# OOO기업 영업비밀보호규정

OO관리부
제정: 2025. 04. 18.
개정: 2026. 04. 18.

## 제1장 총칙

**제1조(목적)**
이 규정은 회사의 영업비밀 관리 및 보호에 필요한 사항을 정함으로써, 임직원 및 관련자가 영업비밀을 적절하게 취급하고, 부정한 유출 또는 사용으로부터 이를 보호하여 회사의 경쟁력을 유지·강화하며, 궁극적으로 회사의 지속 가능한 발전을 도모하는 것을 목적으로 한다.

**제2조(적용범위)**
① 이 규정은 회사에 신규 채용되어 근무 중이거나 퇴직한 모든 임직원 및 근로자, 그리고 계약, 업무상 접근 또는 신의칙에 따라 회사의 영업비밀에 접근하거나 이를 인지하게 된 협력업체, 외주업체, 용역 인력 등 제3자에게 적용한다.
② 이 규정은 「부정경쟁방지 및 영업비밀보호에 관한 법률」, 「개인정보 보호법」, 「근로기준법」 등 관련 법령에 근거하여 제정되며, 본 규정이 관계 법령과 상충될 경우에는 관계 법령을 우선 적용한다.
③ 본 규정은 회사의 정보보안규정, 임직원 행동강령, 인사관리규정 등 관련 사내 규정과 함께 적용되며, 규정 간 내용이 충돌하는 경우 영업비밀 보호의 필요성과 중요성을 고려하여 본 규정을 우선 적용한다.

**제3조(용어의 정의)**
본 규정에서 사용하는 용어의 정의는 다음과 같다.

1. 영업비밀: 회사가 보유 또는 사실상 보유한 정보로서, 공공연히 알려져 있지 아니하고, 독립된 경제적 가치를 가지며, 상당한 노력에 의해 비밀로 유지된 기술상 또는 경영상의 정보를 말한다. (「부정경쟁방지 및 영업비밀보호에 관한 법률」 제2조 제2호 준용)
2. 유출: 비밀로 분류된 정보나 자산이 외부로 누설되어 회사의 재산상 피해가 발생하거나 발생할 우려가 있는 행위를 말한다.
3. 위반행위: 본 규정에서 정한 영업비밀 보호 의무를 고의로 위반하거나, 중대한 과실 또는 방관으로 인해 결과적으로 규정에 위배되는 모든 행위를 포함한다.
4. 종업원: 회사의 지휘나 감독을 받아 업무를 수행하는 자를 말하며, 임직원을 포함한다.

5. 제3자: 회사와 계약관계에 있는 자로서 협력업체, 인력파견회사, 수탁가공업체, 하도급업체, 공동연구기관, 기술거래업체, 프랜차이즈 가맹점, 컨설팅회사, 법률대리인, 장비·시설 설치 및 유지보수업체, 외국인 등을 포함하며, 실질적으로 계약관계에 있는 상시 거래처도 이에 해당한다.
6. 비밀문서: 그 내용이 외부에 누설될 경우 회사에 유해한 결과를 초래할 우려가 있는 문서로, 연구노트 등 대외비 문서를 포함한다.
7. 일반문서: 비밀문서를 제외한 운영계획서, 예산서 등 회사의 고유 업무 내용이 담겨 있어 유출 시 보호가 필요한 문서를 말한다.
8. 전자문서: 정보처리장치에 의하여 전자적 형태로 작성, 송신, 수신 또는 저장된 문서로서, 이메일, 전자결제문서, 전자보고서 등 일체의 전자형 문서를 포함한다.
9. 정보: 회사의 경영 또는 활동에 필요한 일체의 지식을 말한다.
10. 정보자산: 정보(데이터) 자체와 이를 수집, 처리, 전송, 보관, 폐기, 보호하는 시스템 등 정보보호와 관련된 유·무형의 모든 자산을 의미한다.
11. 정보시스템: 회사가 보유한 컴퓨터, 전산시스템, 네트워크, 소프트웨어, 영상매체시설물 등 정보 관리에 사용되는 일체의 장비 및 시스템을 말한다.
12. 정보처리장치: 정보시스템 중 정보의 전자적 처리, 저장, 검색, 출력 등을 수행할 수 있는 장비로서 컴퓨터, 서버, 스마트기기, 복합기, 저장장치 등을 포함한다.
13. 전자기록매체: 정보를 전자적 방식으로 기록·저장할 수 있는 장치로, 하드디스크, SSD, USB, CD/DVD, 메모리카드 등 물리적 매체뿐만 아니라 클라우드 저장소 등 가상 공간을 포함한다.

## 제2장 영업비밀 보호대상 및 보안관리 체계

**제4조(보호대상)**

이 규정은 회사가 보유하고 있는 다음 각 호를 보호대상으로 한다.

1. 반도체 제조 공정 기술, 회로 설계와 최적화 및 칩 아키텍처, 전력 최적화 알고리즘 등에 관한 연구 관련 정보와 기술적 정보, 경영상의 정보와 관련한 영업비밀 그 자체
2. 영업비밀이 체화된 물건 및 물체(예시: 서류, 도면, 복사물, 자기테이프, 자재, 생산품, 금형, 정보시스템에 저장된 파일과 같은 정보자산 등)
3. 영업비밀 생산설비와 장비
4. 영업비밀 통제구역
5. 기타 회사 기밀과 관련된 정보

**제5조(영업비밀 보호운영협의회 설치 및 기능)**

① 회사는 영업비밀 보안심의위원회(이하 "위원회")의 심의·의결 사항에 따라, 영업비밀 보호 정책의 실행계획을 수립하고 실무를 조정·지원하기 위해 영업비밀 보호운영협의회(이하 "협의회")를 설치·운영한다.

② 협의회는 대표이사를 의장으로 하며, 정보보호 최고책임자(CISO)가 총괄보안담당관으로 한다. 관리 및 정보보안담당관은 협의회의 간사가 된다.
③ 협의회의 전략적 의사결정 및 사업부문별 보안 현안 조율을 위하여, 메모리사업부장, 파운드리 사업부장, 시스템LSI사업부장, 법무팀장은 협의회의 상임 참석자로 지정되며, 각 부문의 특수성과 보안요구사항을 반영한 협의에 참여한다.
④ 관리 및 정보보안담당관은 협의회 회의록의 기록 유지 및 일반 서무를 관장하며, 영업비밀 보호 관련 교육 및 인식 제고 활동을 담당한다.
⑤ 협의회는 다음 각호의 사항에 대하여 심의 결정한다.
1. 위원회에서 심의·의결된 정책 및 기준의 실행방안 수립 및 구체화
2. 전사 보안 실행 계획의 수립, 점검 및 부서 간 업무 조율
3. 영업비밀 유출 예방을 위한 실무 대응 방안 마련 및 점검
4. 신기술(예: 생성형 AI) 도입 관련 부서 협의 및 실무 가이드 마련
5. 영업비밀 보호 관련 교육, 캠페인 등 인식 제고 활동의 기획 및 실행
6. 기타 영업비밀 보호 업무 실행을 위해 필요한 실무 조정 및 후속조치

**제6조(보안총괄책임자의 지정 및 임무)**
① 회사는 영업비밀 보호 및 보안 체계의 전사적 총괄을 위하여 보안총괄책임자를 1인 지정한다.
② 보안총괄책임자는 정보보호 최고책임자(CISO)가 담당하며, 경영진에 직접 보고할 수 있는 권한을 가진다.
③ 보안총괄책임자는 다음 각 호의 임무를 수행한다.
1. 회사 전반의 보안 전략 및 정책 수립 및 총괄
2. 관리보안 및 정보보안 각 영역의 협업 조정 및 통합 보안관리 체계 운영
3. 보안담당관(관리보안담당관 및 정보보안담당관)의 업무 수행 점검 및 지원
4. 보안 사고 발생 시 총괄 대응 및 의사결정
5. 기타 회사의 보안 수준 향상을 위한 조정·지휘 업무

**제7조(보안담당관의 지정 및 임무)**
① 회사는 영업비밀 보호 및 보안업무의 효율적 수행을 위하여 다음 각 항의 보안담당관을 각각 1명씩 지정한다. 보안담당관은 회사의 전반적인 보안 체계를 지원하며, 각자의 영역에서 보안업무를 지휘·조정·통제하고 감독할 수 있는 자로서 수석급 이상으로 임명한다.
② 관리보안담당관은 다음 각 호의 임무를 수행한다.
1. 영업비밀 보호를 위한 보안 정책 및 제도 운영계획의 수립, 조정 및 감독
2. 영업비밀 보호 관련 교육, 보안서약, 인사관리 집행
3. 기밀 자료의 등록 및 물리적 보관·운용 관리
4. 통제구역 및 보안구역의 인가·해제 관리
5. 기타 영업비밀 보호와 관련된 관리적·조직적 조치의 기획 및 집행
③ 정보보안담당관은 다음 각 호의 임무를 수행한다.
1. 정보시스템 및 통신망 내 영업비밀 보호에 관한 계획 수립 및 기술적 보안 조치 수행

2. 연구정보, 개발자료 및 기술 관련 영업비밀에 대한 보안 관리
3. 영업비밀 소유 현황 조사 및 정보 유출방지 대응
4. 자체 정보보안 점검 및 침해사고 대응 체계 운영
5. 기타 영업비밀 보호에 필요한 정보보안·기술보안 관련 업무
④ 회사는 영업비밀 보호 업무의 전문성과 효율성을 제고하기 위하여, 관리보안과 정보보안을 이원화하여 각 담당관이 독립적으로 해당 영역을 분장·관리하도록 한다.

**제8조(분임 보안담당관의 지정 및 임무)**
① 각 보안담당관은 각 부서의 업무 특수성을 고려하여 각 분야별 분임 보안담당관을 책임급으로 임명할 수 있다.
② 분임 보안담당관은 해당 보안담당관의 지휘 및 감독을 받아 자체 소관 업무의 범위 내에서 다음 각 호의 임무를 수행하여야 한다.
1. 소관업무에 관한 자체 보안계획의 수립 및 시행
2. 회사 내 여러 서비스에 관한 정기적인 보안진단
3. 부서 내 영업비밀 및 기밀 자료의 소유 현황 및 관리
4. 연구 과정 및 성공 유무에 관계없는 비밀 유지
5. 비밀취급 인가증 및 인가자 관리
6. 소속 직원에 대한 기초 및 AI 및 클라우드 관련 보안 교육
7. 기타 보안담당관이 지시하는 사항
③ 분임 보안담당관은 사안의 성격에 따라 관리보안담당관 또는 정보보안담당관의 지휘 및 감독을 받아 업무를 수행할 수 있다.

**제9조(보안실무자 지정 및 임무)**
① 분임 보안담당관은 비밀을 취급하는 해당 부서에서 업무상 영업비밀을 가장 많이 취급하는 과의 책임자를 보안실무자(이하 "정" 실무자라 한다)로 임명하고, "부" 실무자를 선임 및 사원으로 임명한다.
② 과 및 분야별 업무가 상이할 시, 과 또는 분야별 "부" 실무자를 둘 수 있다.
③ 보안실무자는 "부" 실무자를 지휘 및 감독하여 다음 각 항의 임무를 수행한다.
1. 영업비밀을 최선의 상태로 보관되도록 관리한다.
2. 비밀의 도난, 누설, 분실 및 기타 손괴 방지를 위한 감독업무를 이행한다.
3. 비밀관리기록부, 비밀 열람 및 비밀 대출부 등의 기록을 철저히 유지한다

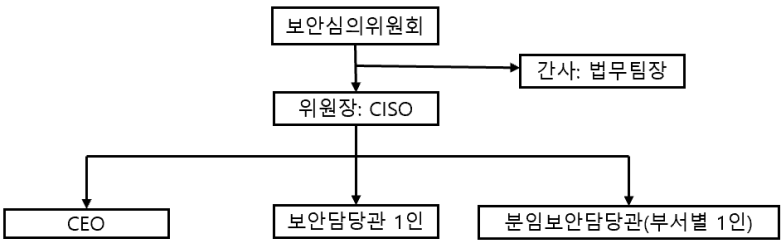
**제10조(영업비밀 사용 이력 관리 및 점검)**
① 보안실무자는 제12조제3항의 서류를 별도로 보관하고, 회사 내의 컴퓨터 및 전자기록매체 등의 존재 및 사용현황을 수시로 확인하여야 한다.
② 영업비밀자료에 대한 사용 이력은 정보시스템과 서류 내에서 최소 3년 이상 유지 및 보관한다.
③ 관리보안담당관은 연간 1회 이상 영업비밀 관리현황을 종합 점검하고 점검결과를

작성하여 총괄보안담당관에게 승인을 받아야 한다.

## 제3장 영업비밀 보안심의위원회

**제11조(영업비밀 보안심의위원회의 설치)**
회사는 영업비밀 보호와 보안업무의 효율적 수행을 위하여 영업비밀 보안심의위원회(이하 "위원회")를 두며, 위원회는 영업비밀 보안에 관한 주요 사항을 심의·의결하며, 구성 및 운영에 관한 세부사항은 별도의 지침으로 정한다.

**제12조(위원회의 구성 및 임무)**
① 위원회는 다음 각 호와 같이 구성한다.
1. 위원장: 정보보호 최고책임자(CISO)
2. 위원: 최고경영자(CEO), 보안담당관 1인 및 분임보안담당관 각 부서별 1명
3. 간사: 법무팀장




② 위원회는 다음 각 호의 사안을 심의 및 의결한다.
1. 영업비밀 보호 정책 및 지침의 제·개정
2. 영업비밀 보호를 위한 예산 및 자원 할당
3. 보안사고 및 영업비밀 위반사항의 심사 및 조치
4. 신기술 및 중요정보의 보호 방법 결정
5. 외부 협력업체와의 계약 시 정보 공개 범위 결정
6. 내부감사 결과 및 후속 조치 검토
7. 보안 관련 부서의 요청사항 검토
8. 보안감사 일정조율 및 인력지정
9. 국회, 언론, 정부기관 등 외부기관 제출 문서에 대한 사전 보안심의
10. 기타 위원장이 필요하다고 인정하는 사항

**제13조(안건의 제출 및 심의 절차)**

① 위원회는 위원장이 소집하며, 위원장이 그 의장이 된다.
② 위원회의 회의는 재적 위원 과반수의 출석과 출석 위원 과반수의 찬성으로 의결한다. 단, 가부 동수인 경우에는 위원장이 결정한다.
③ 회의는 원칙적으로 회의 형식으로 개최하되, 경미한 사안 또는 긴급한 경우에는 서면 결의로 처리할 수 있다.
④ 위원장은 필요 시 관계자를 출석시켜 의견을 청취할 수 있다.
⑤ 위원회는 정기적으로 월 1회 이상 개최하며, 필요한 경우 수시로 소집할 수 있다.
⑥ 위원회의 의결사항은 위원장 결재 후 즉시 효력을 발생한다.
⑦ 최고경영자(CEO)는 모든 위원회 회의에 당연히 참석하며, 필요 시 의견을 제시하거나 의결에 참여할 수 있다.

# 제4장(인원보안)

**제14조 (신규 채용자, 현직 임직원, 퇴직(예정)자에 대한 보안 조치)**
신규 채용자는 다음 각 호에 따른 절차를 거친다.
1. 입사 전 배경 조사 및 산업기밀 유출 이력을 확인한다.
2. 채용 확정 시, 영업비밀 보호 서약서를 제출 및 입사 초기 보안 교육을 이수해야 한다.
3. 입사자에 대해 국가보안법, 산업기술보호법 관련 위반 이력을 검토한다.
현직 임직원은 다음 각 호에 따른 절차를 거친다.
1. 입사 시 영업 비밀 보호 서약서를 제출하고 연 1회 이상 보안 교육 이수해야 한다.
2. 재직 중 알게 된 반도체 기술 및 제조 공정 정보를 외부에 누설하거나 사적 유용할 경우 형사 및 민사 책임을 진다.
3. 업무 수행 시 기밀 접근 로그는 자동 저장 및 모니터링되며 이상 접근 탐지 시 보안부서가 즉시 확인·조치한다.
퇴직(예정)자는 다음 각 호에 따른 절차를 거친다.
1. 퇴직 전 보안 면담 실시하고 모든 영업 비밀 자료(문서, 전자파일, 저장 매체 등)를 반환,해야 하며  미반환 시 법적 책임을 진다.
2. 퇴사자 보유 기기의 디지털 포렌식 분석을 통해 회사 정보 보유 여부를 점검하고 회사 관련 정보는 모두 삭제하고 보고한다.
3. 퇴사자의 개인 저장 매체(USB, 외장 하드), 개인 이메일, 클라우드 저장소에 저장된 회사 정보는 삭제 확인서를 통해 삭제 여부를 명확히 한다.
4. 반도체 핵심 기술을 취급한 자에 한해 퇴직 후 최대 2년 동안 경쟁사 취업을 제한할 수 있으며, 이에 대한 정당한 보상(재직 중 인센티브, 퇴직 후 일정 보상 등)이 제공된다.
5. 퇴사자의 시스템 계정, 접근 권한은 퇴직 즉시 해지하며, 정보 보안 담당 부서는 계정 비활성화, 이메일 종료, 저장 기기 회수 및 삭제 여부 확인을 기록으로 남긴다.

**제15조 비밀 취급의 인가 및 해제**

① 회사는 반도체 기술, 제조 공정 등 영업 비밀 정보를 취급하는 직원에 대하여 비밀 취급 인가 절차를 적용하며, 인가는 직무의 필요성, 보안 위험 평가, 신원 정보 등을 종합적으로 고려하여 결정한다.
② 비밀 취급 인가는 보안 등급(1급, 2급, 3급)에 따라 구분되며, 다음 사항을 포함한다.
1. 인가 대상자의 소속, 직무, 인사 이력
2. 정보 접근 필요성과 범위
3. 비밀 보호 서약서 및 보안 교육 이수 여부
4. 신원 진술서 및 전력 확인 결과(필요 시)
③ 비밀 취급 인가는 정보보호 최고책임자(CISO)의 승인을 거쳐야 하며, 인가 이력은 비밀 취급 인가대장에 등록 및 보관한다.
④ 인가된 직원은 최소 연 1회 보안 점검 및 재검토 절차를 이행하며, 직무 변경, 장기휴직, 퇴직, 비위 행위 발생 시 즉시 인가를 해제하거나 등급을 하향 조정할 수 있다.
⑤ 비밀 취급 인가가 해제되는 경우, 관련자의 정보 접근 권한은 즉시 차단되며, 인가 해제 사실은 본인 및 관련 부서에 통보되고 인가 대장에 해제 사유 및 일시를 기록한다.
⑥ 비밀 취급 인가와 관련된 모든 서류 및 기록은 최소 5년간 보관한다.

**제16조(임시직 및 단순 고용직 관리)**
① 임시직 및 단순 고용직을 채용하고자 할 때에는 보안 담당관의 사전 합의를 거쳐야 한다.
② 임시직이나 단순 고용직으로 임용되는 자 중 중요 시설·지역의 통제·출입 및 중요 문서·자재의 취급자로서 당해기관의 장이 보안상 필요로 하는 자 외에는 신원 조사를 생략한다.
③ 임시직 또는 단순고용직에게는 보안상 책임있는 임무를 부여하여서는 아니 된다.
④ 임시직 또는 단순 고용직에 대하여 부득이 비밀 취급을 인가하고자 할 때에는 소속 보안심사 위원회 또는 자체 심의 기구의 의결을 거쳐야 한다.
⑤ 임시직 또는 단순 고용직으로 인하여 야기되는 보안 책임은 소속기관장이 진다.

**제17조 (외부인에 대한 보안 조치)**
① 회사 방문객(협력 업체, 외부 용역 업체, 고객, 연구 기관 관계자 등)은 사전 등록 및 출입 승인을 받아야 하며, 출입증을 패용해야 한다.
② 외부인은 허가된 장소 외에는 출입할 수 없으며, 필요 시 보안 담당자의 동행 하에 이동한다.
③ 외부 방문객은  비밀유지계약(NDA)을 작성하고, 촬영, 녹음, 무단 저장 행위는 엄격히 금지된다.
④ 외부 용역 및 협력 업체 인력은 업무 수행 전 보안 교육 이수 후 제한된 범위 내에서 정보 접근 권한이 부여되며, 기간 종료 후 즉시 회수된다.

**제18조 (외국인 고용에 따른 보안 조치)**
① 외국인 직원을 채용할 경우, 국가별 보안 리스크를 반영한 신원 확인 및 보안 등급을

부여한다.
② 반도체 핵심 기술 및 제조 공정 관련 업무에 외국인이 배정될 경우, 전용 보안 서약서를 작성하고 주기적인 보안 점검을 실시한다.
③ 외국인 직원 퇴사 시, 디지털 포렌식 및 저장 매체 점검을 포함한 정보 반출 여부를 확인하고 모든 기밀 정보의 삭제 여부를 점검한다.
④ 필요 시, 특정 국가 출신 인력의 채용 또는 보안 구역 접근을 제한할 수 있으며, 이에 대한 기준은 국가보안법 및 대외 무역법을 따른다.

**제19조 (보안 등급 및 접근 권한 부여)**
① 영업 비밀 보호 수준에 따라 보안 등급을 '1급', '2급', '3급'으로 구분하며, 핵심 기술 및 생산 공정 정보는 '1급(극비)'으로 분류한다.
② '1급' 자료는 연구소, 생산 기술팀 등 핵심 인력에 한해 접근이 가능하며, 이들은 별도 보안 교육 및 서약서를 이수해야 한다.
③ 접근 권한은 직무별로 최소 권한 원칙에 따라 부여되며, 접근 이력을 주기적으로 감사한다.
④ 모든 권한 부여는 정보보호 최고책임자(CISO)의 승인을 거쳐야 하며, 6개월마다 검토·갱신한다.

**제20조 (보안 교육 및 정기 점검)**
① 전 직원 및 외부 협력 업체 직원은 연 2회 이상 영업비밀 보호 교육을 의무적으로 수강해야 한다.
② 교육 내용은 기술 유출 사례 분석, 위반 시 법적 책임, 보안 사고 대응 절차, 디지털 기기 및 매체 관리 방안 등을 포함한다.
③ 정보 보안 부서는 정기 점검 및 비정기 로그 감사를 통해 인원 보안 준수 여부를 확인하며, 위반 시 즉각 시정 조치를 실시한다.

## 제5장(임직원의 영업비밀 보호 의무)

**제21조 (임직원의 기본 의무)**
① 모든 임직원은 직무 수행 중 취득한 영업비밀을 비밀로 유지하고, 회사의 사전 승인 없이 유출, 누설, 공유하거나 사적으로 이용할 수 없다.
② 반도체 공정, 연구개발 자료 및 주요정보를 저장, 전송, 파기할 때에는 회사의 정보보안 지침을 반드시 준수해야 한다.
③ 퇴사 이후에도 최소 3년간 영업비밀 보호의무가 지속되며, 퇴직자는 이를 유출하거나 타

목적으로 활용해서는 안 된다.

**제22조 (주요 직무자 지정 및 관리)**
① 회사는 중요정보(개인정보, 인사/재무 정보, 영업비밀 등) 또는 주요 시스템(DB, 서버 등)에 접근하는 직무를 '주요 직무'로 분류하고, 이를 수행하는 자를 '주요 직무자'로 지정한다.
② 주요 직무자는 최소 인원으로 지정하며, 지정 현황은 정보보안팀에서 목록으로 관리하고 6개월마다 검토·갱신한다.
③ 개인정보를 처리하는 자는 '개인정보취급자'로 별도 지정·관리하며, 수탁업체 인력도 포함된다.
④ 주요 직무자 및 개인정보취급자는 직무 변경, 퇴직 시 즉시 권한을 회수하고 목록에서 해제한다.

**제23조 (직무 분리 및 보완통제)**
① 개발, 운영, 보안, 개인정보 처리 등은 직무를 분리하여 권한 오·남용을 방지해야 하며, 부득이하게 분리 불가능할 경우 아래와 같은 보완통제를 적용한다.
1. 직무자 간 상호 검토 절차
2. 상위 관리자의 승인 및 정기 모니터링
3. 모든 작업 로그 기록 및 감사 시스템 구축
② 외부 위탁업체에는 계정 생성/삭제 권한을 부여하지 않으며, 불가피한 경우 보완통제를 적용한다.

**제24조 (비밀취급 인가 및 해제)**
① 반도체 핵심 기술 또는 중요정보에 접근하기 위해서는 CISO의 승인을 통해 비밀취급 인가를 받아야 한다.
② 비밀취급 인가자는 별도 서약서(별지 제4호)를 작성하며, 프로젝트 참여 시 별도 서약서(별지 제5호)를 추가 제출한다.
③ 인가 해제는 다음 사유로 즉시 이행되며, 관련 기록은 5년간 보관한다.
1. 직무 변경 또는 퇴직
2. 프로젝트 종료
3. 보안 위반 발생 시

**제25조 (공동연구 및 협력업체 제공자료의 보안관리)**
① 공동 연구 시에는 사전에 보안 등급, 문서 보관·파기 기준, 비밀 유지 서약서 및 공동 연구 계약서를 체결해야 한다.
② 연구 종료 시 자료는 전량 회수 및 폐기하고, 보유 시점 이후 무단 사용 시 형사/민사 책임이 부과된다.
③ 협력 업체 제공 자료는 별도 보안 표기를 부여하고, 접근 권한자는 기록으로 관리하며

종료 시 반납 또는 폐기를 확인한다.
④ 기술 이전 시에도 정보 제공 범위, 목적, 보관 기한 등을 명시한 계약서 및 보안 서약서를 작성하여야 한다.

**제26조 (국가R&D 및 국외수혜정보 보고 의무)**
① 임직원은 국가 R&D 연구성과 중 수출입 통제 대상 기술에 해당할 경우, '국외수혜정보 보고 제도'에 따라 사전 보고 의무가 있다.
② 국가 연구개발 성과물은 외국 기관 및 업체와 공유 시 산업기술보호위원회 승인 및 내부 보안점검을 거쳐야 한다.

**제27조 (법적 책임 및 관련 법률)**
① 다음의 법률에 따라 영업비밀 침해 시 민형사 책임이 부과된다.
-「부정경쟁방지 및 영업비밀보호에 관한 법률」
-「산업기술의 유출방지 및 보호에 관한 법률」
-「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
-「형법」 제 314조 업무방해죄 및 제 320조 비밀침해죄 등
② 침해 시 회사는 손해배상 청구 외에 형사고소, 징계 조치 등을 병행할 수 있다.

**제28조 (퇴직 시 보안조치 및 서약서 징구)**
① 퇴직자는 모든 영업비밀 및 관련 자료를 반납하고, 정보보안 부서 주관 하에 디지털 포렌식 및 저장매체 점검을 받아야 한다.
② 퇴직자는 퇴직 시점에 '비밀유지 서약서'를 다시 작성하고, 보안교육 및 퇴직 면담을 이수해야 한다.
③ 재직 중 반도체 핵심기술을 취급한 자에 대해 최대 2년 간 경쟁사 취업 제한이 가능하며, 이에 상응하는 보상이 제공된다.

**제29조 (영업비밀 보호 모임 및 경험 공유 활동)**
① 회사는 영업비밀 유출 방지 및 보안 문화 확산을 위하여, 임직원 간 경험과 사례를 공유하는 '영업비밀 보호 모임'을 정기적으로 운영할 수 있다.
② 본 모임은 정보보안팀 주관 하에 월 1회 이상 개최되며, 다음 각 호의 활동을 포함한다.
1. 부서별 영업비밀 관리 사례 및 이슈 공유
2. 유출 방지를 위한 예방 활동 및 실패 사례 분석
3. 최신 산업기술 보호 동향 및 관련 법령 변화 안내
4. 공동연구, 협력업체, 기술이전 시 발생한 보안관리 경험 공유
③ 모임을 통해 수렴된 현장 의견 및 개선사항은 정보보안 정책 및 교육 프로그램에 반영될 수 있다.
④ 필요 시 외부 보안 전문가 또는 산업기술보호 유관기관과의 협력 세미나를 병행할 수

있다.
⑤ 본 활동은 사내 정보보호 인식 제고 및 영업비밀 보호 역량 강화를 위한 비정형 학습 활동으로 간주한다.

# 제6장(문서보안)

**제30조(영업비밀의 취급)**
① 제6장 제3조에 의하여 분류된 영업비밀의 취급자격은 다음 각 호와 같다.
1. 1급 비밀: 대표이사, 대표이사가 지정한 임직원, 각 사업부의 사업부장, 사전에 허가된 보안담당관
2. 2급 비밀: 1급 비밀 취급자, 해당 영업비밀이 속한 담당부서의 분임 보안담당관 및 사전에 허가된 보안실무자
3. 3급 비밀: 1, 2급 비밀 취급자, 해당 영업비밀이 속한 담당부서의 보안실무자, 사전에 허가된 담당자
② 영업비밀로 관리하여야 하는 자료는 업무상 필요성이 있는 경우 이외에는 외부인 혹은 외부기관에 공개하거나 제공하지 않음을 원칙으로 한다.
③ 영업비밀을 취급하는 자는 비밀이 누설되지 않도록 본 규정에 따른 보안 조치를 취하여야 한다.

**제31조(영업비밀의 분류)**
① 회사는 영업비밀에 대해 그 중요성과 가치의 정도에 따라 아래와 같이 3단계로 분류하며, 등급별 세부 분류 기준은 별표1과 같다.
② 회사의 보안담당관 또는 선임은 각 영업비밀의 특성을 고려하여 다음 표의 보존기간보다 장기간을 보존기간으로 지정하도록 요청할 수 있다.

| 자료 등급 | 자료구분 | 내 용 | 보존기간 |
|---|---|---|---|
| 1급 | 별도관리자료 | 유출 시 회사의 존속, 법적 책임, 대외 신뢰도에 심각한 영향을 미치는 정보 | 영구보존 |
| 2급 | 특별보호자료 | 유출 시 경쟁력 또는 수익성에 중대한 영향을 미치나, 회사 존속 수준에는 이르지 않는 정보 | 10년 |
| 3급 | 일반보호자료 | 유출 시 제한된 범위 내에서만 영향이 발생하거나, 외부 협력사와 제한적으로 공유 가능한 정보 | 5년 |

③ 필요시 보안담당관 이상의 권한이 부여된 자에 한해 절차를 거쳐 영업비밀의 등급 분류를 변경할 수 있다.
④ 영업비밀은 본 관리규정에 따라 영업비밀로 관리되는 경우에는 원칙적으로 보존된다.
⑤ 보존기간이 만료되면 보안담당관 혹은 그 이상의 권한이 부여된 자에 한해 다시 영업비밀로 분류할 수 있다.

**제32조(영업비밀의 표시 및 보관)**

① 영업비밀은 그 문서의 표지 중앙 상단에 각 등급에 따라 다음과 같은 예고문을 붉은색으로 표시하여야 한다.

| 대 외 비 |
| --- |
| 1 급 비 밀 |
| 영 구 보 존 |

| 대 외 비 |
| --- |
| 2 급 비 밀 |
| 20 . . . 까지 |

| 대 외 비 |
| --- |
| 3 급 비 밀 |
| 20 . . . 까지 |

② 영업비밀이 화체된 서류, 물건 등은 일반 문서, 물건 등과 분리하여 별도의 보관함, 금고 등 보안장치를 구비하고 있는 용기에 넣어 특별히 관리해야 한다.

③ 영업비밀이 포함되어 있는 전자문서는 일반 전자문서와 분리하여 비밀번호를 설정하고, 영업비밀 취급자격이 있는 자 이외에는 열람할 수 없는 방법으로 보관하여야 한다.

④ 보관용기에 넣을 수 없는 영업비밀은 제한구역 또는 통제구역에 보관하는 등 그 내용이 노출되지 아니하도록 특별한 보호대책을 마련하여야 한다.

⑤영업비밀의 보관용기 외부에는 영업비밀의 보관을 알리거나 나타내는 어떠한 표시도 해서는 아니 된다.

⑥보관용기의 잠금 장치의 종류 및 사용방법은 보관책임자 외의 사람이 알지 못하도록 특별한 통제를 하여야 하며, 다른 사람이 알았을 때에는 즉시 이를 변경하여야 한다.

**제33조(보관책임자)**

① 보관책임자는 사내 비밀취급 인가를 받은 임직원 중에서 비밀등급별로 지정한다.

② 2급 비밀취급 인가를 받은 보관책임자는 3급 보관책임자를 겸할 수 있으나, 1급 비밀취급 인가를 받은 보관책임자는 2급, 3급 보관책임자를 겸할 수 없다.

② 보관책임자는 보안물품 보관 부서 단위로 1명의 주책임자를 지정하며, 보관 장비 수량 또는 보관 장소의 분산 정도에 따라 다수의 부책임자를 함께 둘 수 있다.

③ 보관책임자는 다음 각 호의 업무를 수행한다.

1. 영업비밀이 담긴 자료 또는 설비를 적정한 상태로 안전하게 보관할 것
2. 영업비밀의 유출, 절도, 분실 및 기타 훼손 등을 방지하기 위한 일상적 관리·감독을 수행할 것
3. 비밀관리기록부를 비치하고 최신 상태로 유지하며, 비밀대출부 및 비밀열람기록철에 대한 내용을 주기적으로 확인하고 점검할 것

**제34조(영업비밀의 접수・발송)**

① 영업비밀의 접수・발송은 다음 각 호에 따른다. 다만, 1급 비밀은 제1호 또는 제2호에 따라서만 접수・발송할 수 있다.

1. 암호화하여 사내 보안 정보통신망으로 접수・발송할 것
2. 비밀취급 인가를 받은 취급자가 직접 전달하거나 직접 수령하여 접수・발송할 것

3. 사내 공문 수발 체계 또는 지정된 물류 경로를 통하여 접수・발송할 것
4. 보안 등기우편 또는 사내에서 승인된 보안 택배 서비스를 이용하여 접수・발송할 것
② 영업비밀을 발송할 때에는 이중 봉투로 포장하여야 한다.
③ 문서 형태 외의 영업비밀(예: USB, 외장 저장장치 등)은 내용이 노출되지 아니하도록 완전 밀봉 또는 차광 포장하여야 한다.
④ 동일 부서 또는 사업장 내에서 영업비밀의 접수・발송 또는 전파 절차는 부서장 또는 보안담당관이 정하되 영업비밀이 충분히 보호될 수 있도록 운영하여야 한다.
⑤ 다른 부서 또는 외부 기관으로부터 접수한 영업비밀은 원 발신 부서 또는 발신기관의 승인 없이 다시 다른 외부로 발송할 수 없다. 다만, 영업비밀을 이첩・시달하는 경우는 그러하지 아니하다.
⑥ 영업비밀의 접수・발송 업무에 종사하는 사람은 2급 이상의 사내 비밀취급 인가를 받은 사람이어야 한다.

**제35조(전자적 수단에 의한 비밀문서의 관리)**
① 회사는 영업비밀을 전자적 수단으로 생성할 경우, 예고문을 파일 메타데이터에 입력하여 열람 또는 출력 시 해당 비밀등급이 화면 또는 출력물 상에 자동 표시되도록 설정하여야 한다.
② 회사는 영업비밀을 전자적 수단으로 생성, 보관, 열람, 인쇄, 송수신 또는 이관하는 경우, 관련 행위에 대한 기록(로그)이 자동으로 저장 및 유지되도록 시스템을 운영하여야 하며, 송수신 또는 이관 시에는 전자적으로 생성된 접수증 또는 전송 확인서를 사용하여야 한다.
③ 회사는 영업비밀을 전자적으로 생성한 후에는, 업무 목적상 불필요한 경우 해당 내용이 저장된 컴퓨터에서 즉시 삭제하여야 한다. 다만, 업무 수행상 필요한 경우에는 사내 승인된 보안 USB, 암호화 저장장치 또는 내부 지정 저장소(보안서버 등)에 보관할 수 있으며, 이 경우 반드시 암호화 처리 또는 접근권한 통제조치를 함께 취하여야 한다.
④ 회사는 일부 문서에 한하여 문서 중앙화 시스템을 운영한다.
1. 문서중앙화 적용 대상은 다음 각호 중 하나 이상에 해당하는 것으로 한다.
가. 보안등급 1급으로 분류된 문서
나. 외부 반출 가능성이 있거나 사내 협업 대상이 되는 중요 문서
다. 보안담당관이 별도로 지정한 문서
2. 문서 중앙화 시스템에는 다음의 기능이 별도로 포함되어야 한다.
가. 문서는 중앙 서버 내에서만 작성·보관되도록 하며 개인 pc에 저장하는 것을 제한한다.
나. 문서는 저장 시 자동 암호화되며, 열람 시에도  복호화 권한이 부여된 사용자만 접근 가능하다

**제36조 (복제・복사의 제한 표시)**

| |
|---|
| 이 비밀의　　는 생산기관장의 허가없이 복제・복사할 수 없음 |

2급비밀 및 3급비밀의 복제・복사를 제한하려는 때에는 그 영업비밀의 표지 뒷면 또는 예

고문 위에 다음과 같이 붉은색으로 기입한다.

**제37조(파기)**

① 영업비밀을 파기할 때에는 파쇄, 용해 그 밖의 방법으로 원형을 완전히 소멸시켜야 한다.
② 영업비밀을 파기할 때에는 보관책임자 또는 그가 지정하는 비밀취급 인가자가 참여한 가운데 그 영업비밀의 처리담당자가 행하며, 비밀관리기록부의 확인란에 참여자의 파기 확인을 받아야 한다.
③ 영업비밀을 저장·관리하였던 USB 등 **전자기록매체**는 보관책임자가 그 비밀의 내용을 복구할 수 없도록 완전 삭제한 후 파기하여야 한다. 다만, 보조기억매체를 비밀보관용으로 재활용할 경우에는 보안담당관의 승인을 받은 후 사용하여야 한다.

**제38조(일반문서 및 중요 정책자료 보안대책)**

① 일반문서라도 외부 유출 시 기업에 불이익을 초래할 수 있는 경우, 보안등급 분류 기준에 따라 관리하고 사내 문서관리 원칙에 포함하여야 한다.
② 회의자료 및 정책보고서는 다음 각 호에 따라 보안 조치를 적용한다.
1. 작성 단계에서 보안 등급을 표시한다.
2. 사내 문서유통 시스템에 등록하고, 자동 이력기록 기능을 활성화한다.
3. 회의 종료 후 회수한다.
③ 비밀(대외비) 정책 또는 사업의 추진을 위하여 관계자 회의 등을 여는 기관(부서)의 장은 참여자에 대하여 사전에 보안준수사항을 알린 후 서약을 집행해야 한다.

**제39조(국회, 언론, 외부기관 등 대외 자료제공 시 보안대책)**

① 국회, 언론, 정부기관 등 외부기관 제출용 문서 중 영업비밀이 포함될 가능성이 있는 경우, 보안심의위원회의 사전 심의를 받아야 한다.
② 비밀자료는 직접 휴대하여 열람시킨 후 회수하는 것이 원칙이며, 부득이하게 제공해야 하는 경우 다음 각 호의 조건을 충족하여야 한다.
1. 적정등급으로 분류하여 경고문 및 반납일자 등을 명기하여 최소 부수만 제공한다.
2. 전자 문서 형태로 제공할 경우 PDF 보안 설정, 복사·인쇄 제한 등 보안 포맷으로 변환해야 하며, 내부 시스템을 통해 열람 전용으로 제공한다.
3. 자료 제공부서는 회수·파기 등의 보안조치를 하여야 한다.
4. 문서 제공 이력을 기록하고, 최소 3년간 보관한다.
③ 사내 보안부서는 외부 문서 제출 이력을 주기적으로 검토하고, 제공 리스크가 발견될 경우 즉시 보고 및 재평가를 실시한다.

## 제7장(물리보안)

**제40조(적용범위)**
이 장은 회사의 모든 보호구역, 중요시설, 정보보유설비 및 장비, 정보처리 매체 등에 적용하며, 영업비밀을 취급하거나 저장하는 모든 공간과 장비가 대상이다.

**제41조(보호구역의 설정)**
회사는 반도체 기술 및 설비 관련 영업비밀의 보호를 위하여 다음 각 호에 해당하는 장소를 보호구역으로 설정할 수 있다.
1. 통합비밀보관실
2. 암호자재 보관실 또는 암호화 전용장비실
3. 공정운영 통제실 또는 생산설비 중앙제어실
4. 생산상황 종합관제실
5. 통신장비실 또는 네트워크 운영실
6. 전산실, 서버실 또는 데이터센터
7. 반도체 제조설비 구역 또는 기술보안이 요구되는 공정구역
8. 장비 보관소, 정밀 분석실 등 제한이 필요한 특수 기술처리실
9. 그 밖에 보안상 특별한 통제가 요구되는 지역 또는 시설

**제42조(보호구역의 설정)**
① 회사는 보호구역을 다음 각 호와 같이 구분하며, 보호구역의 중요도에 따라 접근 제한 기준을 달리 정한다.

1. 제한지역: 사옥 외곽, 로비, 안내데스크, 주차장 등 외부인의 접근이 가능한 공간으로, 기본적인 감시 및 출입기록 유지를 통해 출입자 식별이 가능한 구역
2. 제한구역:일반 사무공간, 테스트 장비 운영공간 등 일정 수준의 기밀자료가 취급되는 구역으로 직원의 안내가 요구되는 지역
3. 통제구역: 설계자료, 공정정보, 연구개발자료 등 영업비밀을 직접 다루는 보안상 매우 중요한 구역으로, 인가되지 않은 자의 출입이 전면 금지되는 구역

② 회사는 보호구역에 대해 비인가자의 접근이나 출입을 제한하거나 금지할 수 있는 보안대책을 수립·시행하여야 하며, 제한구역 및 통제구역에는 그 구역의 기능 및 구조에 따라 다음 각 호의 대책이 마련되어야 한다.
1. 출입할 수 있는 사람의 지정과 비인가자에 대한 출입 통제대책
2. 주야간 경계대책
3. 외부로부터의 투시, 도청 및 파괴물질의 투척 방지 대책
4. 방화대책 및 경보대책
5. 통제구역입구 CCTV설치 및 감시 대책
6. 그 밖에 필요한 보안대책

③ 제한구역 및 통제구역의 설정은 업무 목적과 보안 필요성에 따라, 가능한 최소한의 범위

로 제한되어야 한다.

**제43조(중요시설 및 설비 정의 및 보호조치)**

① 다음 각 호의 시설 및 설비를 영업비밀 관련 중요시설 및 설비로 정의한다.

1. 반도체 연구개발실, 설계실 등 R&D 공간
2. 서버실, 백업서버 보관실, 전산실
3. 문서 출력기기(복합기, 프린터), 팩스, 외부 저장장치 사용 가능한 설비

② 중요시설 및 설비에는 다음과 같은 보호조치를 시행한다.

1. 고급 출입통제 시스템

가. Anti-Passback 제어 방식에 따라 입실 인증을 받은 사용자만 퇴실 가능하며, 재입실 전 퇴실 인증을 요구한다.

나. 등록된 주인 또는 지정된 관리자가 해당 구역 내에 있을 때만 타인의 출입이 가능하다.

다. 서버 점검실, 보안 유지보수실, 기밀 출력실 등 단시간 접근이 위험한 구역에서는 출입 후 일정 시간이 지나야 퇴실할 수 있도록 제한한다.

라. 중요시설 및 설비 구역에  2개 이상의 출입문(이중문)이 있는 경우, 하나의 문이 닫히기 전에는 다른 문이 열리지 않도록 설계된 출입통제 시스템을 적용한다.

2. 출입자수 제한

가. 최소인원 차단: 일정 인원 이하로는 출입이 제한되어 지정된 인원 이상이 모여야 출입 허용

나. 최대인원 제한: 지정된 출입구역 내 동시 입실 인원을 초과할 경우 출입 차단

3. 외부저장장치(USB 등) 연결 차단 및 제어
4. 백신 및 보안 프로그램 상시 가동
5. 통제구역 입구 및 내부 주요지점에 고해상도 CCTV 설치 및 24시간 영상 감시 체계 구축

**제44조(화재, 정전, 재해 발생 등에 대비한 중요 장비 보호조치)**

① 화재, 정전, 천재지변 등 비상상황 시에도 영업비밀이 안전하게 보호되도록 다음과 같은 조치를 마련한다.

1. UPS 등 무정전 전원장치 설치
2. 내화·내진 기능의 금고 및 문서 보관함 사용
3. 화재감지기, 경보장치, 소화기 등의 필수 보안설비 구축
4. 비상대응 매뉴얼 정비 및 정기적인 훈련 시행

**제45조(중요자재의 반출입 관리)**

① 전자저장매체 및 출력물 반출입 시 다음과 같은 보안장비를 활용하여 통제한다.

1. 스피드게이트: 출입 통제 및 출입자 인가 확인
2. 금속탐지기: USB, 저장매체 등 탐지 (문형, 휴대형 병행)
3. X-ray 검색대: 가방, 물품 내 은닉 장비 탐지
4. 바디스캐너: 인체 은닉 여부 탐지

② 중요자재 반출입은 보안담당자의 승인 하에 가능하며, 반출입기록은 시스템에 등록하고 최소 1년간 보관한다.

**제46조(물품, 정보의 반입, 반출)**

① 회사의 자산 및 물품을 반입·반출하는 임직원은 관리보안담당관 또는 관련부서 선임의 사전승인을 얻어야 한다.

② 컴퓨터 등 정보처리장치(휴대용을 포함하며, 이하 '컴퓨터'라 한다) 및 USB메모리, 외장 HDD 등 전자기록매체(이하 '전자기록매체'라 한다) 등을 사용하고자 하는 임직원은 사전에 정보보안담당관 또는 담당선임의 승인을 얻어야 하며, 회사의 업무를 위해서만 사용하여야 한다.

③ 컴퓨터 또는 전자기록매체를 반입·반출하는 경우, 이를 사용하는 사용자는 관련 규정에 따라 반입·반출일자, 기기사양, 사용용도, 사용자 정보 등을 작성하여 담당 선임에게 제출하고, 담당 선임은 이를 직접 확인한 이후 사용자가 제출한 서류를 정보보안담당관에게 제출하여야 한다.

# 제8장(연구개발 보안에 관한 규정)

**제46조(연구개발 정보보호)**

① 연구개발 관련 정보는 회사의 핵심 영업비밀로 간주하며, 다음 각 호의 보안조치를 시행한다.

1. 연구기획, 설계, 개발, 시험 등 각 단계별 산출물은 보안등급을 지정하고 해당 등급에 따라 보관한다.
2. 연구성과물(설계도면, 시제품, 보고서 등)은 인가된 인원 외 접근을 제한하며, 보안함 또는 서버에 암호화 저장한다.
3. 외부와의 공동연구 시 비밀유지계약(NDA)을 필수로 체결하며, 기술자료 반출 시 사전 승인 절차를 거친다.
4. 해외 전시, 학회 발표, 특허출원 전에는 반드시 사내 보안심의 절차를 진행해야 한다.

**제47조(연구과제의 분류 및 보안과제 선정기준)**

① 연구개발 과제는 보안 필요 수준에 따라 다음 각 호와 같이 분류한다.

1. 보안과제란 수행 성과가 외부에 유출될 경우 기술적 또는 사업적 손실이 발생할  우려가 있어 일정 수준의 보안조치와 접근통제가 요구되는 과제를 의미한다.
2. 일반과제란 보안과제로 지정되지 않은 일반 연구개발 과제를 의미한다.

② 보안과제의 선정 기준은 다음과 같다.

1. 특허 또는 지식재산권 확보와 직결되며, 핵심기술 유출 가능성이 존재하는 연구과제

2. 글로벌 최고 수준의 기술력 확보 또는 초격차 제품 개발에 직결되는 연구과제
3. 외산 의존도가 높아 국산화가 추진 중이거나, 향후 기술적·경제적 가치와 사업 성장성이 높은 기술 분야로서 보호 필요성이 인정되는 연구과제
4. 기술 이전 또는 수출이 제한되거나, 국가 안보 관련 기술로 전용 가능성이 있는 연구과제
5. 시험, 평가, 시제품 개발 등 사업수행 과정과 그 결과에 대해 비공개 관리가 요구되는 연구과제

**48조(연구과제 산출물의 보안등급 분류 및 관리)**
① 연구개발 과제 수행 중 생성되는 모든 문서 및 자료는 기술적 중요도, 기밀성, 유출 시 파급효과 등을 고려하여 보안등급을 지정하고, 등급에 따라 구분·관리하여야 한다

1. 1급 자료
다음 각 목 중 하나 이상에 해당하는 경우로, 유출 시 회사의 핵심 기술 보호, 특허 전략, 경쟁우위에 중대한 영향을 줄 수 있는 자료
가. 특허 출원 전 단계의 발명 설계서, 핵심 기술 개념 요약서
나. 반도체 설계자료, 공정조건서, 회로 설계 파일, GDS, Layout 등
다. 전략기술과 관련된 연구성과 요약보고서 중 공개 시 경쟁사 추적 가능성이 있는 산출물
라. 법령상 보호대상에 해당하는 국가핵심기술 또는 수출 제한 기술자료

2. 2급 자료
다음 각 목 중 하나 이상에 해당하는 경우로, 외부에 공개될 경우 사업상 경쟁력 저하 또는 고객·협력사와의 신뢰도 훼손이 우려되는 자료

가. 공정시험 결과, 성능 평가 결과, 시제품 관련 분석자료
나. 고객사 요구사양이 포함된 시험자료 또는 수탁개발 결과보고서
다. 중간보고서, 기술 검토자료, 공정 개선안 등 내부 기술자료

3. 3급 자료
다음 각 목 중 하나 이상에 해당하는 경우로, 내부 관리 필요는 있으나 외부 유출 시 피해
가. 실험노트, 연구일지, 내부 회의용 초안
나. NDA에 따라 외부 제출된 기술설명서 또는 발표자료
다. 기술보고서 초안, 외부 검토 전의 사내 작성 자료

② 보안등급별 연구과제 산출물 보호조치는 다음 각 호와 같다.

1. 1급 자료의 보호조치
가. 해당 문서는 전용 보안서버 또는 이중 잠금장치가 있는 보안구역 내에 암호화하여 저장하여야 한다.
나. 접근은 제1급 비밀취급 인가를 받은 인원에 한하며, 접근기록은 전자적으로 자동 저장하

고 6개월 이상 보관하여야 한다.
다. 출력은 사전 승인 하에 가능하며, 출력물에는 보안등급, 문서번호, 작성자를 명시하고, 지정된 보관함에 보관하여야 한다.
라. 외부 반출은 원칙적으로 금지하며, 부득이한 경우 보안책임자의 사전 서면 승인을 받은 후 암호화 조치하여 제한적으로 허용할 수 있다.

2. 2급 자료의 보호조치
가. 해당 문서는 부서 전용 보안서버 또는 잠금장치가 있는 보관함에 저장하여야 한다.
나. 접근은 지정된 인가자에 한하며, 접근기록은 시스템 로그 또는 별도 대장을 통해 1개월
다. 출력물에는 보안등급을 표기하고, 출력 이력을 관리하여야 하며, 출력물은 잠금장치가 있는 공간에 보관하여야 한다.
라. 외부 반출은 과제 책임자 및 보안담당자의 사전 승인 후 가능하며, 전송 시 암호화 또는 보안포맷(PDF, 워터마크 등)을 적용하여야 한다.

3. 3급 자료의 보호조치
가. 해당 문서는 일반 보안서버 또는 잠금장치가 있는 보관함에 저장할 수 있으며, 로컬 저장 시 비인가자 접근 차단 조치를 하여야 한다.
나. 접근은 인가된 인력 범위 내에서 공유할 수 있으며, 인원 변경 시 접근 권한을 즉시 조정하여야 한다.
다. 출력물에는 보안등급을 명시하고, 출력 전후의 이력은 필요 시에 한하여 기록한다.
라. 외부 반출은 부서장의 사전 승인을 받은 후 가능하며, NDA 체결 여부 확인과 함께 비밀번호 설정 또는 열람 제한 조치를 취하여야 한다.

③ 보안등급 지정은 과제 착수 시 책임자가 분류하며, 필요 시 보안관리 담당자의 검토를 거쳐 조정할 수 있다.
④ 본 연구과제 산출물 보안등급 분류는 회사 전체 영업비밀 등급 분류체계와는 별도로 독립적으로 운영되며, 다만, 특정 산출물이 영업비밀로도 지정된 경우에는 해당하는 모든 보호조치를 취해야 한다.

# 제9장 정보(통신)보안

**제49조(정보통신보안 관리)**
① 회사는 정보시스템, 통신수단, 저장매체 등을 통한 영업비밀의 유출을 방지하고, 정보자산의 기밀성·무결성·가용성을 확보하기 위하여 별도의 「정보(통신)보안 규정」을 제정·운영한다.
② 「정보(통신)보안 규정」에는 다음 각 호의 사항을 포함하여야 한다.
1. 정보시스템 보호에 관한 관리방법과 보호대책

2. 해킹, 악성코드, 이메일, 노트북, USB·외장하드 등 저장장치의 사용 및 반출입 보안대책
3. 정보통신망법, 정보보안 관련 법령상의 유의사항 및 관련 지침 사항
③ 정보(통신)보안 규정의 제정, 개정 및 시행은 보안심의위원회의 심의를 거쳐 대표이사의 승인을 받아야 한다.
④ 임직원은 정보(통신)보안 규정 및 관련 지침을 준수하여야 하며, 위반 시 회사는 인사규정에 따라 필요한 조치를 취할 수 있다.

## 제10장 보안감사 및 보안점검

**제50조(보안감사의 정의 및 종류)**
① "보안감사"란 회사의 보안정책, 절차, 기준 및 실행 상태의 적정성과 효과성을 확인하기 위한 활동을 말한다.
② 보안감사는 다음 각 호로 구분한다.
1. 정기 보안감사: 연 1회 이상 전사적 차원에서 실시하는 계획적 감사
2. 수시 보안점검: 보안사고 발생, 내부 신고, 외부 감사 대응 시 등 필요에 따라 실시
3. 특별 감사: 고위험 부서, 주요기술 보유부서 또는 신규 사업부 등 특정 대상에 대한 집중 감사

**제51조(감사 대상 및 항목)**
① 보안감사의 주요 대상은 다음과 같다.
1. 정보시스템 및 네트워크 접근 관리 현황
2. 영업비밀 보호 대상 자료 및 문서 관리 상태
3. 출입통제 및 물리보안 이행 여부
4. 보안 교육 및 사용자 인식 수준
5. 보안사고 대응 체계 및 이력
② 감사 항목은『보안감사 체크리스트』(별표 2)에 따라 사전에 정의하고, 관련 문서 및 시스템 로그 등 근거자료를 기반으로 검토한다.

**제52조(감사 수행 및 권한)**
① 보안감사는 보안담당부서 또는 보안심의위원회가 지정한 전담 인력이 수행하며, 필요 시 외부 전문기관에 위탁할 수 있다.
② 감사 수행자는 감사 목적 달성을 위해 관련 부서에 자료 제출, 인터뷰, 시스템 점검을 요구할 수 있으며, 해당 부서는 이에 성실히 협조하여야 한다.

**제53조(감사 결과 및 후속조치)**
① 보안감사 결과는 감사 종료 후 10영업일 이내에 『보안감사보고서』로 작성하여 보안심의위원회에 보고한다.
② 감사 결과 확인된 보안 미비 사항에 대해서는 시정조치계획을 수립하고, 지정기한 내 이행하여야 한다.
③ 보안담당부서는 시정조치 이행 여부를 모니터링하고, 완료 결과를 기록·보관하여야 한다.

**제54조(자체 점검 체계 운영)**
① 각 부서장은 월 1회 이상 부서 내 보안관리 실태를 자체 점검하고, 점검 결과를 보안담당부서에 보고하여야 한다.
② 자체 점검은 『부서 보안 점검표』에 따라 실시하며, 반복 위반 또는 고위험 항목 발견 시 보안담당부서는 즉시 조치할 수 있다.
③ 자체 점검 결과 고위험 항목이 발견된 경우, 보안담당부서는 해당 부서에 신속한 시정조치를 요구하며, 해당 부서는 정해진 기한 내 시정조치 결과를 제출하여야 한다. 시정조치 미이행 시 보안심의위원회에 보고하여 추가 조치를 논의할 수 있다.

**제55조(외부 감사 대응)**
① 정부기관, 감사원, 감사법인 등 외부기관의 정보보호 관련 감사 요청이 있는 경우, 보안담당부서는 신속하게 대응 체계를 구성한다.
② 외부 감사 대응 결과 및 후속 조치는 내부 감사 절차에 준하여 처리한다.

## 제11장 영업비밀 침해사고 대응

**제3조(침해사고의 정의)**
다음 각 호 중 하나에 해당하는 경우 영업비밀 침해사고로 간주한다.
1. 반도체 제조 공정, 설계, 테스트 등 기술정보의 외부 유출 또는 유출을 시도하는 행위
2. 내부자에 의한 무단 복사, 반출, 저장매체 전송 등 유사 행위
3. 외부 사이버 공격(해킹, 랜섬웨어 등)에 의한 정보탈취 시도
4. 전자기록매체를 통한 비인가 정보 저장 및 반출
5. 퇴직(예정)자의 정보 유출 정황 확인 시
6. 당사의 생성형 인공지능(AI)을 통해 생성된 사내 기밀 정보를 외부 AI 학습 데이터로 활용하거나, 사내 시스템 외부로 유출 또는 유출을 시도하는 행위
7. 기타 회사의 영업비밀을 외부로 유출하거나 유출을 시도하는 행위

**제57조(초동대응 및 통보)**
① 침해사고 또는 그 징후를 인지한 자는 즉시 구두 및 전자문서 방식으로 담당 보안담당관에게 보고하여야 하며, 최초 인지 시점으로부터 1시간 이내 보고를 원칙으로 한다.
② 담당 보안담당관은 즉시 '영업비밀 사고 대응팀(이하 대응팀이라고 한다.)'을 소집하고, 초동대응을 지시한다.
③ 초동대응에는 다음 각 호의 조치가 포함된다.
1. 가시적 증거(메일, 로그기록, CCTV 등) 확보
2. 관련 장비 격리 및 사용자 일시 업무정지 조치
3. 2차 피해 방지를 위한 네트워크 차단 및 접근권한 회수
4. 디지털 포렌식 조사 착수: 침해 관련 로그, 장비 내 메타데이터, AI 사용 이력을 포함하여 모든 기록 확보 및 분석
5. 생성형 AI 도구에 입력된 정보 추적 여부 및 로그 삭제 여부 확인

**제58조(대응팀 구성 및 역할)**
① 대응팀은 관리보안담당관을 팀장으로 하며, 정보보안담당관, IT보안팀, 법무팀, 인사팀, 관련 부서장 등으로 구성한다.
② 대응팀은 필요 시 외부 디지털포렌식 전문가, 법률자문, 정부기관과의 협업도 병행한다.
③ 대응팀의 임무는 다음과 같다.
1. 사고 경위 및 유출 범위 조사
2. 사고 유형별 원인분석 및 자료 회수
3. 보안 위반자 또는 책임자에 대한 사실 확인 및 보고
4. 유관기관(산업부, 경찰, KISA 등)에 법적 절차에 따른 신고 진행

**제59조(사후조치 및 재발방지)**
① 사고조사 종료 후 5영업일 이내에 '침해사고 결과 보고서'를 작성하여 정보보호 최고책임자 및 영업비밀 보안심의위원회에 보고한다.
② 위반자에 대해서는 인사규정에 따라 징계 절차를 개시하며, 고의성 판단 시 형사고발을 포함한 법적 조치를 병행할 수 있다.
③ 해당 사고는 유사 사례 재발방지를 위한 내부 보안교육 콘텐츠로 가공·활용할 수 있다. 단, 당사자 식별정보는 비식별화 처리한다.

## 제12장 보안교육 및 홍보

**제60조(보안교육 시기 및 대상)**

1. 신규 입사자: 입사 3일 이내 보안 입문교육(오프라인 필수)
2. 재직 임직원: 연 2회 이상 정기 보안교육 및 퀴즈(온라인+오프라인 병행)
3. 고위험 부서 구성원: 분기 1회 심화교육
가. R&D: 설계자료, 공정정보 보호 및 보안툴 활용 실습
나. 생산기술팀: 공정 로그 유출 사례 및 설비망 보안
다. AI 개발팀: AI 학습 시 보안 리스크 및 데이터 사전 필터링 가이드, 생성형 AI 사용 금지 지침 및 예외 기준 안내
라. 마케팅/기획팀: 외부 커뮤니케이션 및 생성형 콘텐츠 활용 시의 보안 유의사항 교육
마. 인사/총무팀: 개인정보 포함 문서의 AI 입력 방지, 출력물 관리 주의사항
4. 협력업체 및 외주인력: 계약 체결 전 보안교육 이수 확인
5. 퇴직(예정)자: 퇴사 1주 전 별도 보안 퇴직자 교육 필수

**제61조(보안교육 내용)**
1. 영업비밀 관련 법령 및 규정(부정경쟁방지법 등)
2. 산업기술유출 사례 분석 및 대응 시뮬레이션
3. AI·클라우드 등 최신 기술환경에서의 보안 리스크 인식
4. 사내 허용 AI 사용 범위, 외부 AI 입력 시 금지 데이터 유형 및 안전한 사용 매뉴얼 숙지
5. 생성형 AI 및 내부 AI 서비스 사용 시 보안 수칙과 승인 절차 안내
6. 문서보안, 접근통제, 이메일 보안 등 실무 가이드라인
7. 비상 대응 연락망 및 사고보고 절차 교육

**제62조(보안홍보 및 캠페인 활동)**
사내 보안 인식 강화를 위해 다음 각 호의 홍보활동을 수행한다.
1. 월간 보안 뉴스레터 발행 및 이메일 배포
2. 사내 보안 포스터·표어·슬로건 경진대회 연 1회 실시
3. '보안 아이디어 공모전' 개최 (포스터, 카드뉴스, 영상 등 자유 형식)
가. 우수작 시상 및 주요 장소 게시
나. 인트라넷, 사내 TV, 엘리베이터 내 화면 등 다채널 활용
4. 매월 '보안의 날' 운영 (강연, 보안 퀴즈, 해킹 시뮬레이션 체험 등 포함)
5. 보안 캐릭터 'Chippo(별표 3)' 및 사내 마스코트를 활용한 콘텐츠 제작 및 배포
가. 캐릭터 Chippo(Chip + Protect)는 반도체 정보보안 수호자를 모티브로 한 사내 마스코트로, 보안 포스터, 캠페인 영상, 퀴즈 이벤트 등에 활용함
나. 구성원의 보안 인식 제고와 흥미 유발을 위한 콘텐츠 제작 가능
다. 마스코트 활용 범위와 콘텐츠 종류는 정보보안팀이 기획 및 관리함.

**제63조(이수관리 및 효과측정)**
① 모든 교육은 이수자 명부와 이수확인서를 정보보안팀에서 관리한다.
② 미이수자는 자동 알림 후 7일 내 보완교육을 이수해야 하며, 반복 시 관리자에게

통보된다.
③ 교육 효과성 평가는 퀴즈 점수, 만족도 조사, 이해도 테스트 등을 활용하여 분기별 분석한다.
④ 분석 결과는 차기 교육 프로그램 기획 및 부서별 맞춤형 교육 설계에 반영한다.

## 제13장 보칙

**제64조 (교육)**
① 보안담당관은 전체 임직원에 대해 정기적으로 영업비밀 및 사이버 레질리언스 관련 교육을 실시하여야 한다.
② 영업비밀 교육은 외부에 위탁하여 실시할 수 있다.
③ 사이버 레질리언스 교육은 침해 사고 대응, 위기 복구 계획, 위협 감지 및 대응 프로세스를 포함하여야 한다.

## 부칙

1. 이 규정은 2025년 4월 18일부터 시행한다.
2. 이 규정 시행 전부터 보유하고 있는 영업비밀 중 주요 영업비밀에 대해서는 규정시행 후 1개월 이내에 등급분류(재분류)를 하여 등급을 지정(재지정)한다.

1. '1급 비밀'을 기록한 문서, 도면, 사진, 서적, 자기 테이프, FD, CD, 컴퓨터 서버 등 (이하 '기록매체')의 보관, 열람, 복제, 반출, 파기, 망분리 정책은 다음과 같다.

**가. 보관**

- 기록매체는 별도의 영업비밀 보관대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 시건 장치가 있는 보관함에 엄중히 보관해야 한다. 이 때 열쇠 등은 보관책임자가 보관한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 정보시스템 기기를 통제 구역 내에 설치한다. 만일 해당 정보시스템 기기를 통제구역 내에 설치할 수 없는 경우에는 보관책임자는 타인의 접근을 방지하기 위한 최선의 보안조치를 취하여야 한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부 기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 보관책임자가 보관한다.

- 보관 시설 출입 시 이중 인증을 요구하고, 보안 감시 장치를 활용하여 접근을 기록해야 한다.
- 보관 위치는 정기적으로 점검하며, 보관책임자는 보안점검 기록을 유지해야 한다.

**나. 열람**

- 해당 정보에 접근이 허락되지 않은 자는 기록매체를 열람할 수 없다.
- 기록매체는 상당한 필요성이 인정되는 경우 보관책임자 승인 후 보관책임자의 입회하에 열람할 수 있다.
- 보관책임자는 별도의 영업비밀 열람대장에 열람자명, 일시 등을 기록한다.
- 전자화된 정보의 화면 표시는 입실이 제한되고 해당 정보의 보유자가 실재하는 장소에서 타인에게 보이지 않도록 각별한 주의를 기울이며 실시되어야 한다.
- 열람자는 노트, 필기구, 촬영 장비 등의 반입을 금지하며, 사전에 승인된 경우에 한하여 제한적으로 사용할 수 있다.
- 모든 열람 기록은 주기적으로 점검되며, 이상 징후 발견 시 즉시 대응 조치를 취해야 한다.
- 열람이 허용된 공간은 CCTV 등 감시 시스템을 활용하여 높은 보안 수준을 유지한다.
- 보관책임자는 모든 열람 기록을 주기적으로 점검해야 한다.

**다. 복제**

- 보관책임자의 허가 없이 기록매체를 복제할 수 없다.
- 복제물은 원본과 동일한 방식으로 취급되며, '1급 비밀'로 분류하여 별도로 관리해야 한다.
- 전자화된 정보의 복제는 보관책임자만이 실시할 수 있다.
- 보관책임자는 복제자명, 일시, 목적 등을 별도의 영업비밀 복제대장에 기록해야 한다.
- 복제 시 무단 유출 방지를 위해 보안 라벨을 부착하며, 복제본의 유통 이력을 철저히 관리해야 한다.
- 복제된 기록매체는 암호화 및 보안 조치를 취한 후 보관해야 한다.
- 복제된 기록매체는 시건 장치가 있는 보관함에 보관해야 하며, 열쇠 등은 보안담당관이 보관한다.
- 보관책임자는 모든 복제 기록을 주기적으로 점검해야 한다.

**라. 반출**

- 보안담당관의 허가 없이 기록매체를 반출할 수 없다.
- 보안담당관은 반출자명, 일시, 목적, 반환 시기 등을 별도의 영업비밀 반출대장에 기록해야 한다.
- 반출 시 보안 밀봉 장치 또는 지정된 보안 가방을 사용해야 하며, 이동 중 외부인이 접근하지 못하도록 조치해야 한다.
- 보관책임자의 허가가 있을 경우에도 허가를 받은 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 반출된 정보는 사전 승인된 장소에서만 사용 가능하며, 외부 네트워크 연결은 제한된다.
- 반출 후 지정된 시간 내에 반입해야 하며, 지연될 경우 즉시 보관책임자에게 보고해야 한다.
- 보관책임자는 모든 반출 기록을 주기적으로 점검해야 한다.

**마. 파기**

- 기록매체는 사용 후 보관책임자의 감독 하에 적절한 방법에 의해 파기하도록 한다.
- 전자화된 정보는 보관책임자의 승인을 얻어 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 파기하도록 한다.
- 보관책임자는 별도의 영업비밀 파기대장에 파기 일시 및 등을 기록해야 한다.
- 기록매체 파기 후, 보관책임자는 파기증명서를 작성하여 보관해야 한다.
- 보관책임자는 모든 파기 기록을 주기적으로 점검해야 한다.

**바. 망분리 완화**

- 급 비밀 정보는 망분리 완화가 절대 불가하며, 외부 시스템과의 연결은 원칙적으로 차단된다.
- 1급 비밀 정보를 다루는 시스템은 외부 네트워크와 물리적/논리적으로 완전 분리되며, 이를 위한 망분리가 반드시 유지되어야 한다.
- 내부망 내에서도 데이터 전송 시 암호화 및 접근 통제를 강화하여 보안 조치를 이행해야 한다.
- 모든 내부 전송 및 저장되는 정보는 AES-256 이상의 최고 수준의 암호화가 적용되어야 하며, 관리자는 암호화 키를 철저히 관리해야 한다.
- 외부 네트워크와 연결된 기기는 1급 비밀 정보와 관련된 작업을 처리할 수 없으며, 내부망에서의 정보 유출을 방지하기 위한 고강도의 보안 조치가 이루어져야 한다.
- 보안담당자에 의해 승인되지 않은 저장 장치(USB, 외장하드 등)의 사용을 엄격히 금지한다.
- 모든 연결과 정보 전송 기록을 실시간 모니터링하며, 비정상적인 접근은 즉시 차단 및 보고되어야 한다.
- 네트워크 보안 점검을 정기적으로 수행하며, 의심스러운 접근기록이 발견될 경우 즉시 조치해야 한다.

2. '2급 비밀' 기록매체의 보관, 열람, 복제, 반출, 파기, 망분리 정책은 다음과 같다.

**가. 보관**

- 기록매체는 영업비밀 통합 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별 하여 시건 장치가 있는 보관함에 엄중히 보관해야 한다. 이 때 열쇠 등은 분임 보관책임자가 보관한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 및 접근 제어 등의 적절한 조치를 취하고 해당 정보시스템 기기를 통제 구역 내에 설치한다. 만일 해당 정보시스템 기기를 통제 구역 내에 설치할 수 없는 경우에는 주책임자는 보관책임자의 감독하에 타인의 접근을 방지하기 위한 최선의 보안조치를 취하여야 한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 및 접근 제어 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이때 열쇠 등은 주책임자가 보관한다.

**나. 열람**

- 기록매체는 필요성이 인정되는 경우 분임 보관책임자 승인 후 영업비밀 보관책임자의 입하하에 열람할 수 있다.

- 열람 공간은 승인된 장소에서만 가능하며, 열람자는 보안 규정을 준수해야 한다.
- 전자화된 정보의 화면 표시는 타인에게 보이지 않도록 주의를 기울이며 실시되어야 한다.
- 주책임자는 영업비밀 통합 관리대장에 열람자명, 일시 등을 기록해야 한다..
- 외부 시스템과 연결 시 접근 통제, 암호화 등의 보안 조치를 적용해야 한다.
- 주책임자는 모든 열람 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**다. 복제**

- 기록매체는 중대한 필요성이 인정되는 경우 주책임자의 승인 하에 복제하는 것이 가능하다. 단, 복제물은 원본과 동등하게 '2급 비밀'로 취급해야 한다.
- 복제된 기록매체는 암호화 및 보안 조치를 취한 후 보관해야 한다.
- 전자화된 정보의 복제는 주책임자의 승인을 얻어 승인된 보안 시스템에서 배부받은 자의 책임 하에 실시할 수 있다.
- 주책임자는 영업비밀 통합 관리대장에 복제자명, 일시, 목적 등을 기록해야 한다.
- 복제물은 별도의 보안 라벨을 부착하여 무단 유출을 방지해야 한다.
- 주책임자는 모든 복제 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**라. 반출**

- 업무상 필요성이 인정되는 경우에만 기록매체를 반출할 수 있다.
- 이 경우 기록매체를 반출한 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 반출 시 보안 가방 또는 봉인 장치를 사용하여 유출을 방지해야 한다.
- 주책임자는 영업비밀 통합 관리대장에 반출자명, 일시, 목적, 반환시기 등을 기록해야 한다.
- 주책임자는 모든 반출 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**라. 파기**

- 기록매체는 사용 후 분임 보관책임자의 감독하에 적절한 방법을 통해 파기하도록 한다.
- 전자화된 정보는 주책임자의 승인을 얻어 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 파기하도록 한다.
- 주책임자는 영업비밀 통합 관리대장에 파기 일시 및 등을 기록해야 한다.
- 주책임자는 모든 파기 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.
- 주책임자는 파기 증명서를 작성하여 보관한다.

**마. 망분리 완화**

- 2급 비밀 정보는 망분리 완화가 절대 불가하며, 외부 시스템과의 연결은 원칙적으로 차단된다.
- 2급 비밀 정보를 다루는 시스템은 외부 네트워크와 물리적/논리적으로 완전 분리되며, 이를 위한 망분리가 반드시 유지되어야 한다.
- 내부망 내에서도 데이터 전송 시 암호화 및 접근 통제를 강화하여 보안 조치를 이행

해야 한다.

- 모든 내부 전송 및 저장되는 정보는 AES-256 이상의 최고 수준의 암호화가 적용되어야 하며, 관리자는 암호화 키를 철저히 관리해야 한다.
- 외부 네트워크와 연결된 기기는 2급 비밀 정보와 관련된 작업을 처리할 수 없으며, 내부망에서의 정보 유출을 방지하기 위한 고강도의 보안 조치가 이루어져야 한다.
- 보안담당자에 의해 승인되지 않은 저장 장치(USB, 외장하드 등)의 사용을 엄격히 금지한다.
- 모든 연결과 정보 전송 기록을 실시간 모니터링하며, 비정상적인 접근은 즉시 차단 및 보고되어야 한다.
- 네트워크 보안 점검을 정기적으로 수행하며, 의심스러운 접근기록이 발견될 경우 즉시 조치해야 한다.

3. '3급 비밀' 기록매체의 보관, 열람, 복제, 반출, 파기, 망분리 정책은 다음과 같다.

**가. 보관**

- 기록매체는 영업비밀 통합 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 보관해야 한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이때 열쇠 등은 주책임자가 보관한다.
- 보관 위치는 정기적으로 점검되며, 출입 기록 및 보안 감시 장치를 활용하여 접근을 모니터링한다.

**나. 열람**

- 업무상 필요에 의해 기록매체를 열람할 수 있으며, 주책임자의 허가가 있어야 한다.
- 전자화된 정보의 화면 표시는 타인에게 보이지 않도록 주의를 기울이며 실시되어야 한다.
- 주책임자는 영업비밀 통합 관리대장에 열람자명, 일시, 목적 등을 기록해야 한다.
- 주책임자는 모든 열람 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**다. 복제**

- 업무상 필요에 의해 복제가 가능하며, 주책임자의 승인이 필요하다. 복제물은 원본과 동일하게 3급 비밀로 취급된다.
- 전자화된 정보의 복제는 비밀 보관책임자의 승인을 얻어 승인된 보안시스템에서 복제하며, 복제된 기록매체에 대한 관리는 배부 받은 자의 책임이다.
- 주책임자는 영업비밀 통합 관리대장에 복제자명, 일시, 목적 등을 기록해야 한다.
- 복제본에는 보안 라벨을 부착하여 유출을 방지하며, 복제물의 유통 이력을 철저히 관리한다.
- 주책임자는 모든 복제 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**라. 반출**

- 업무상 필요에 의해 기록매체를 반출할 수 있으며, 주책임자의 허가가 필요하다.
- 기록매체를 반출한 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 주책임자는 영업비밀 통합 관리대장에 반출자명, 일시, 목적, 반환시기 등을 기록해야 한다.
- 주책임자는 모든 반출 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**마. 파기**

- 기록매체는 사용 후 주보관책임자의 승인을 받아 기록매체를 배부 받은 자의 책임하에 적절한 방법에 의해 파기하도록 한다.
- 전자화된 정보는 주책임자의 승인을 얻어 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 파기하도록 한다.
- 주책임자는 영업비밀 통합 관리대장에 파기 일시 및 등을 기록해야 하며, 파기 증명서를 작성하여 보관해야 한다.
- 주책임자는 모든 파기 기록을 주기적으로 점검해야 하며, 점검 결과를 보관책임자에게 제출해야 한다.

**바. 망분리 완화**

- 3급 비밀 정보는 망분리 완화가 제한적으로 허용된다.
- 업무상 필요한 경우, 특정 외부 시스템과의 연결이 허용된다. 다만, 외부 시스템과의 연결은 업무에 직접적으로 관련이 있는 경우에만 허용되고, 이 연결은 최소화되어야 한다.
- 외부 시스템과의 연결이나 정보 전송 시, 반드시 암호화가 적용되어야 하며, 최소한 AES-128 이상의 암호화 기술을 사용해야 한다.
- 외부 시스템에 접근할 수 있는 사람은 반드시 승인된 사람만 가능하며, 다단계 인증을 통해 강력한 인증 절차가 요구된다.
- 외부 시스템과의 연결 시에는 반드시 보안 강화 조치가 적용되어야 하며, 암호화 및 접근 통제가 필수적이다.
- 외부망과의 연결을 허용할 수 있지만, 내부망에서 민감한 정보가 포함된 시스템은 외부망과 완전히 분리해야 하며, 연결된 시스템은 별도의 보안망에서 운영된다.
- 외부 네트워크를 사용할 경우, 사용 내역을 로그로 남기고 주기적으로 점검해야 한다.
- 파일 전송 시에는 반드시 암호화된 시스템을 사용해야 하며, USB, 외장하드 등의 외부 저장장치의 사용은 원칙적으로 금지된다. 만약 외부 저장 장치 사용 시에는 보안 담당관에 의해 승인된 장치만 사용 가능하다.

4. '개인정보'의 취급은 다음과 같다.

가. **비밀 등급**

- 종업원, 고객 등의 개인정보는 "1급 기밀"로 취급한다.
- 1급 비밀의 관리 방침에 맞춰, 개인정보의 열람, 복제, 반출, 보관 등이 엄격하게 제한되고, 외부 시스템과의 연결 차단 및 보안 강화를 철저히 해야 한다.

**나. 망분리 완화**

- 개인정보 보호법 등 관련 법규에 따라 개인정보는 반드시 물리적으로 격리된 보안망에서만 처리해야 한다. 외부망과의 연결은 전면 차단되어야 하며, 정보시스템 간의 연결은 최소화해야 한다.
- 개인정보를 포함한 파일에 대해서는 AES-256 등의 암호화를 해야 하며, 접근 시에는 허가받은 자에 대한 다단계 인증이 필요하다.
- 개인정보를 처리하는 시스템은 내부망과 외부망의 완전 분리가 필요하며, 고강도 방화벽, 침입 탐지 시스템 등의 추가적인 보안 장치를 배치해야 한다.
- 로그 기록 및 보안 점검을 주기적으로 수행하며, 비정상적인 접근을 발견할 경우 즉시 차단하고 보고해야 한다.
- 이 모든 사항은 개인정보보호법을 준수하며, 해당 법의 규정에 우선하여 처리해야 한다.

5. '비식별화된 개인정보'의 취급은 다음과 같다.

**가. 비밀 등급**

- 가명정보는 원칙적으로 2급 기밀로 취급한다. 다만, 분석 결과가 개인 또는 기업의 전략에 영향을 줄 수 있는 경우, 혹은 해당 정보의 분석 결과가 개인의 성향, 위치, 소비 특성 등을 유추할 수 있는 경우에는 해당 정보는 1급 기밀로 상향 분류할 수 있다.
- 익명정보는 원칙적으로 3급 기밀로 취급한다. 다만, 정보의 활용 목적, 또는 전략적 가치에 따라 2급 이상 기밀로 상향 분류할 수 있다.
- 가명정보는 원본 개인정보와 분리 저장하고, 추가 정보에 의한 재결합이 불가능하도록 관리한다.
- 그 외의 사항은 해당하는 비밀의 관리 방침에 맞춰, 비식별화된 개인정보의 열람, 복제, 반출, 보관 등이 제한되고, 외부 시스템과의 연결 시 보안 강화를 철저히 해야 한다.

**나. 망분리 완화**

- 익명정보는 해당하는 비밀 등급에 따라 제한적으로 외부 시스템과 연결할 수 있으며, 외부 시스템과의 연결 시에는, 해당하는 비밀 관리 방침에 따른 강화된 보안 조치가 반드시 적용되어야 한다.
- AI 시스템이 3급 비밀에 해당하는 익명정보를 처리할 때는 개인정보보호법에 따라 '통계작성', '과학적 연구', '공익적 기록 보존'을 위해서만 처리 가능하다.
- 3급 비밀에 해당하는 익명정보가 AI 시스템에서 활용되는 경우, 해당 시스템은 보안 등급 기준에 따라 별도의 보안망에서 관리되어야 한다. 또한, 익명정보라도 외부 정보와의 결합 등을 통해 재식별 위험이 발생하지 않도록, AI 분석 및 처리 과정 전반에 걸쳐 철저한 보안관리와 기술적 보호조치가 이행되어야 한다.
- 외부 시스템과 연결되는 경우 각 비밀 등급에 따른 암호화, 접근 제어, 최소 권한 원칙 등을 적용해야 하며, 특히 AI 시스템과의 연결에서는 AI 보안 정책을 준수하고, 개인정보보호법에 따라 추가적인 법적 요구 사항을 충족시켜야 한다.

- 이 모든 사항은 개인정보보호법을 준수하며, 해당 법의 규정에 우선하여 처리해야 한다.

6. 사이버 레질리언스

**가. 침해 사고 대응**

- 보관책임자는 영업비밀 침해 사고 발생 시 즉각적인 탐지 및 대응 절차를 수행하여야 한다.
- 모든 영업비밀 관련 보안 사고는 사고 보고 체계를 통해 신속히 공유되어야 하며, 관련 부서와 협력하여 대응해야 한다.
- 영업비밀 침해 사고 발생 시 IT 보안팀 및 법무팀과 협력하여 추가적인 정보 유출 및 피해를 방지해야 한다.

**나. 복구 계획 수립**

- 회사는 영업비밀 침해 발생 시 신속한 복구를 위한 위기 복구 계획을 수립해야 한다.
- 복구 계획은 최신 보안 위협과 기술 변화를 반영하여 정기적으로 검토 및 업데이트되어야 한다.
- 중요 영업비밀 및 관련 데이터에 대한 보호 및 복구를 위한 백업 정책을 마련하고 주기적으로 점검해야 한다.

**다. 위협 감지 및 대응**

- 회사는 영업비밀 보호를 위해 실시간 위협 감지 시스템을 운영하고, 내부 및 외부 위협을 사전에 예방해야 한다.
- 보안담당관은 정기적으로 영업비밀 관련 사이버 위협을 분석하고 대응 전략을 수립해야 한다.
- 영업비밀 유출 징후가 발견될 경우 즉각적인 차단 및 대응 조치를 수행하며, 필요 시 법적 조치를 검토해야 한다.

[별표1] 영업비밀 자료등급 분류기준

| 자료등급 | 자료구분 | 기획/행정 | 사업 | 기술개발 |
|---|---|---|---|---|
| 1급 | 별도관리자료 | • 경영진의 전략적 의사결정 자료(M&A, 구조조정, 투자 계획)<br>• 공시 전 감사결과, 내외부 리스크 대응 시나리오<br>• 조직개편안 및 임원급 인사이동 계획 | • 고객사별 전략 및 수익모델 설계자료<br>• 최상위 계약조건, 거래단가 내역, 수익기여도 분석<br>• 매출 상위 고객사 이탈 시뮬레이션 자료 | • 특허 출원 관련 핵심 반도체 설계도, 제조공정 조건<br>• 신제품 핵심 알고리즘, 공정 시퀀스 전략<br>• 양산화 미도달 단계의R&D 기술 성과 문서<br>•AI 기반 설계 자동화 |

| | | | | |
|---|---|---|---|---|
| | | | | 툴 개발자료 및 학습 데이터셋 |
| 2급 | 특별보호자료 | • 연간 사업계획, 부문별 예산안<br>• 중간 결산보고서, KPI 실행 계획안<br>• 팀별 평가 기준 및 인력 배치 계획 | • 주요 고객사 대응 전략 및 내부 가격 정책<br>• 협력사 평가자료, 공급망 위험 예측 자료<br>• 시장 점유율 분석 및 경쟁사 동향 정리문서 | • 비핵심 모듈 설계자료, 시제품 시험성적서<br>• 공정개선 회의록, 파일럿 테스트 결과보고<br>• 외부 자문과정에서 사용된 설명자료 |
| 3급 | 일반보호자료 | • 사내 공지사항, 일정표, 일반 회의자료<br>• 사내 복리후생 및 교육 안내문<br>• 일상 운영 매뉴얼 | • 비핵심 고객사 거래이력 정리표<br>• 기존 수주건 사후 보고서<br>• 공개 가능성이 있는 견적요청 회신문서 | • 제품 사양서(카탈로그 수준)<br>• 외부 공유용 교육자료, 학회 발표자료<br>• 설비 운영 일반지침서 |

## [별표 2]「보안감사 체크리스트」제10장 제33조 2항

| 구분 | 감사 영역 | 점검 항목 | 점검 기준 | 확인 방법 | 비고 |
|---|---|---|---|---|---|
| 1 | **정보시스템 보안** | 업무망·인터넷망·OT망의 물리/논리적 분리 상태 | 망 간 불법 연계 차단 여부 | 네트워크 구성도, 장비 설정, 패킷 추적 | |
| 2 | | 정보시스템 접근 권한 관리 | 최소권한 원칙, 계정 만료 설정 | 사용자 권한 목록, 계정 정책 | 인턴/파견직 포함 |
| 3 | | 시스템 접근 로그 보관 및 감사 기능 설정 | 1년 이상 보관, 로그 위변조 방지 | 로그관리 설정, SIEM 연계 여부 | |
| 4 | **영업비밀 보호** | 영업비밀 자료 지정 및 보관 관리 | 사내 등록자료 목록 존재 여부 | 영업비밀 DB, 등급 분류 현황 | |
| 5 | | 기밀자료 외부 전송 시 승인 및 암호화 여부 | 부서장/보안 승인, 암호화 조치 | 전송 기록, 승인 로그 | |
| 6 | **저장매체 보안** | USB 등 저장장치 사용 승인 및 암호화 여부 | 사용신청 및 승인 내역 존재 | 신청서, 장비 암호화 여부 | FAB 내 사용 장비 포함 |
| 7 | | 반출입 기록의 문서화 및 1년 이상 보관 | 반출입 이력 문서화 여부 | 기록지, 보안담당부서 보관 여부 | |
| 8 | **물리적 보안** | FAB/서버실/생산실 보안통제 여부 | 출입통제 시스템 운영 | 출입기록, CCTV, 접근권한 설정 | |
| 9 | | 무선기기 반입 통제 및 RF 감시 운영 | RF 탐지기 운영, 위반 대응 여부 | 탐지 로그, 단속 이력 | |
| 10 | **보안교육 및 인식** | 정기 보안교육 이수 여부 | 연 1회 이상, 이수율 100% | 교육이수 기록, 참석부 | 협력업체 포함 여부 |
| 11 | | 보안사고 시 신고 및 대응 체계 숙지 | 전사 공지/지침 준수 여부 | 사용자 인터뷰, 공지사항 | 내부 신고 제도 확인 |
| 12 | **사고 대응 및 재해복구** | 보안사고 발생 시 대응 절차 존재 여부 | 『정보보안 사고보고서』 작성 체계 | 사례 리뷰, 대응 이력 | 최근 1년 이내 사고 여부 |
| 13 | | FAB 내 공정정보 백업 및 복구 체계 구축 여부 | 주기적 백업, 이중화 시스템 운영 | 백업 스케줄, 복구 테스트 기록 | |
| 14 | **외부 감** | 외부기관 감사 대응 체계 수립 여부 | 보고서 존재 여부 및 대응일정 | 대응 매뉴얼, 실행이력 | 감사 후 재 |

| | | | | | |
|---|---|---|---|---|---|
| | 사 대응 | | 관리 | | 발방지 포함 |

[별표 3] 보안캐릭터 'CHIPPO' - 제12장 제4조 5호


# 「정보(통신)보안 규정」

## 제1장 총칙

**제1조(목적)**

본 규정은 회사의 반도체 설계·공정·장비제어 등 기술 및 생산 관련 핵심 정보와 정보자산 및 통신수단을 통해 처리되는 영업비밀 등 중요 정보의 유출, 변조, 훼손 등을 방지하고, 안전한 정보통신 환경을 조성하기 위한 보안 관리 기준을 정함을 목적으로 한다.

**제2조(적용 범위)**

① 본 규정은 다음 각 호에 해당하는 자 및 자산에 적용된다.

1. 회사의 임직원(정규직, 계약직, 인턴, 파견직 포함)
2. 회사와 계약 관계에 있는 협력업체, 외부 위탁업체, 용역 제공자
3. 회사의 정보시스템에 접속하거나 회사의 정보를 처리하는 모든 사용자

② 적용 대상 자산은 다음 각 호를 포함하며, 이에 국한되지 않는다.

1. 정보시스템(ERP, MES, 이메일, 클라우드 등)
2. 정보통신 인프라(서버, 네트워크 장비, 라우터, 방화벽, 스위치 등)
3. 단말장비(PC, 노트북, 모바일, 태블릿, 공용 단말 등)
4. 저장매체(USB, 외장하드, SD카드, DVD/CD 등 물리 저장매체 포함)
5. 반도체 생산설비에 연결된 시스템, 공정정보 서버, SPC 시스템 등 생산지원 시스템
6. 설비제어망(OT), 생산망, 업무망, 개발망, 시험망 등 모든 전산망

③ 회사의 정보보호 활동은 전사적으로 적용되며, 정보 보유·처리의 전(全) 수명주기(생성, 처리, 저장, 전송, 폐기)에 대해 관리되어야 한다.

**제3조(용어 정의)**

① 본 규정에서 사용하는 용어의 정의는 다음과 같다.

1. 정보자산이란 정보(데이터) 자체와 이를 수집, 처리, 전송, 보관, 폐기, 보호하는 시스템 등 정보보호와 관련된 유무형의 모든 자산을 의미한다.
2. 정보시스템이란 회사가 보유한 컴퓨터, 전산시스템, 네트워크, 소프트웨어, 영상매체시설물 등 정보 관리에 사용되는 일체의 장비 및 시스템을 말한다.
3. 정보보안 사고란 해킹, 악성코드 감염, 비인가 접근, 자료 유출, 무단 반출 등 회사 정보자산의 기밀성, 무결성, 가용성에 영향을 미침으로써 결과적으로 본 규정에 위배되는 모든 행위
4. OT망이란 반도체 장비 제어, 공정제어 등 설비운영 시스템이 연결된 전산망을 말한다.
5. FAB란 반도체 제조가 실제로 이루어지는 생산 공장 또는 라인을 말한다.

② 이 외의 용어는 관련 법령 및 회사 내 타 보안 관련 규정에서 정하는 바에 따른다.

## 제2장 정보시스템 및 네트워크 보안

**제4조(설비망과 업무망의 망분리)**

① 회사는 업무망, 인터넷망, 생산망(OT망)을 상호 분리하여 운영하며, 물리적 또는 논리적 망분리를 기본으로 한다.

② 특히, 반도체 생산설비 및 장비 제어 시스템이 연결된 OT망은 인터넷망과 물리적으로 완전히 분리하여야 하며, 외부와의 연계 또는 통신은 원칙적으로 금지한다.

③ 불가피하게 외부에서 원격으로 설비에 접속할 필요가 있는 경우, 사전에 보안담당부서의 승인을 받아야 하며, 전용 게이트웨이를 통해 접속하여야 한다.

④ 모든 외부 원격 접속 세션은 실시간 모니터링되며, 접속 로그 및 작업 내역은 기록·보관하여야 한다.
⑤ 망분리 상태에 대한 정기 점검 및 검증은 분기 1회 이상 실시하며, 망 간 연계 가능성이 있는 시스템은 별도 보안 진단 대상에 포함하여야 한다.
⑥ 업무망과 인터넷망이 논리적으로 분리된 환경에서는 중간 매개체(파일, 데이터 등)의 이동 시 DLP 시스템의 사전 검토 및 보안담당부서 승인을 받아야 한다.

**제5조(업무망 접근 통제)**

① 업무망에 연결된 정보시스템은 사용자 별 최소권한 원칙에 따라 접근을 통제한다.
② 모든 정보시스템은 인증절차(사번 기반 계정, 비밀번호, OTP 등)를 거쳐야 하며, 시스템 접근 및 사용 기록은 자동 저장되어야 한다.
③ 1급 비밀에 대한 접근은 이중승인 절차를 적용할 수 있으며, 관련 정책은 별도의 지침에 따른다.
④ 시스템 접근 로그, 자료 다운로드 기록 등은 정보보안 감사 및 사고 조사 시 활용될 수 있도록 최소 1년 이상 보관하여야 한다.

**제6조(보안시스템의 운영)**

① 회사는 다음 각 호에 해당하는 정보보호 시스템을 설치·운영하여야 한다.
침입차단시스템(IPS), 침입탐지시스템(IDS)
네트워크 접근제어(NAC) 시스템
이상행위 탐지 및 경보 시스템(UEBA, SIEM 등)
중요자료 유출 방지 시스템(DLP)
엔드포인트 위협 탐지 대응(EDR) 시스템
② 각 보안 시스템은 연계되어 통합 관제되며, 보안담당부서는 주기적으로 로그 및 이상징후를 점검하여야 한다.

## 제3장 정보전송 및 저장매체 보안

**제7조(정보전송 보안)**

① 영업비밀 및 중요 정보의 외부 전송은 암호화 조치를 필수로 하며, 부서장 및 보안담당부서의 사전 승인을 받아야 한다. 승인 없이 외부로 전송하는 행위는 금지된다.
② 이메일, 메신저, 클라우드 스토리지 등 정보전송 수단은 회사에서 지정·승인한 시스템만을 사용하여야 하며, 개인 이메일, 개인용 클라우드 계정, 외부 메신저는 사용을 금한다.
③ DLP(Data Loss Prevention) 시스템을 통해 전송 대상, 파일 내용, 확장자, 수신처 등을 자동 감시하며 특정 확장자 파일과 회사가 지정한 기밀 파일 유형은 탐지 및 차단한다.
④ 승인된 외부 전송 시에도, 수신자 식별, 전송 목적 명시, 전송 이력 기록이 필수이며, 전송 후 3영업일 이내에 해당 사실을 보안담당부서에 보고하여야 한다.

⑤ 반복적 또는 고의적으로 승인되지 않은 채널을 통해 정보를 전송한 경우, 관련 임직원에게는 징계 등 인사조치를 취할 수 있으며, 외부 수신자에 대해서도 민형사상 조치를 검토할 수 있다.

**제8조(저장매체 통제)**

① 회사는 정보자산 유출을 방지하기 위하여 저장매체의 사용을 제한하며, USB, 외장하드, SD카드 등 외부 저장장치는 원칙적으로 금지한다.
② 불가피하게 저장매체 사용이 필요한 경우, 사전 사용신청서를 제출하고 보안담당부서의 승인을 받아야 하며, 승인된 저장매체는 암호화 및 백신 검사 후 사용하여야 한다.
③ 저장매체 반출 시에는 저장자료 목록을 첨부하여 반출 승인을 받아야 하며, 사용 후 즉시 회수 또는 자료 폐기를 확인하여야 한다.
④ 저장매체 사용 및 반출입 이력은 문서화되어 최소 1년 이상 보관되어야 하며, 위반 시 관련자에 대한 징계 조치를 취할 수 있다.

**제9조(FAB 및 보안구역 내 저장매체 통제)**

① FAB, 서버실, 생산기술실 등 보안통제구역 내에서는 저장매체 사용을 원칙적으로 금지하며, 예외적으로 공정 데이터 수집이나 설비 진단 목적의 사용이 필요한 경우 사전승인을 받아야 한다.

② FAB 내 사용이 허용된 저장매체는 사전에 등록된 암호화 저장매체에 한하며, 보안담당부서의 감독하에 사용되어야 한다.

③ 무단 저장매체 반입·사용 적발 시, 해당 장비는 즉시 회수 및 검사되며, 필요시 디지털 포렌식 절차를 거쳐 자료 유출 여부를 조사한다.

**제10조(모바일 및 무선기기 관리)**

① 개인 모바일기기(휴대폰, 스마트워치, 블루투스 장비 등)는 보안통제구역 내 반입을 금지하며, 출입 시 보안담당자의 확인을 받아야 한다.
② 회사는 무선기기 반입 차단을 위하여 RF탐지기, 금속 탐지기 등을 운용할 수 있으며, 위반 적발 시에는 징계 및 출입 제한 조치를 취할 수 있다.
③ FAB 내 사용 가능한 모바일 단말기는 회사에서 등록된 전용 장비에 한하며, 사용기록은 보안담당부서가 주기적으로 점검하여야 한다.

**제11조(장비 반입 및 전산기기 관리)**

① 외부 장비(유지보수 노트북, 진단장비 등)의 반입은 보안담당부서의 사전승인과 보안설정 확인 후 허가되며, 반입 후에는 지정된 구역에서만 사용하여야 한다.
② 외부 장비 사용 시에는 인터넷 접속 차단, 저장매체 포트 차단 등 사전보안조치를 실시하여야 하며, 작업 종료 후 보안담당자의 점검을 받아야 한다.
③ 모든 사내 전산기기는 보안자산으로 등록되어야 하며, OS 업데이트, 백신 설치, 권한 관리 등 보안패치를 정기적으로 유지하여야 한다.

## 제4장 악성코드 및 해킹 대응

**제12조(비인가 무선통신 차단 및 감시)**

① 회사는 FAB, 설비기술실, 서버실 등 중요구역 내에서 비인가된 무선통신 수단(Wi-Fi, Bluetooth, NFC 등)의 사용을 원칙적으로 금지하며, 모든 무선 통신기기는 사전 등록된 장비에 한해 사용하여야 한다.

② 보안담당부서는 무선신호 탐지 시스템(RF 탐지기 등)을 통해 상시 감시체계를 운영하며, 비인가 무선기기가 탐지된 경우 즉시 해당 구역에 대한 현장조사 및 사용자 확인을 실시하여야 한다.

③ 개인 소지의 스마트폰, 스마트워치, 무선이어폰 등 무선 송수신 가능 장비는 보안통제 구역 내 반입이 금지되며, 필요시 입출입 시 반입물품 등록절차를 거쳐야 한다.

④ 위반이 확인된 경우, 관련 장비는 보안검사를 위해 회수되며, 해당 직원 또는 외부인은 인사규정 또는 계약서에 따라 징계 및 출입제한 조치를 받을 수 있다.

⑤ 무선차단이 기술적으로 불가능한 장비가 있는 경우, 별도의 차폐조치 또는 보안격리 공간에서만 사용하도록 하며, 해당 장비는 지정표식 및 보안담당부서의 관리대장에 등록하여야 한다.

**제13조(악성코드 및 보안패치 관리)**

① 장비 제어용 컴퓨터, 생산망 단말기, 분석장비 연계 단말 등 OT 환경 내 시스템은 외부 인터넷과 논리적으로 분리되어야 하며, 최신 백신 프로그램을 설치하여 자동 업데이트 기능을 유지하여야 한다.

② 정기적인 악성코드 탐지 및 시스템 검사 결과는 문서로 기록·보관하며, 감염 또는 의심 징후 발생 시 즉시 해당 장비를 격리하고, 원인 분석을 실시하여야 한다.

③ 운영체제(OS) 또는 응용프로그램에서 보안 취약점이 발견된 경우, 패치 가능 장비는 즉시 최신 보안패치를 적용하여야 하며, 적용이 불가한 장비에 대해서는 아래의 대체조치를 시행하여야 한다.

인터넷 및 외부망과의 연결 차단
화이트리스트 기반 접근제어 체계 적용
논리적 네트워크 분리 및 별도 보안장비 설치

④ 보안패치 계획은 보안담당부서가 연 1회 이상 점검하며, 미이행 장비에 대해서는 위험도 평가 후 사용중지 또는 보완계획 수립 조치를 명령할 수 있다.

## 제5장 정보보안 사고 대응

**제14조(정보유출 사고 대응)**

① 설계도면, 공정파일, 장비로그, 테스트결과 등 영업비밀에 해당하는 정보가 유출되었거나 유출이 의심되는 경우, 보안담당부서는 즉시 아래의 항목에 대해 조사를 착수하여야 한다.

관련 사용자의 시스템 접근기록, 자료 열람 및 복사 기록
파일 전송, 이동, 복제 등의 로그 데이터
USB, 이메일, 메신저 등 경유 수단 확인

② 분석 결과 이상징후가 확인된 경우, 관련 계정을 즉시 차단하고, 해당 시스템은 격리 조치하며, 필요한 경우 디지털 포렌식 절차를 통해 근거를 수집한다.

③ 사고 분석 결과 및 대응 조치는『정보보안 사고 보고서』형태로 정보보안심의위원회에 보고하여야 하며, 재발 방지를 위한 보안 정책 개정, 기술 조치, 사용자 교육계획 등을 포함하여야 한다.

④ 정보보안 사고의 은폐, 지연보고, 허위보고가 확인된 경우, 관련 임직원 및 부서에 대해 인사규정에 따라 책임을 물을 수 있다.

**제15조(FAB 내 정보보안 강화)**

① FAB 내에서 운용 중인 모든 IT 장비 및 시스템은 보안자산으로 등록되어야 하며, 보안담당부서는 장비의 현황, 보안패치 이력, 점검결과 등을 주기적으로 관리하여야 한다.

② 보안자산으로 등록된 장비는 다음의 조건을 충족해야 한다.

최신 보안패치 및 백신 설치 여부 확인
관리자 계정, 접근 권한 설정 점검
무선통신 기능(와이파이, 블루투스 등) 비활성화 여부 확인

③ 제조공정 데이터(SPC, APC, 레시피 등)에 대해서는 실시간 이중화 시스템 또는 주기적 백업체계를 구축하여, 시스템 장애 또는 보안사고 발생 시 신속한 복구가 가능하도록 하여야 한다.

④ 백업된 공정정보는 암호화되어 별도 저장소 또는 물리적 보관매체에 분리 보관되며, 복구 테스트는 분기 1회 이상 시행하여야 한다.

⑤ 보안담당부서는 FAB 내 전체 IT 자산 및 공정데이터의 백업·복구체계에 대해 연 1회 이상 정기 점검을 실시하고, 결과를 정보보안심의위원회에 보고하여야 한다.

## 제6장 임직원의 보안책임 및 교육

**제16조(보안의무)**

① 임직원은 정보보안 관련 법령, 본 규정, 관련 지침 및 매뉴얼을 숙지하고 준수하여야 한다.

② 보안규정 위반 또는 과실로 인한 사고 발생 시 인사규정 및 징계규정에 따른 조치를 받을 수 있다.

**제15조(보안교육)**

① 전 임직원은 연 1회 이상 정보보안 교육을 이수하여야 하며, 교육 이수 후 이해도 점검을 위한 간단한 평가를 병행한다. 해당 평가는 교육 이수 실적에 포함하여 기록·관리한다.

② ①항의 정보보안 교육은 신규 입사자, 승진자 및 외부 협력사 인력에 대하여도 사전 교육의 형태로 실시하여야 한다.
③ 교육 내용에는 해킹 사례, 자료 유출 방지법, 최신 보안 위협 동향 등이 포함되어야 한다.

**제16조(생성형 AI 및 클라우드 서비스의 사용)**
① 사내 임직원은 외부 생성형 AI 서비스(예: ChatGPT, Copilot, Bard 등)를 업무에 활용하거나 회사 정보를 입력하는 행위를 금지한다.
② 회사 내부에서 운영하는 생성형 AI 및 클라우드 서비스의 경우, 영업비밀 중 자료등급이 3급으로 분류된 정보에 한하여 사용할 수 있다. 이때에도 업무 목적에 부합하는 최소한의 정보만을 입력하여야 한다.
③ 생성형 AI, 데이터 분석 툴 등 기술 수단을 통해 2차적으로 생성된 정보라 하더라도, 그 기초가 된 정보가 영업비밀이며 해당 정보의 본질적 가치가 유지되거나 재현된 경우, 그 2차 정보는 동일한 등급의 보호조치를 적용한다.
④ 내부 서비스 사용 시에도 정보보안담당관의 판단에 따라 사전 승인 및 로그 보존 등의 절차를 요구할 수 있다.

## 부칙

(시행일) 본 규정은 2025년 0월 0일부터 시행한다.
(개정) 본 규정의 제정 및 개정은 보안심의위원회의 심의를 거쳐 대표이사의 승인을 받아야 한다.