든 영업비밀은 경우를 막론하고 대외로 유출하여서는 안되며 "이를 위반할 시 '영업비밀 및 정보보호서약서'에 의거하여 민형사상의 책임을 질 수 있다"는 내용을 공지해야 한다.
- (2) 퇴직(예정)자가 해당업무 수행기간 동안 습득한 모든 영업비밀을 소속팀(부문)에 인계, 개인이 소지하고 있는 영업비밀은 재사용 불가한 상태로 파기하도록 요청하고, 이를 확인해야 한다.

3) 임직원

- (1) 임직원은 퇴직자가 동종업종 또는 경쟁사에 재취업하는 것을 인지하였을 경우 즉각 보안담당부서에 통보해야 한다.

4) 기술보안담당자

- (1) 퇴직 명령이 발령된 후 퇴직자에 대한 출입 및 시스템상의 모든 접근 권한은 절차에 따라 모두 삭제되어야 한다.
- (2) 업무인수 인계에 따른 권한삭제 유예는 팀(부문)보안책임자의 승인에 따라 처리하며 최대 2주를 초과할 수 없다

2.4.8 보안 위반자 관리

1) 전사보안책임자

- (1) 위반사항의 경중을 1차 판단하고, 경미한 위반의 경우 CSO명의로의 주의조치를 해당 직원 및 소속 팀(부문)장에 통보하며, 중요한 위반



이라고 판단되는 경우 CSO보고를 통해 조치여부를 결정한다.

- (2) 보안 위반에 대한 징계는 취업규칙과 인사규정에 정한 징계 종류 및 절차에 따른다.
- (3) 유사사고 재발방지를 위한 대책을 수립, 시행하고, 임직원의 정보보호 의식을 고취시키기 위해 징계 결과는 익명을 사용하여 임직원 전원에게 공지할 수도 있다.

2) 임직원

- (1) '표준보안관리' 및 관련 지침/절차를 위반한 사실을 인지하는 경우 전사보안책임자 또는 전사보안담당자에 즉시 위반사실을 통보해야 한다.
- (2) 본인의 실수 또는 의도하지 않게 정보가 노출, 제공되었음을 확인하는 경우 전사보안담당자 또는 전사보안책임자에 관련사실을 통보해야 한다.

3) 위반자 경중 판단 기준

(1) 경미한 위반

- a. 위반 내용이 실수 또는 과실에 의한 단순한 규칙/지침 위반이라고 인정되는 경우
- b. 위반이력이 없는 임직원이 규정, 절차 등의 미 인지로 규칙/지침을 위반한 경우
- c. 본인의 위반사실을 통보해온 경우 중 중대한 위반에 사유가 되지 않는 경우

(2) 중대한 위반

- a. 고의로 보안 규정, 절차, 지침을 우회하는 행위를 한 경우
- b. 부정한 정보취득이나, 보안사고에 관련된 사안으로 인정되는 경우
- c. 중대한 과실이거나, 동일한 위반을 반복적으로 지적 받는 경우

d. 본인의 과실/위반으로 회사에 손실을 주는 사유가 인정되는경우

2.4.9 정보자산 분류

1) 분류주체 및 주기

- (1) 팀(부문)보안책임자는 각 팀 단위로 분류 기준을 마련하고, 이를 바탕으로 정보의 생성자 (문서작성자)가 최초분류를 시행하도록 공지, 점검한다.
- (2) 임직원은 문서를 생성할 때 분류기준에 따라 등급을 구분하여 회사 보안정책이 준수되도록 분류기준을 인지하고, 항상 분류된 상태로 문서를 관리한다.
- (3) 팀(부문)보안담당자는 팀 내 업무 변동사항 발생 시 2주 이내, 특별한 변동 사항이 없는 경우에도 6개월에 1회 정기적으로 검토/조정을 시행한다.
- (4) 등급이 분류된 정보자산은 인식할 수 있는 관리자, 자산번호, 보관위치 등을 확인할 수 있는 인덱스를 부착하여 관리한다.

2) 정보자산의 구분

- (1) 일반자료는 대외적으로 노출, 공개되는 경우도 특별히 문제가 되지 않을 내용으로 공시자료 등 대외공개를 목적으로 만들어 졌거나. 인터넷 검색 등을 통해 쉽게 취득할 수 있는 자료로 재 분류될 때 까지는 관리 대상에서 제외한다.
- (2) 대외비는 모든 임직원이 사용할 수 있으나, 외부인의 사용은 제한되는 자료로, 누설될 경우 회사에 일시적 손해를 끼치거나 해로운 결과를 초래할 우려가 있는 내용을 말한다.
- (3) 비밀은 누설될 경우 회사에 상당한 손실을 초래하거나 회사 사업계획의 폐기 및 수정을 초래할 우려가 있는 내용을 말한다.
- (4) 극비는 누설될 경우 회사의 경영상 막대한 손실을 초래하거나 회사보존을 위태롭게 할 우려가 있는 내용을 말한다.



3) 정보자산의 관리

- (1) 전사보안책임자는 팀(부문) 단위에서 작성할 수 있는 정보자산분류기준을 제공해야 한다.
- (2) 각팀(부문)장은 1년에 1회 이상 파악된 정보자산의 리스트를 확인하여 작성되어야 한다.

2.4.10 영업비밀관리기준

1) 영업비밀의 정의

- (1) '영업비밀'이란 비밀로 유지된 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말하며, 회사가 사용을 위하여 타사와의 계약관계 등을 통하여 도입한 타사의 영업비밀을 포함한다.

2) 영업비밀의 보관 및 관리

- (1) 영업비밀은 생성시부터 관리를 해야 하며 중간과정의 산출물도 생성 확정된 자료와 동일하게 관리되어야 한다.
- (2) 출력된 영업비밀은 문서등급, 출력자명, 작성 일시를 표기하고, 임의 접근이 가능하지 않은 장소에 보관하고 팀(부문) 보안책임자가 지정하는 자가 관리한다.
- (3) 임직원은 자리 이석 시 영업비밀이 책상 위 또는 노출된 장소에 방치되지 않도록 관리해야 한다.

3) 영업비밀의 이관

- (1) 보직 변동으로 해당 영업비밀을 소유할 필요가 없는 경우 전보자는 '업무인수인계서'에 취급 영업비밀의 인수인계 내용을 작성하고, 전자 문서 및 출력문서 등 모든 종류의 영업비밀을 인수자에 인계한다.
- (2) 팀(부문)별 보안책임자는 인계/인수 절차에 따라 영업비밀이 적절히 이관되었는지 확인하고 인계자 소유하고 있는 영업비밀이 모두 파기되었는지 확인한다.

4) 영업비밀의 배포 및 반출



- (1) 영업비밀을 언론기관, 국가기관, 협의회 및 본인의 업무와 직접적으로 관련이 없는 곳으로 반출하거나 외부의 요청으로 영업비밀을 제공해야 하는 경우 전사보안책임자의 사전 승인을 얻어 반출한다.
- (2) 1항에 해당되지 않는 업무상 사외 반출의 경우 팀(부문)보안책임자의 승인을 얻고 회사가 정한 방법으로 반출한다.
- (3) 사전 승인을 얻지 못한 경우 반출 24시간 이내 서면으로 팀(부문)보안책임자에 사후 승인을 받아야 한다.
- (4) 사내 배포의 경우 영업비밀의 소유권자(작성자)의 판단에 따라 회사가 정하는 보호조치가 적용된 상태로 필요한 인원에게 한정하여 배포한다.
- (5) 본인이 작성한 영업비밀이 아닌 경우 배포, 반출할 수 없으며, 작성자의 승인을 얻거나 작성자에 반출, 재 배포를 요청한다.

5) 영업비밀의 파기

- (1) 전자문서 형태의 영업비밀은 회사가 정하는 소프트웨어를 활용하여 복원 불가능한 상태로 파기한다.
- (2) 인쇄된 영업비밀은 문서 세단기를 사용하여 원형을 확인할 수 없는 상태로 파기해야 한다.

2.4.11 준거성

- 1) 전사보안책임자는 보안관련법령이 개정되거나, 고객사의 보안정책이 변경되는 경우 내부규정, 절차, 지침에 영향이 있는지 전사보안 담당자를 통해 검토해야 하고 필요 시 개정해야 한다.
- 2) 전사보안책임자는 법령개정 및 고객사 정책변경 등 변경사항을 내부규정 변경사항과 함께 전 임직원이 인지할 수 있도록 공문 또는 게시판을 통하여 공지해야 하며, 필요 시 별도 교육을 실시해야 한다.
- 3) 기술보안담당자는 시스템의 취약점을 주기적으로 점검하여, 내부 규정 또는 외부 법령에 위반사항이 없도록 확인하고 개선이 필요한 경우 전사보안 책임자, CSO에 보고하고 조치한다.



2.4.12 보안점검/감사

1) 목적

- (1) 회사에서 정한 보안통제가 적절히 이행되고 있는지 확인함으로써, 잠재적인 정보보안 침해의 가능성과 그로 인한 피해를 최소화하는데 그 목적이 있다.

2) 시행 주체 및 주기

- (1) 전사보안책임자의 주관하에 사전 계획에 따라 시행하며 점검/감사를 시행할 인원은 전사보안책임자가 지명하고 CSO의 승인을 받은 임직원으로 한다.
- (2) 매월(마지막주 금요일) 또는 분기별 각 보안책임자, 보안담당자의 조직별 보안점검을 계획 시행해야 한다. (보안의 날을 지정하여 보안점검 실행 계획을 전산부문에서 통보할 수 있다)
- (3) 다음의 경우 상기 일정과 별도로 점검/감사를 실시할 수 있다.
 - a. CSO가 필요하다고 인정할 때
 - b. 보안사고의 발생 우려가 있을 때 또는 보안사고 발생시

3) 점검/감사 대상

- (1) 모든 인원 및 정보자산을 대상으로 한다.

4) 점검/감사 시행

- (1) 피감사 팀(부문) 및 피감사인은 점검 및 감사요청에 협조해야 한다.
- (2) 조치결과가 부진한 경우 지속적으로 시정을 요청할 수 있으며, 감사결과가 중대한 보안규정의 위반사항으로 발견시 인사부서의 협조를 구해 징계조치를 이행한다.
- (3) 보안보고서는 감사로 드러난 위험에 대한 대책방안 및 권고사항을 포함해야 하며 CSO에게 보고후 기록으로 관리 유지한다.

3. 물리적 보안

3.1.1 보호구역 설정

1) 보호구역의 구분

보호구역은 그 중요도에 따라 다음과 같이 제한지역, 통제구역으로 구분한다.

2) 제한지역

회사의 영업비밀 및 자산의 보호를 위하여 외부인의 출입을 제한하는 지역으로 회사의 모든 사무, 생산공장이 이에 해당하며 임직원 외 외부인은 절차에 따라 승인 후 출입하도록 한다.

3) 통제구역

영업비밀보호를 위해 임직원의 출입을 통제할 필요가 있는 지역으로, 사진촬영 및 비인가 임직원의 출입을 제한한다.

3.1.2 보호구역 설정 및 표기

1) 통제구역은 팀(부서)보안책임자의 의견을 수렴하여 물리보안담당자가 설정하고 전사 보안책임자 및 CSO에 보고 후 시행한다.

2) 표기는 출입 시 쉽게 확인이 가능한 출입문 중앙상단 등에 부착한다.

3) 가로2, 세로1의 비율을 유지하여 가로 18cm, 세로 13cm 이상의 크기로 표기한다.

구분	제한지역	통제구역
지역	사내 전 지역	000 연구동 , 회계팀금고실, 전산실 그외 보안관련 시설.
경고문1	-	 통제구역 No Entry
경고문2	-	촬영금지  경 고 이 구역내의 출입은 출입 인가자로서 업무상 관계있는 자에 한하며 무단촬영을 금함. 촬영을 요할시는 보안담당관의 승인을 득할 것.

3.1.3 보호구역의 출입관리

1) 출입인가

- (1) 임직원은 근무지역 및 제한지역의 출입이 가능하다.
- (2) 업무상 통제구역의 출입이 필요한 경우 소속팀(부서)장의 승인을 받아 물리보안담당자에 권한 요청을 부여받아 출입이 가능하다.
- (3) 물리적보안 주관부서에서는 출입권한 요청에 대한 승인여부를 요청팀(부서)에 회신하고 이를 관리하여야 한다.

2) 출입관리

- (1) 통제구역은 일반시설과 분리하여 설치하여야 한다.
- (2) 일반시설과 분리가 불가한 경우 보안 및 경계대책을 별도로 강구하여야 한다.
- (3) 통제구역은 외부인은 물론 임직원도 출입인가자 외는 출입을 금하며 소정의 서식에 의한 출입자명부를 비치하여 기록 유지하여야 한다.
- (4) 출입허가를 받은 외부인이 보호구역내에서 업무를 수행할 때에는 담당책임자의 통제를 따라야 하며 이를 위반 시 강제퇴실 또는 퇴장 조치한다.

(5) 통제구역 내에서는 일체의 면회(상담, 회의 등)을 금한다.

(6) 통제구역 내에서 활동은 전사보안담당자가 승인하고 임직원의 관리하에서 가능하다

3.1.4 출입 통제

1) 관리주체

(1) 물리보안담당자는 효율적인 출입통제를 위하여 사원증에 출입기능을 부가한 출입증을 발급 패용하며 출입통제 업무를 주관한다. (단, 아산공장, 영동공장 출입통제 주관은 노사상생팀장의 책임하에 관리 주관한다.)

2) 출입증의 구분

- (1) 임직원 출입증: 당사의 임직원에 한해 발급되는 출입증
- (2) 협력업체 출입증: 당사에 출입이 필요한 협력업체에 발급되는 출입증
- (3) 임시출입증: 당사 임직원이 출입허가를 요청한 자에 발급하는 출입증
- (4) 협력업체 또는 각종 용역 등 정기적으로 출입하는 외부인은 보안등록 절차에 의거 장기 출입증을 경비부담 조건으로 발급운용 할 수 있다.

3) 외부인 출입증의 발급

- (1) 출입신청 시 발급
- (2) 외부인이 당사에 업무적으로 출입이 필요한 경우만 방문을 요청할 수 있다.
- (3) 외부인의 방문 신청은 유관부서의 담당자가 방문 신청해야 하며, 물리보안담당자의 승인 후 출입이 가능하다
- (4) 방문한 외부인이 업무목적 이외의 행위를 하거나 회사에 유해한 행위를 하는 경우 방문 신청을 대행한 임직원도 책임이 있다.

4) 임시 방문 시 발급

- (1) 방문의 신청은 외부인의 제한지역 내 진입이전에 등록되어야 하며 사



전 통보 없이 방문한 경우 내부 업무관련자의 방문신청 전까지 대기하여야 한다.

- (2) 외부인은 경비실에 신분확보에 필요한 기재사항을 기록하고 신분증을 위탁 후 방문증을 수령하여 제한지역에 출입한다.

5) 장기출입 신청 시 발급

- (1) 월 15회 이상 당사 방문이 필요한 외부인은 장기출입증의 발급을 요청한다.
- (2) 장기출입증은 필요한 서류 및 사진의 제출, 팀(부서)장의 승인 후 물리보안담당자에게 신청하여 수령한다.

6) 출입증 재발급 및 권한 변경

(1) 출입증 분실 시 재발급

‘첨부 15 출입(사원)증 분실 경위서’에 의거 5일 이내에 사진 1매 (3 × 4cm)를 첨부하여 보안관리 부서에 재발급 의뢰한다.

(2) 오손, 훼손, 파손 시 재발급

분실 시 재발급에 준하여 재발급 신청한다.

(3) 기간만료 및 기타 변동사항 발생 시 재발급

- a. 인가자의 출입증에 장애가 있는 경우 출입증을 재 발급하고 장애 조치 시 원상태로 복원한다.
- b. 장기출입증의 경우 기간이 만료되는 경우 신청절차에 따라 기존 출입증을 회수 하고 재발급 한다.
- c. 보직 또는 재발급 인원이 소수일 경우 개인신청도 가능하다.

(4) 권한 변경

- a. 근무구역이 변경될 시에는 물리보안담당자에 통보하여 출입권한을 재획득하여 변경된 사원증으로 재발급 받아야 한다.

(5) 출입증의 갱신 및 폐기



- a. 점검결과 분실 또는 재발급등의 사유로 보안유지가 불가하다고 판단될 때에는 재가를 득하여 즉시 폐기하고 새로이 갱신한다.
- b. 출입증 양식, 도안 등은 보안유지상 갱신시점에서 표시를 변경하여 발급 운용하며 별도의 품의에 의거 발급한다.

(6) 출입증의 패용

- a. 회사 내 출입하는 방문자는 식별이 가능하도록 출입증을 패용해야 한다.
- b. 물리보안담당자는 경비실에 출입통제 지침을 공지하고 단속(점검) 권한을 부여하며 미 패용자에 대하여는 아래와 같이 조치한다.
 - 1회 적발자: 2회 이상 적발 시 조치사항에 대한 안내문 고지
 - 2회 적발자: 경위서 제출, 경고조치
 - 3회 적발자: 시말서 제출, 소속 팀(회사)에 경고장 발부
 - 4회 이상 적발자: 사업장 출입금지 및 사규에 의거 조치
- c. 경비실은 사전 통보된 방문자에 한해 소정의 신분증을 접수 받고 출입을 허가하며 방문 종료 후 경비실에 출입증과 신분증을 재고 환하여 출입을 종료한다.

(7) 출입자 제한사항

- a. 출입증에 허가된 지역만 출입이 허용되며 권한이 없는 지역에 출입해서는 안 된다.
- b. 출입증의 기술적인 장애 시 물리보안담당자에 통보 후 임시출입증을 발급 받아 출입한다.
- c. 통제구역에서는 사진, 동영상 등 어떠한 형태의 촬영도 할 수 없다.
- d. 당사의 자산은 반출증이 없는 경우 반출할 수 없다
- e. 노트북 등 전산장비의 반.출입이 필요한 경우 해당 팀(부서)장은 보안조치계획 및 출입자 보안서약서를 작성한 후 물리보안담당자에 요청하고, 전사보안책임자의 허가를 득하여 반.출입한다.



(8) 출입증 반납

퇴사 또는 직무변경에 의해 당사 근무자로 인정되지 않는 경우 직원증 (출입증)을 반납해야 한다.

(9) 차량 통제

방문객의 경우 사전에 차량출입을 신청하고, 물리보안담당자에 의해 승인된 차량에 대해 출입을 허용한다.

(10) 배달 및 하역 제한

a. 물품의 반입

경비실에서 내용을 확인하고 안전, 보안상 지장이 없는 물품에 한해서 반입을 허가한다.

b. 택배 및 생수 배달자

- 택배는 배달원이 정문에 접수시키고 수령 자에게 이를 통보한다.
- 정문에 접수한 택배 물품에 대한 책임은 수령자가 오랫동안 찾아가지 않고 분실할 경우 물품에 대한 분실 및 오손 책임은 없다.

c. 생수배달원은 2인 이하로 운영하고, 관련 지역 보안책임자가 생수 배달 회사와 배달원에게 서약을 집행하고 임시출입증을 발급한다.

3.1.5 업무연속성 관리

1) 업무연속성 관리절차 내 보안의 반영

- (1) 천재지변, 화재, 폭동 등과 같은 비상사태 발생에 대비하여 전사에 걸쳐 업무연속성 계획을 개발하고 유지하기 위한 조직 및 관리 프로세스가 수립되어야 한다.
- (2) 비상사태 발생시 정보시스템의 계속적 운영과 업무 중단 시 최단 시간 내에 업무를 재개할 수 있도록 업무 우선순위에 따라 비상계획이 수립되고 운영 되어야 한다.
- (3) 업무연속성 계획의 변경 절차가 수립되어야 하며, 변경된 업무연속성 계획을 관련 임직원에게 교육하고 공지하여야 한다.



- (4) 업무연속성 계획은 정기적으로 테스트되고 그 유효성이 검증되어야 한다.

4. 기술보안

4.1 최종사용자보안지침

4.1.1 목적

- 1) 업무상 목적으로 회사에서 지급한 데스크탑PC 및 노트북(이하 'PC'라 한다.), 프린터, 스캐너 등 개인업무용 전산장비의 정보기술 보호를 위한 요구사항을 제공함에 그 목적이 있다.

4.1.2 관리항목

- 1) 개인용 전산장비는 영문+숫자+특수문자포함 8자리 이상의 로그인, 화면 보호기 비밀번호가 설정되어 있어야 한다.
- 2) 모든 PC에는 회사 업무용 목적으로 사용되는 회사에서 배포되는 프로그램만 설치가 가능하며, 불법 S/W 사용에 대한 책임은 본인에게 있다.
- 3) 모든 PC에는 악성코드실행방지솔루션 등 보안시스템이 설치되어야 하며, 사용자는 최신업데이트 및 최신보안패치 적용을 해야 하고, 그 현황이 유지되어야 한다.
- 4) PC내의 파일을 공유할 필요가 있을 경우, 비밀번호가 설정된 공유폴더를 설정하여, 인가된 사용자만 접근할 수 있도록 해야 한다.
- 5) 공용PC에 대한 관리자를 지정해야 하며, 공용PC에는 보안문서를 저장할 수 없다.
- 6) 인터넷을 사용하는 경우 회사 보안정책(접근차단시스템 등)을 준수하며, 승인되지 않은 인터넷망을 사용하여서는 안된다.
- 7) 보안문서는 외부로 공중 네트워크(인터넷 등)를 거쳐 전송하는 것은 불허하며, 부득이한 경우는 사전 또는 사후에 관리자의 승인을 받아야 한다.

- 8) 사용자는 회사에서 지급한 H/W, S/W의 변경을 임의로 하여서는 안되며, 이동형 저장장치는 승인절차를 거친 후 사용한다.

4.2 네트워크보안

4.2.1 목적

사내 네트워크 구성 및 외부 네트워크 연결 시 요구되는 정보기술보호의 수준을 향상시킴으로써 안정적인 네트워크 인프라를 갖추는데 그 목적이 있다.

4.2.2 관리항목

- 1) 사내 네트워크는 외부에서 접근이 통제되는 사설망을 구축해야 한다.
- 2) 외부에서 공중망을 통해 내부 네트워크로 접속하고자 할 경우, 암호화 및 인증 절차를 통하여 업무상의 목적으로만 사용해야 하며, 접근기록을 관리해야 한다.
- 3) 중요도가 높은 시스템 및 네트워크는 분리되어야 한다.
- 4) 허가되지 않은 전산장치의 회사 네트워크 사용을 금지한다.
- 5) 외부 방문객 또는 개인 노트북의 네트워크 사용 시 정보기술보안관리자의 승인을 받은 후 사용해야 한다.
- 6) 신규 네트워크 설치 또는 구성 변경 시 테스트 등 검증 과정을 거친 후 승인절차에 의해 설치 및 변경해야 한다.
- 7) 인가되지 않은 AP는 통제되어야 하며, 무선랜은 128bit 이상의 암호화 키를 적용해야 한다.
- 8) 네트워크장비 설정 내용 백업 등 장애발생에 대비해야 한다.
- 9) 네트워크장비의 접근통제가 이루어져야 한다.

4.3 서버보안

4.3.1 목적

서버시스템을 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운영 관리하는데 그 목적이 있다.

4.3.2 관리항목

- (1) 서버의 운영 프로세스에 대한 지침이 마련되어야 한다.
- (2) 시스템 설치 시 기본적으로 생성되는 계정 및 사용하지 않는 계정은 삭제 및 변경되어야 하며, 적절한 계정관리를 통하여 접근 통제되어야 한다.
- (3) 비밀번호는 영문, 숫자, 특수문자 혼합으로 8자리 이상이며 3개월 이내 변경되어야 한다.
- (4) 서버시스템은 개발과 운영시스템이 분리되어야 한다.
- (5) 데이터 및 어플리케이션의 개발 및 변경은 적절한 절차에 따라 승인되어야 하며, 테스트 후 운영에 반영되어야 한다. (전산부문장은 개발.보수요청서/데이터변경요청서 및 개발보수/data변경 요청등록 내역을 승인후 관리 서버 직접 적용/배포)
- (6) 테스트데이터는 사용자 정보 등 중요정보를 포함하여서는 안된다.
- (7) 서버시스템에 대한 주기적인 취약점 점검 및 조치가 이루어져야 한다.
- (8) 운영체제, 데이터베이스에 대한 백업 및 원격지 소산이 되어야 한다. (전산 부문의 기록류에 관한 기준 의거 관리)
- (9) 서버시스템 장애에 대비한 복구계획이 마련되어야 한다.

4.4 정보통신보안시스템운영

4.4.1 목적

- (1) 정보통신보안시스템(침입차단시스템, 악성코드차단시스템 등)을 안정적, 효율적으로 운영관리하기 위한 지침을 제공하는데 그 목적이 있다.

4.4.2 관리항목

- (1) 정보통신보안시스템의 운영에 대한 지침이 마련되어야 한다.

- (2) 시스템은 인가된 사용자만이 접근해야 하며, 비밀번호는 영문, 숫자, 특수 문자 혼합으로 8자리 이상으로 설정되어야 한다.
- (3) 침입차단시스템은 필요한 서비스만을 명시적으로 허용하고, 그 외는 모두 불허한다.
- (4) FTP와 P2P서비스는 차단하며, 필요 시 승인절차를 통해 허용한다.
- (5) 이동형 저장장치를 통제할 수 있는 시스템을 구축해야 한다. (DLP시스템으로 등록승인 한다)
- (6) 보안시스템 관리자는 로그 기능이 항상 가동되도록 하고, 주기적으로 모니터링 및 분석해야 하며, 관련 로그는 1년 동안 보관해야 한다.
- (7) 분기별 1회 이상 취약점 분석을 통한 취약점을 보완해야 한다.

4.5 정보통신보안사고관리

4.5.1 목적

- (1) IT 침해사고에 대한 대응 및 복구업무를 포함하고 있으며, IT인프라에 대한 피해를 최소화하고 재발 방지를 통하여 정보자산의 보안성과 안정성을 유지하는데 필요한 지침을 제공하는데 그 목적이 있다.

4.5.2 관리항목

- (1) 정보통신보안사고 발생 시 정보기술보안관리자는 긴급히 대응하고, 그 처리 결과를 전사보안책임자 또는 대표이사에게 보고해야 한다.
- (2) 사내의 모든 사용자는 침해사고 발견 시 즉시 정보기술보안관리자 또는 전사보안관리자에게 보고해야 한다.
- (3) 외부에서 침입한 흔적이 의심되는 경우 정보기술보안관리자는 보안진단 도구나 체크리스트를 이용하여 점검해야 하며, 데이터의 변조나 불법 접근이 있을 경우 해당 서비스를 중지시킨다.
- (4) 침입자를 식별하기 위한 증거 수집 및 모든 기록을 유지 관리해야 한다.

- (5) 사안에 따라 공동작업이 필요하다고 판단될 경우 외부업체 및 대외 기관에 통보하고 협조를 요청한다.
- (6) 침해사고에 의한 정보시스템의 장애 시 신속히 복구되어야 하며, 장애복구에 대한 모의훈련이 주기적으로 실시되어야 한다.
- (7) 조치된 사안에 대해서는 근본 해결책을 강구하고, 재발방지를 위한 대응책을 마련한다.
- (8) 공개가 허용된 침해사고는 임직원에게 공지 또는 교육해야 한다.

5. 보조기억매체 관리

5.1 보조기억매체는 승인,등록으로 관리한다.

5.2 보조기억매체 관리요령

- 1) 일반용은 캐비닛 등에 안전하게 보관하여야 한다.
- 2) 각 팀(부문)장은 부서의 보조기억매체 관리에 책임이 있으며 팀원들에게 교육을 통해 업무 목적외에는 사용할 수 없도록 관리해야 한다.
- 3) 보조기억매체 불용처리 및 재사용
 - (1) 업무상 목적으로 사용한 보조기억매체는 불용처리시 물리적 파기를 원칙으로 하고 각팀(부문)장이 책임관리 한다.
 - (2) 타부서 이전 또는 용도를 전환하여 사용하고자 할 경우에는 수록된 자료를 완전히 삭제.포맷 후 사용하여야 한다.
- 4) 보조기억매체의 분실, 소각시 대처방안
 - (1) 취급자는 보조기억매체의 분실 또는 소각 등의 사유가 발생한 즉시 관리책임자(팀(부문)장)에게 그 사실을 보고한다.
 - (2) 관리책임자는 보조기억매체의 분실 또는 소각사실을 보고 받은 즉시 전산부문장에게 통지하여야 한다.

5) 보조기억매체 고장.훼손,오인삭제.포맷시 대처방안

(1) 보조기억매체의 고장,자료의 훼손 또는 자료의 오인삭제,포맷시 '3)보조기억매체 불용처리 및 재사용'에 의거 불용처리를 원칙으로 한다. 다만, 자료의 복구가 필요한 경우 상용 소프트웨어 활용 및 민간업체에 의뢰할 수 있다.

6. 자료접근권한 및 패스워드 관리

6.1 자료접근 권한부여 요청

6.1.1 해당 부문장은 중요 전산자료에 대하여 자료접근권한이 부여된 상황을 유선,또는 e-mail 등의 방법으로 전산부문장에 자료 요청할 수 있다.

6.1.2 해당 부문장은 공유될 자료와 공유되지 말아야 할 자료가 구분되고, 전산에 권한이 부여된 사용자를 면밀히 검토후에 권한부여가 변경되어야 할 사항을 '자료권한 및 메일계정 부여요청서'에 의거 전산부문장에 요청하여야 한다.

6.2 자료접근 권한부여 설정

6.2.1 전산 부문장은 권한부여 요청에 대한 즉시 설정 변경하여야 한다.

6.2.2 검토결과 설정변경 불가 및 타부서의 의견이 필요로 할 경우에는 '자료권한부여요청서' 로 해당부문장에 설정변경 불가사유를 밝히고 설정변경 불가함을 통보할 수 있다.

6.3 자료접근 권한 관리

6.3.1 자료접근권한 부여관리는 '자료접근권한 계정관리지침'에 의거 관리한다.

6.3.2 전산부문장은 원활한 전산운영에 필요하다고 판단될 경우에는 권한부여 설정사항을 변경할 수 있으며 이때에는 해당부문장에 설정변경 필요 사유를 유선 또는 E-Mail로 통보하여야 한다.

6.3.3 권한부여처리사항은 접수받은 요청서를 파일(철)하여 관리 되어야 한다.

6.4 패스워드 관리

- 6.4.1 서버장비와 네트워크 장비에 대하여 3개월마다(90일) 패스워드 설정을 변경토록 한다.
- 6.4.2 패스워드는 영문자,특수문자,숫자 조합을 원칙으로 하며 8자리 이상으로 한다.
- 6.4.3 서버장비와 네트워크 장비의 '사용자ID 및 패스워드 관리지침'에 의거 관리하며 사내비, 대외비 문서로 관리한다.
- 6.4.4 사용자 컴퓨터 및 해당부문에서 사용되는 컴퓨터의 패스워드관리는 해당 부문장 및 개인별 사용자에게 의해 관리되어야 한다. (전산자료로서 기록, 보관, 관리될 사유는 없다)

7. 협력사 보안 제재방안

- 7.1 협력사는 회사의 승인없이 일방적으로 제3자에게 누설하여서는 아니되며, 만약 위반 시 법적인 책임은 물론 징계위원회에 회부되어 협의를 거쳐 징계 조치 한다.
- 7.2 경미한 위반인 경우 : 경고장 발행 ,사장 명의 경위서 및 대책서 접수 등을 받는다.
- 7.3 중대한 위반인 경우 : 협력사 고객에게 중대위반 통보, 민형사상 고발조치 및 거래중지 조치하여야 한다.
- 7.4 협력사와 회사간 체결한 계약내용을 성실히 이행하여야 하며 이를 위반 했을 시 계약을 파기할 수도 있다.
- 7.5 그외에 협력사가 회사에 재산상의 불이익을 가했을때 법적조치 및 징계위원회에 회부된다.
- 7.6 민형사상 고발조치 및 거래중지 항목
 - 7.6.1 본 항목은 통상적인 항목만을 기술한것으로 표기되지 않은 항목도 조치



대상에 포함될 수 있다.

7.6.2 거래시 품명, 단가, 품질가공규격, 불량, 설비 유지관리, 소재(가공,반철) 회수 등

7.6.3 영업정보(비밀), 생산계획, 도면정보 및 파일, 기타거래정보 등

7.6.4 바이러스유포, 해킹, 미승인자료 웹상공개, 기타각종정보파일 등

7.6.5 그 외에 협력사가 회사에 손해를 끼치는 행위 등을 제재대상에 포함된다.

8. 소프트웨어 자산관리(원칙)

8.1 소프트웨어는 정품사용을 원칙으로 한다.

8.2 정보관리부서에서 지정한 소프트웨어 외에는 임의로 다운로드/복사/설치하여 사용할 수 없다.

8.3 업무상 필요한 소프트웨어는 사전 승인을 득한다음 사용할 수 있다.

8.4 불법소프트웨어 사용에 위반되는 행위로 회사에 손해를 끼치는 임직원은 민/형사상 책임 및 징계대상에 해당된다.

9. 기록관리

본 지침서에 관련된 기록들은 '기록관리 지침서'에 따라서 관리되어야 한다.

10. 관련 문서

10.1 문서정보관리 절차서

10.2 전산장비 운영관리 지침서

10.3 전산업무 지침서