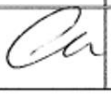
엔스텔정보통신㈜ 방위산업기술보호 내규

담당	검토	검토	승인
			

제 정 2025. 03. 17

제 1 장 총 칙

제 1조【 목 적 】

본 내규는 「방위산업기술보호법」 및 「방위산업기술보호법 시행령」에 따라, 엔스텔정보통신㈜(이하 “회사”라고 한다)의 방위산업기술 보호에 필요한 사항을 규정함을 목적으로 한다.

제 2조【 적용범위 】

본 규정은 회사 임직원(정 직원 및 계약직원) 및 외부 협력업체와 파트너, 기타 회사를 출입하는 모든 사람에게 적용한다. 단, 본 규정에 정한 범위 내에서 특수성과 실정에 따라 그 적용범위에 예외를 두어 적용할 수 있다.

① 외부 협력업체 또는 회사 출입자에 한하여 개인 또는 단체에 적용할 수 있다.

② 별도 비밀 및 보안을 요하는 업무 수행 시, “비밀유지서약서”를 작성 및 준수하여야 한다.

제 3조【 방위산업기술 보호 내규의 개정 】

① 회사는 방위산업기술보호 내규 개정 시, 방산기술보호 심의회의 의결 및 대표이사의 승인을 득하여야 한다.

② 회사는 방위산업기술보호 내규 개정 시, 개정된 내규에 대해 전 직원 교육을 실시 혹은 전 직원의 회람 확인 서명을 실시한다.

③ 회사는 방위산업기술보호 내규의 개정과 관련하여 다음 각 호의 사항을 검토한다.

1. 기술보호책임자 및 기타 보안 관련 업무 담당자 변경 여부
2. 방위산업 기술보호 관련 법령이나 훈령 등의 제·개정사항 여부
3. 보안진단 과정에서 나타난 취약점 대응방안 및 개선권고 사항
4. 정부 권고사항 등 기타 보안 강화를 위해 필요한 사항

제 4조【 방위산업기술보호 연간 시행계획의 수립 】

대표이사는 방위산업기술보호법 제5조에 따른 방위산업기술의 보호에 관한 시행계획 및 회사의 특성을 참고하여, 매년 아래의 내용을 포함한 자체 방위산업기술보호 시행계획을 수립 및 시행하여야 한다.

① 클린데스크 활동 실시 계획 및 주기

② 임직원 보안교육 실시 계획

③ 업무용 PC 취약점 진단 실시 계획 및 주기

제 5조【 기술 보호 대상 종류 및 보관방법 】

① 대상기관이 보호하여야 할 종류(이하 “보호종류”라 한다)는 다음 각 호와 같다.

1. 방위산업기술 등의 도면(관련 소프트웨어를 포함한다) 및 품질보증 요구서
2. 방위산업기술 등을 설명하는 규격서 및 보고서
3. 방위산업기술 등이 포함된 견본, 시제품, 전자매체기록, 기술자료
4. 그 밖에 방위산업기술 등을 포함하는 자료

② 방위산업기술보호법 제 8조에 따라 보호되어야 하는 개발성과물은 연구개발 단계별 산출물로서 전항 각 호와 같다.

③ 관리대상기술의 보관방법은 종이 출력물과 전자파일 형태 등으로 구분하여 관리하며 보호대책을 강구한다.

제 6조【 기술보호 책임자의 임명 】

① 대표이사는 방위산업기술 보호업무 수행을 위하여 기술보호 총괄책임자를 임명하여야 하며, 기술보호 총괄책임자를 보좌하기 위한 각 부서별 기술보호 책임자를 임명할 수 있다.

② 기술보호총괄책임자는 방위산업기술 보호 관련 정보의 공유와 방위산업기술의 유출 및 침해에 대한 공동 예방·대응을 위하여 부서별 기술보호 책임자들과 함께 방위산업기술보호 협의회를 구성·운영할 수 있다.

제 7조【 기술보호 책임자의 직무 】

① 기술보호 총괄책임자는 대표이사로부터 방위산업기술 보호업무 전반을 위임받아 다음 사항의 업무를 수행한다.

1. 보호대상 기술의 식별 및 관리 체계의 운영·관리 총괄 및 조정·감독
2. 인원통제 및 시설보호 체계의 운영·관리 총괄 및 조정·감독
3. 정보보호 체계의 운영·관리 총괄 및 조정·감독
4. 그 밖에 방위산업기술보호 내규의 이행을 위하여 필요한 사항

② 기술보호 책임자는 제 1항 각 호의 업무에 대한 지원 및 기술보호 총괄책임자로부터 위임받은 업무를 수행한다.

③ 기술보호 책임자는 소속 부서가 보유·취급하는 관리대상기술을 보호하기 위하여 제1항 제1호부터 제3호까지의 체계에 대한 운영·관리 업무 등을 수행한다.

④ 기술보호 책임자는 국방기술보호국장이 지정한 교육기관에 의한 방위산업 기술 보호 교육을 반드시 이수하여야 한다.

제 8조【 방위산업 기술보호 교육 실시 】

① 회사는 회사 소속 방위산업 관련자 및 방위산업분야 기술협력 등을 위해 회사에 상주하거나 상시 출입하는 외부인・외국인(단순 용역 인력은 제외한다)에 대하여, 개인별로 매년 1회 1시간 이상 방위산업기술 보호에 관하여 다음 각 호의 어느 하나에 해당하는 교육(이하 “방위산업 기술보호 교육”이라 한다)을 실시하여야 한다.

1. 국방기술보호국장이 지정한 교육기관에 의한 교육
2. 회사 내부 교육계획에 따라 시행하는 자체교육. 이 경우 자체교육은 기술보호 책임자(기술보호 총괄책임자, 부서별 기술보호책임자를 말한다. 이하 이 조에서 같다) 또는 기술보호 책임자의 위임을 받은 기술보호 전담부서 소속 담당자가 실시하여야 한다.
3. 방위산업 기술보호 전문 교육 업체, 혹은 방산 기술 보유한 체계 업체에서 위탁 실시하는 교육

② 회사는 방위산업기술보호교육을 집합교육, 온라인교육, 교육자료 배포 등 다양한 방법으로 실시할 수 있으며, 체계업체에 위탁 실시할 수 있다.

③ 회사는 매년 전 직원을 대상으로 한 기술보호 관련 교육계획을 수립하며, 교육 실적을 기록·유지한다.

제 9조【 방산기술보호 심의회 】

① 대표이사는 관리대상기술의 식별 및 관리와 방위산업기술 보호에 관한 다음 각 호의 사항을 심의하기 위하여 방위산업기술보호심의회(이하 “심의회”라 한다)를 구성·운영하여야 한다.

1. 관리대상기술의 식별
2. 내규 제·개정 관련 사항
3. 방위산업기술 보호에 관한 주요사항
4. 기술보호구역 설정 관련 사항
5. 보안사고자 및 내규 위반자 처리에 관한 사항
6. 그 밖에 대표이사 또는 심의회의 장이 방위산업기술 보호와 관련하여 필요하다고 인정하는 사항

② 보안심의회의 구성은 다음 각호와 같으며 보직과 동시에 당연직으로 한다.

1. 보안심의회 위원장 : 대표이사
2. 위원 : 기술보호총괄책임자 및 기술보호책임자

③ 보안심의회의의 심의·의결 절차는 다음 각호와 같다.

1. 재적위원 2/3 이상의 출석과 출석위원 과반수 찬성으로 의결한다.
2. 보안심의회 위원장 공석 시 기술보호 총괄책임자가 그 직무를 대행한다.

④ 의결결과는 보안심의회 의결서에 기록하고 위원장의 승인을 득한 후 시행한다.

제 10조【 기술 유출 및 침해 사고 대응 】

① 회사는 방위산업기술 및 영업비밀, 기타 중요정보 등의 침해 및 유출사고 발생 시, 다음 각 호의 절차를 준수한다.

1. 방위산업기술 유출 및 침해 상황조사
2. 방위사업청 방위산업기술 유출·침해사고 신고센터(1577-1118), 국정원(111), 군사안보지원사령부(1337) 등 신고센터에 신고
3. 고객사 보안팀에 보고
4. 사고 내용, 범위, 시기, 방법 등 상세내역을 사내에 공지
5. 기술정보 유출의 책임소재가 있는 직원에게 6시간 이상의 보안교육 실시
6. 보안심의회 및 인사위원회 회의를 통하여, 아래 각 호와 같은 직원을 징계 조치

가. 기술정보 유출의 책임소재가 있는 직원

나. 방위산업기술의 유출 및 침해 정황을 인지하였으나 보고의무를 이행하지 않은 직원

② 회사는 방위산업기술 유출 및 침해 재발방지 활동에 만전을 기하며, 방위산업기술 유출 및 침해 대응 준비 상태를 상시 확인・점검한다.

제 2 장 방위산업기술 보호

제 1 조【 기술식별 및 관리 】

회사는 방위산업기술정보 및 기술자료 보호를 위하여, 아래 각 호와 같은 방법으로 기술을 식별 및 관리하여야 한다.

① 식별 및 확인 : 회사가 생산하거나 고객사 등으로부터 접수한 기술자료 중에서 방위산업기술에 해당하거나 해당 가능성이 있는 기술을 심의회를 거쳐 식별하여야 한다.

② 보호 관리 : 회사는 1항에 따라 식별·판정된 방위산업기술 등을 제1장 제5조에 따른 보호종류의 형태로 보호 및 관리하여야 한다.

③ 접근 통제 : 정보자산을 업무의 성격 및 중요도에 따라 구분하고, 이에 따라 사용자별 정보자산의 접근 권한 및 범위를 차등 부여하고 관리하여야 한다.

④ 정보 분리 : 기술정보 및 기술자료에 대한 접근이 가능한 장소 및 PC를 설정하고, 사내 기타 정보와 분리하여 별도의 문서보관함 혹은 대용량저장장치 등에 관리하여야 한다.

⑤ 기록 관리 : 수령 또는 산출된 기술정보와 자료의 목록을 기록하고, 별도 표시하여 관리하여야 한다.

⑥ 책임부여 및 추적 : 방위산업기술 관련자들에 대해서 의무와 책임을 명확히 하고, 정보 유출 및 침해 등의 보안사고 발생 시 책임을 추적하여 제 1장 제 10조의 유출 및 침해 대응 절차를 수행하여야 한다.

제 2 조【 방산기술 자료 외부 공개 및 제공 시 보안 조치 】

① 회사는 방산 기술 자료를 외부에 공개하거나 제공하고자 하는 때(계약에 의한 자료의 제공은 제외한다)에는 방산기술보호대책을 강구하여 관련 부서장의 사전검토를 거친 후, 해당 관리대상기술을 활용·관리하는 부서에 속한 기술보호 부서책임자가 이를 확인하고 기술보호 총괄책임자가 이를 승인하도록 하여야 한다.

② 전항에 따른 사전검토 결과에는 다음 각 호의 사항이 포함되어야 하며, 대상기관의 장은 해당 결과를 기록·유지하여야 한다.

1. 검토 일자
2. 검토 자료명
3. 검토 결과 및 조치
4. 승인 여부 등

③ 기술보호총괄책임자는 사전 검토결과의 적정성을 매 반기 1회 이상 확인하여야 하며, 확인 결과 관리대상기술의 보호를 위하여 필요한 조치를 할 수 있다.

제 3 조【 방산기술 관련 수출 및 국내 기술이전시 보안 조치 】

① 방산기술 관련 수출 및 국내 기술 이전 업무의 담당자는, 해당 방산기술의 소유권자와의 방산기술보호 특약을 체결하고 기술보호 총괄 책임자의 사전 승인을 얻어야 한다.

② 기술보호 총괄 책임자는 제1항의 규정에 따른 승인신청에 대하여, 방산기술의 수출 및 국내 이전에 따른 파급효과 등을 검토하여 보안 심의를 거쳐 승인할 수 있다.

③ 보안 총괄 책임자는 제 2항의 보안 심의 결과, 방산기술의 수출로 인한 정보 침해・유출의 우려가 있는 경우에는 수출 및 이전 금지 등의 조치를 명할 수 있다.

④ 기술보호 총괄 책임자는 방산기술의 수출 및 국내 이전 담당자가 제1항의 규정에 따른 승인을 얻지 아니하고 수출 및 국내 이전 업무를 진행한 경우, 보안 총괄 책임자에게 조사를 의뢰하고 보안 심의를 거쳐 해당 방산기술의 수출 및 이전 중지・원상 회복 등의 조치를 명령할 수 있다.

제 4 조【 연구개발 보호 절차 】

① 회사는 다음 각 호와 같은 연구개발 보안관리 조치를 하여야 한다.

1. 연구소에 대한 보호구역 설정
2. 연구개발자의 연구소 출입권한 차등 부여 및 출입 현황 관리
3. 연구개발자에 대한 보안교육 실시 및 보안서약서 제출 요청
4. 보안과제를 수행하는 외국인 연구개발자에 대한 기술보호총괄책임자의 승인 및 보안총괄책임자에 대한 보고
5. 보안책임자 지정
6. 기타 연구관리시스템 및 연구개발정보 처리 과정과 결과에 대한 보안관리 조치

② 기술보호총괄책임자는 제 1항에 따른 연구개발 보안관리 실태를 점검하고, 그 결과에 따라 보안총괄책임자와 보안심의회에 필요한 조치를 의뢰할 수 있다.

③ 기술보호총괄책임자는 다음 각 호의 어느 하나에 해당하는 사고(이하 "보안사고"라 한다)가 발생한 경우에는 그 사고를 알게 된 즉시 필요한 조치를 하고, 보안 총괄 책임자에게 보고해야 한다.

1. 연구개발성과의 침해 · 유출 · 누설 · 분실 · 훼손 · 도난
2. 연구개발성과를 유통 · 관리 · 보존하는 시스템의 유출 · 파손 · 파괴

제 3 장 인력 통제

제 1 조【 보안서약서 】

① 모든 임직원은 입/퇴사 시와 연봉계약 시 및 보직이동 시 비밀유지의무를 부과한 "보안서약서"를 제출하고 이에 의거 비밀유지의무를 준수해야 한다.

② 제 1항은 계약직 및 외주 용역에도 동일하게 적용된다.

③ 회사와 상호 협력관계를 유지하는 모든 업체 또는 개인은 매 계약체결 시마다 "비밀유지서약서"를 작성하고 이에 의거 비밀유지의무를 준수해야 한다.

④ 기술보호 책임자는 연구개발, 합작/기술제휴 등 기타 특별관리가 필요한 업무 수행업체 또는 수행자에 대해 별도의 비밀유지서약을 받아야 한다.

제 2 조【 접근 권한 】

① 내방 인원에 대하여는 출입금지 구역 등을 명확히 하고, 사전 계획된 안내 계획에 의하여 안내하고 방문자 임의 행동을 못하도록 통제하여야 한다.

② 비밀을 비인가자에게 열람 및 공개하고자 할 때에는 최고경영자의 승인을 얻어야 한다.

③ 비인가자 또는 외래 방문자는 안내실(또는 회의실)에서 면회함을 원칙으로 하며, 업무관련 시 인솔자 책임하에 동반 출입할 수 있다. 단, 업무 외적 방문자는 회사 출입을 할 수 없으며, 필요 시 회사 출입문 밖에서 면회할 수 있다.

④ 문서실 및 보안등급이 필요한 "제한구역", "보호구역"의 출입 시 관리자가 부여한 출입인가자에 한해 출입을 허용하며, 출입인가자의 보안등급은 기술보호 총괄책임자가 구분하여 관리하여야 한다.

⑤ 출입인가자의 보안등급은 "임직원 보안등급 현황" 기준에 의거한다.

제 3 조【 신원 조사 】

① 회사는 정보수사기관에 방산관련자 및 방산기술 취급인가자 등의 신원조사를 요청할 수 있다.

② 방산관련자 및 방산기술 취급인가자는 회사가 신원조사를 요청할 시 합당한 사유 없이 이를 거부할 수 없다.

③ 제 1,2항은 계약직 및 외주 용역에도 동일하게 적용된다.

제 4 조【 퇴직자 기술보호 조치 】

① 퇴직자는 퇴직 전 보안서약서를 작성하고, 기술보호책임자로부터 방위산업 기술보호교육을 받아야 한다.

② 회사는 퇴직자의 정보체계 계정 및 회사 출입권한을 삭제하여야 한다.

③ 퇴직자는 모든 방위산업 기술 관련 자료 및 컴퓨터 하드디스크와 기타 저장 매체를 반납하고, 회사는 이를 점검 및 보관하여야 한다.

④ 중요 기술정보 취급자의 퇴직 절차 확인은 방위산업 기술보호 심의회 의결 및 위원장의 승인을 득하여야 한다.

제 5 조【 방산기술 접근 권한 변경자의 기술보호 조치 】

회사는 담당업무가 방산업무에서 민수업무로 변경되었거나, 중요 방위산업기술 정보 취급 업무에서 그 외의 업무로 변경되어 방위산업기술 접근 권한의 삭제 혹은 변경이 요구되는 직원들(이하 “방산기술 접근 권한 변경자”라 한다)에 대하여 아래 각 호와 같은 보안 조치를 취하여야 한다.

① 회사는 방산기술 접근 권한 변경자의 정보체계 계정을 삭제 후 재 생성하고, 출입권한을 삭제 또는 변경하여야 한다.

② 방산기술 접근 권한 변경자는 보안서약서를 작성하고, 기술보호책임자로부터 방위산업 기술보호교육을 받아야 한다.

③ 방산기술 접근 권한 변경자의 업무 인수인계 절차는 기술보호책임자의 승인을 거쳐야 한다.

④ 방산기술 접근 권한 변경자는 모든 방위산업 기술 관련 자료 및 컴퓨터 하드디스크와 기타 저장 매체를 반납하고, 회사는 이를 점검 및 백업 보관하여야 한다.

제 6 조【 해외출장자 기술보호 조치 】

① 전 임직원은 공무상 해외 출장 출발 전, 아래의 기술보호 절차를 실시하여야 한다.

1. 보안총괄책임자에게서 해당 출장에 대한 보안성을 검토 및 사전 승인을 득하여야 한다.
2. 출장 전 보안서약서를 작성하고 기술보호교육을 받아야 한다.
3. 출장용으로 지정된 정보통신기기만을 지참하여야 한다.
4. 기술보호 책임자로부터 비상상황 발생시 연락망과 조치사항을 고지받아야 한다.

② 전 임직원은 공무상 해외 출장 중, 아래의 기술보호 조치사항을 준수하여야 한다.

1. 중요 기술 자료는 분실 또는 유출을 방지하기 위해 잠금장치와 함께 보관한다.
2. 계획된 인력 외의 외국인 접촉 이력을 기록한다.

③ 전 임직원은 공무상 해외 출장 종료 및 입국 이후, 아래의 기술보호 절차를 실시하여야 한다.

1. 출장 시 후 지참한 정보통신기기를 기술보호책임자에게 점검 받는다.
2. ②항 2호의 외국인 접촉 이력 및 기타 보안 특이사항을 기술보호 총괄책임자에게 보고한다.

제 7 조【 상주 외부인 보안 조치】

① 회사는 방위산업 분야 기술협력을 위해 상주 또는 상시 출입하는 외부인에 대하여, 다음 각 호와 같은 기술보호대책을 실시하여야 한다.

1. 사전 신원조사 실시 및 보안서약서 징구
2. 기술보호책임자가 외부인/외국인의 업무 수행에 대해 보안성 검토 후 사전 승인
3. 계약서 또는 관련 서류상의 기술보호의무 부과
4. 주기적인 방위산업기술 보호교육 실시
5. 업무장소 지정 및 사내직원과 다른 출입권한 적용으로, 지정된 장소 외 출입통제
6. 전자메일, FAX 등 이용 시 기술보호총괄책임자의 사전 승인
7. 노트북 및 저장장치 반입/반출 통제 (정보통신기기 반출입확인서 작성 및 사전 승인)
8. 사내 모든 정보 및 출력물 등의 외부 반출 통제
9. 계약조건 등에 따라 근무부서에 대해 주기적 기술보호 실태점검 실시
10. 사업 종료 후 교부된 자료와 장비 등의 회수 및 점검

② 회사는 방위산업 분야 기술협력을 위해 상주 또는 상시 출입하는 외부인의 근무 현황(다음 각 호의 내용을 포함)을 작성 및 유지하여야 한다.

1. 해당 근무인원 인적사항
2. 출입권한 부여 현황
3. 상주근무 외부인의 신원조사 결과
4. 정보통신망 구성도 체계 내 접근 가능목록
5. 기술보호 교육 일지
6. 상주근무 구역 점검 일지

제 8 조【 상주 외국인 보안 조치】

① 회사는 방위산업 분야 기술협력을 위해 상주 또는 상시 출입하는 외국인(해당 외국인을 고용하는 경우를 포함하며, 해외사무소도 같다)에 대하여, 다음 각 호와 같은 기술보호대책을 실시하여야 한다.

1. 사전 신원조사 실시 및 보안서약서 징구
2. 기술보호책임자가 외부인/외국인의 업무 수행에 대해 보안성 검토 후 사전 승인
3. 신원 확인 결과 및 방산기술보호대책 등이 포함된 외국인 관리계획서를 작성 및 이행
4. 계약서상의 기술보호의무(국내 기술보호법령 준수) 부과
5. 계약 만료 시에도 보안서약서 징구
6. 주기적 방위산업기술보호교육 실시
7. 업무장소 지정 및 사내직원과 다른 출입권한 적용으로, 지정된 장소 외 출입통제
8. 정보통신망 접근 권한 통제 및 감독
9. 전자메일, FAX 등 이용 시 기술보호총괄책임자의 사전 승인
10. 노트북 및 저장장치 반입/반출 통제 (정보통신기기 반출입확인서 작성 및 사전 승인)
11. 사내 모든 정보 및 출력물 등의 외부 반출 통제
12. 근무부서에 대해 주기적(분기 1회 이상) 기술보호 실태점검 실시
13. 해외 출국 시 내규 제 6조 [해외출장자 기술보호 조치]에 준하는 보안 조치 및, 방위산업기술보호교육을 실시하고 해당 현황을 유지

② 회사는 방위산업 분야 기술협력을 위해 상주 또는 상시 출입하는 외국인의 근무 현황(다음 각 호의 내용을 포함)을 작성 및 유지하여야 한다.

1. 해당 근무인원 인적사항
2. 출입권한 부여 현황
3. 상주근무 외부인 및 외국인의 신원조사 결과
4. 정보통신망 구성도 체계 내 접근 가능목록
5. 기술보호 교육 일지
6. 상주근무 구역 점검 일지

제 4 장 시설 및 장비 보호

제 1 조【 기술보호구역 】

회사는 방위산업기술의 보호와 주요 시설, 장비 및 자재의 보호를 위해 필요한 장소에 “제한구역” 및 “통제구역” (제한구역과 통제구역을 합쳐 “기술보호구역”이라 한다)을 설정하여 이를 비인가자로부터 제한/통제/보호해야 한다.

① 제한구역은 회사업무공간 등 외부인 출입이 제한된 구역을 의미한다.

② 통제구역은 기술문서 보관함, 전산실 등 특히 중요하여 허가된 업무관련자 외엔 출입할 수 없는 구역을 의미한다.

③ 기술보호구역은 각 부서 기술보호책임자에 의해 상시 잠금 장치가 되어 있어야 한다.

④기술보호책임자는 기술보호구역 출입 희망자의 신분과 용무의 타당성 여부를 확인 후 출입을 입회 및 감독하여야 한다.

⑤ 기술보호구역은 그 종류에 따라 제한구역/통제구역 표시판을 출입구에 게시하여야 한다.

제 2 조【 통제구역 】

① 회사는 기술문서 보관함과 전산실 등 특히 중요하여 허가된 업무관련자 외엔 출입할 수 없는 구역을 “통제구역”으로 설정하고, 아래 각 호의 보안조치를 실시하여야 한다.

1. 통제구역 표시판을 통제구역 출입구에 게시한다.
2. 통제구역 출입 희망자는 통제구역이 위치한 부서 기술보호책임자 혹은 기술보호 총괄책임자에 의해 출입 승인을 받아야 하며, 외부인 출입의 경우 “외부인 출입관리대장”에 출입사항을 기록하고 “정보통신장비 반출입 신청서”에 정보통신장비 반출입 이력을 기록하여야 한다.
3. 2항의 “외부인 출입관리대장” 및 “정보통신장비 반출입 신청서”는 기술보호 책임자의 승인을 득하여야 한다.
4. 통제구역은 일반 보호구역의 출입인증시스템과 별도의 보안코드 인식을 통한 2중 출입인증시스템을 갖춰야 한다.
5. 통제구역 입구에는 130만 화소 이상의 CCTV가 설치되어 출입현황 감시와 녹화가 되어야 한다.

② 회사는 기술보호가 필요한 방위산업 기술 문서를 반드시 통제구역 내 이중 시건된 기술문서보관함에 보관하고, 열람 이력을 기록 관리하여야 한다.

제 3 조【 정보통신기기 반출입 통제 기준 】

모바일 기기, 저장매체, 정보시스템 등의 정보통신장비를 사내 중요 업무 구역에 반출입하는 경우, 보안사고 예방을 위한 통제 절차를 이행하여야 한다.

① 반출입 통제 대상 : 모바일 기기(노트북, 스마트패드, 스마트폰 등), 저장매체(HDD, SDD, USB메모리, 외장하드디스크, CD/DVD, 테이프 등), 정보시스템(서버, 네트워크 장비 등) 등

② 정보통신장비의 반출입을 희망하는 외부인은 정보통신장비 반출입 신청서 작성 및 기술보호책임자 사전 승인을 받아야 한다.

③ 반입 기기에 대하여 보안점검을 수행하고, 보안 스티커를 부착한다.

④ 반입을 승인받지 않은 정보통신 장비는 기술보호책임자가 수거하여 보관 후, 보호구역 출입 용무가 종료된 사용자에게 반납한다.

⑤ 사내 업무용 정보통신장비 반출 시 정보통신장비 반출입 신청서 작성 및 기술보호책임자 사전 승인을 받아야 한다.

제 4 조【 출입 관리 시스템 】

사내 중요 업무 구역은 아래 각 호와 같은 출입관리 시스템을 구비하여야 한다.

① 130만 화소 이상의 CCTV를 설치하여 상시 감시와 녹화를 실시한다.

② 24시간 출입보안관제 시스템과 이상탐지 경보장치를 가동한다.

③ 기술보호책임자는 수행업무와 신분에 따라 출입카드의 권한을 차등 부여하며, 출입카드/지문 태그 기록을 주기적으로 확인하여 보안 위반행위를 점검한다.

④ 출입 위반행위가 적발될 경우, 내규 제 1장 제 10조의 기술유출 침해 사고에 준하는 사고조사 절차와 제재 기준을 적용한다.

⑤ 방위산업과 관련 없는 민수 업무를 수행하는 인원들은, 방위산업 관련 업무 수행 구역과 출입문/가림막 등으로 구분된 별도의 업무 공간에 상주한다.

제 5 장 정보 보호

제 1 조 【 웹서버 업로드 시 보안성 검토 절차 】

회사는 웹 기반으로 구축되어 외부에서 접속 가능한 업무 목적의 사이트(공개된 정보시스템, 홈페이지 등)에 자료를 공개 혹은 업로드할 경우, 다음의 보안성 검토 절차를 실시한다.

① 기술보호 중요도 및 보안성 평가 : 공개하려는 자료 내 보호대상인 방위산업 기술 관련 내용이 포함되어 있는지를 점검하여, 기술보호의 중요도 및 보안성 평가

② 웹서버 혹은 웹사이트의 보안 취약점, 위험성 점검

③ 필요시 업로드 전 자료 암호화 및 백업

④ 업로드 후 자료의 다운로드 로그 기록 및, 비정상적인 활동 발생 시 알림 설정

제 2 조 【 정보시스템 접속 권한 통제 】

회사는 사내 정보시스템/서버의 접속 권한에 대하여 다음과 같은 사전 승인 절차를 수행한다.

① 정보시스템 접속을 희망하는 직원은, 필요한 권한 수준을 정의하여 전사 보안업무 총괄 책임자에게 접속 승인을 요청한다.

② 전사 보안업무 총괄 책임자는 기술보호 총괄 책임자와 협의하여 정보시스템 접속 승인 요청을 검토한다.

③ 정보시스템 접속이 승인된 경우, 기술보호 책임자는 해당 직원이 필요한 최소한의 접속 권한만을 부여하며 관련 교육을 해당 직원에게 실시한다.

④ 기술보호 책임자는 정보시스템 접속을 승인받은 직원의 접속 기록을 주기적으로 모니터링하며, 일정 주기로 권한을 검토하고 필요시 회수 혹은 갱신한다.

⑤ 기술보호 책임자는 시스템 장애나 보안 사고 발생에 대비하여, 접근 제어를 변경하거나 긴급히 접속을 차단할 수 있는 절차를 마련한다.

제 3 조 【 외부 업무 수행 시 보안조치 】

회사의 임직원은 출장, 외근, 재택근무 등 회사 외부에서 업무 수행 시 아래와 같은 보안조치를 실시한다.

① 업무용 PC, 저장장치와 같은 정보통신 기기 반출 시에는 반드시 기술보호 책임자의 승인을 득하며, 반출 전 운영체제 및 보안소프트웨어 등을 최신 버전으로 업데이트한다.

② 중요 기술정보 자료 출력물을 반출 시에는 반드시 부서장과 기술보호책임자의 승인을 득하여야 한다.

③ PC 외부 반출 시 분실 방지를 위해 지속적으로 관리하며, 물리적 잠금장치와 비밀번호 등 보안 인증을 설정한다.

④ 기술보호책임자에 의해 승인된 저장장치만을 사용한다.

⑤ 공공장소의 Wi-Fi는 사용을 금지하며, 회사 외부에서 NAS 서버 등 사내시스템에 접속할 때에는 보안 인증된 VPN을 활성화한다.

⑥ 업무 관련 자료는 암호화하여 저장 및 전송하며, 업무 종료 후 로그아웃 및 원격 데이터 삭제 기능을 활성화한다.

⑦ 기술정보 유출 등 보안사고가 우려되는 상황 발생 시에는 반드시 사내 기술보호책임자에게 보고한다.

제 4 조【 이메일 송·수신 관리 】

이메일 사용 시, 아래와 같은 송·수신 절차를 이행한다.

① 자체 메일서버를 이용하고, 외부 상용메일을 통한 방위산업기술 자료의 송수신을 금지한다.

② 이메일 관련 보안문제 발견 시 기술보호책임자에게 즉시 보고한다.

③ 송수신 일자 기준 2년 이상 지난 메일은 삭제(필요시 보안 USB에 백업)한다.

④ 기술자료의 이메일 전송을 금한다.

⑤ 사내 메일에서 첨부파일을 전송할 시에는 지정 승인자의 승인을 득한다.

제 6 장 시설 및 장비 보호

제 1 조【 자산의 분류와 분류기준 】

회사는 자산을 분류하고 그 분류에 따라 관리를 달리하여 영업기밀을 보호한다.

① “보안자산”, ”관리자산”으로 분류된 자산(서류 및 자료 등)은 일반자산과 분리하여 별도의 보안장치를 마련하여 특별 관리하도록 한다.

② 각 부서장은 부서 내의 모든 기업비밀을 관리할 의무와 책임을 가진다.

③ 기업 비밀의 성격과 중요도에 따라 사용자의 접근권한을 달리 설정/관리한다.

④ 사용자의 접근 권한은 사용자의 입/퇴사, 계약의 종료, 역할의 변경 등 사유 발생 시 변경 또는 해제될 수 있다.

⑤ “보안자산”, ”관리자산”의 자료와 주요 시설장비 및 자재의 보호를 위해 이를 관리하는 보호구역을 선정할 수 있으며, CCTV와 시건 장치 설치 및 기타 출입 시 필요한 기준과 절차 등을 마련하도록 한다.

⑥ “보안자산”과 “관리자산” 등급의 기업비밀을 사용하거나 반출 시에는 반드시 부서장 및 보안실무책임자의 사전승인을 받는다.

⑦ 보유자산/자료의 백업을 위한 저장장치를 추가하고, 지정장소에서 별도 관리토록 하며, 별도 관리대장으로 관리한다.

⑧ USB 및 외장하드 등 저장장치는 관리번호가 부여된 업무용만 사용 가능하며, 부서별 보안담당자의 책임 하에 이중 시건 장치로서 보관한다.

제 2 조【 물품의 반입/반출 】

회사의 자산 및 물품의 반입/반출 시 관리책임자의 사전허가를 받아야 하며, 물품의 반입/반출 시 발생한 보안 사고의 책임은 사용자와 관리책임자에게 있다.

① PC 및 전산매체 등의 반입/반출 시 사용자는 기기사양, 사용용도, 사용자 정보 등을 작성하고 관리책임자는 이를 직접 확인/보관한다.

② PC, USB, 카메라, 휴대전화 등 저장매체의 반입/반출 시 사용자는 회사 내 사용유무를 포함한 정보 등을 작성하고 관리책임자는 이를 직접 확인/보관한다.

③ 업무용으로 사용중인 PC 및 NOTE PC는 보안담당 부서에서 정기적인 점검을 실시하고, 그 기록을 확인/보관한다.

④ USB 및 외장하드 등의 저장장치는 임직원 개인 소유의 것은 회사내 사용을 금하며, 회사外 업무를 위한 반출 시 보안담당 부서의 허가를 받아 반출/사용하여야 한다.

⑤ USB 및 외장하드 등 저장장치는 보안담당 부서에서 배포/회수를 관리하며, 정기적으로 보안 실시하여 보안사항 위반에 대하여 확인 후 관리대장에 작성/보관한다.

⑥ 보안관리책임자는 회사의 영업비밀 보호를 위해 물품의 반입/반출 시 물품과 사용자를 검열할 수 있다.

제 3 조【 복합기 운용 절차 】

① 복합기 관리자는 제1항에 따라 복합기를 설치・운용할 경우 다음 각 호의 사항을 포함한 보안대책을 수립・시행하여야 한다.

1. 암호화 저장 기능이 있는 경우 해당 기능 사용
2. 정기적으로 저장된 작업 내용(출력・스캔 등) 완전 삭제
3. 공유 저장소 사용 제한 및 접근 제어
4. 고정 IP주소 설정 및 불필요한 서비스 제거
5. 출력물 워터마크 부착
6. 출력물 외부 반입 시 부서장 및 기술보호책임자의 승인 득

② 복합기 관리자는 다음 각 호의 어느 하나에 해당하는 경우 복합기의 저장매체에 저장된 자료를 완전 삭제하여야 한다.

1. 복합기 사용연한이 경과하여 폐기・양여할 경우
2. 복합기 무상 보증기간 중 저장매체 또는 복합기 전체를 교체할 경우
3. 고장 수리를 위한 외부 반출 등의 사유로 해당 기관이 복합기의 저장매체를 통제 관리할 수 없는 장소로 이동할 경우
4. 그 밖에 저장자료의 삭제가 필요하다고 판단되는 경우

④ 복합기 관리자는 소모품 교체 등 복합기 유지보수를 할 경우 부서 기술보호책임자의 입회・감독 하에 실시하고 저장매체의 무단 교체 등을 예방하여야 한다.

⑤ 복합기 관리자는 복합기를 통해 내부망과 기관 인터넷망 간에 접점이 발생하지 않도록 보안대책을 수립・시행하여야 한다.

⑥ 소속된 기관의 저장매체가 장착되어 있는 복합기 운용과 관련한 보안대책의 적절성을 수시 점검・보완하여야 한다.

제 7 장 보안 관리 등

제 1 조【 보안 점검 】

회사는 년 1회 이상 정기적으로 임직원과 각 부서를 대상으로 보안점검을 실시하여야 하며, 필요 시 특정 임직원 및 부서를 선정하여 불시에 점검할 수 있다.

① 보안점검 결과는 최고경영자에게 보고되고, 회사 전체에 공지되어 자체적인 개선 활동이 이루어지도록 한다.

② 보안점검 시 “보안측정 자가진단 체크리스트”를 추가하여 년 1회 이상 확인한다.

제 2 조【 수출제한 국가와의 무역 행위 및 금융거래 금지 】

북한, 이란, 러시아, 콩고민주공화국, 리비아, 시리아, 남수단 등 수출제한 적색국가와의 제품 및 서비스 상호 납품/판매 등 무역 행위 일체 및 금융거래를 금지한다.

제 3 조【 기타 】

본 규정의 미비 또는 누락된 사항은 대한민국 관련 법규 및 관련 규정, 방위산업기술 보호지침, 사규에 의한다.

① 대한민국 관련 법규는 개정 “방위산업기술 보호법”과 그 상위법에 따른다.

② 방위산업기술 보호지침은 개정 “방위사업청훈령”에 따른다.

제 8 장 부 칙

제 1 조【 시행일 】

① 본 규정은 2025년 03월 17일부터 시행한다.

② 개정된 보안서약서는 차기 연봉계약 시 재 작성한다.