

# 생명공학분야 기술보호 가이드 라인





# 생명공학 분야 산업보안협의회 운영 개요

## □ 생명공학 분야 산업보안협의회 발족

- (일시) '21. 3. 25(목) 15:00
- (참석자) 국가정보원 산업기밀보호센터, 산업통상자원부, 한국바이오협회, 생명공학 전문위원회 관계자 및 국가핵심기술 관련 11개 기업 임원진
- (목적) 생명공학 분야 국가핵심기술 보호 및 관련한 현실적인 대책 마련 및 제도 개선을 위해 산업보안협의회 발족
- (주요 내용) 발족식 개최, TF팀 구성 및 향후 협의회 운영방안 논의 등

\* TF팀 구성 결과

구분	목표	참여 기업
TF1팀	국제공통기술문서 등 수출 판단기준 마련	대웅제약, 휴젤, 제테마, 종근당 바이오, 프로톡스, 휴온스글로벌 총 6개사
TF2팀	생명공학 분야 기술 보호 가이드 수립	삼성바이오로직스, 셀트리온, 메디톡스, SK바이오사이언스, 한국비엔씨 총 5개사

## □ 제2차 생명공학 산업보안협의회 회의

- (일시) '21. 6. 24(목) 14:00
- (참석자) 국가정보원 산업기밀보호센터, 산업통상자원부, 한국바이오협회, 생명공학 전문위원회 관계자 및 생명공학 분야 산업보안협의회 11개 기업 임원진, 실무자
- (주요 내용) 진행 상황 및 향후 계획 보고, 추가 참가 기업 가입 여부 결정 등

\* 파마리서치바이오 TF2팀 참여 결정

구분	목표	참여 기업
TF1팀	국제공통기술문서 등 수출 판단기준 마련	대웅제약, 휴젤, 제테마, 종근당 바이오, 프로톡스, 휴온스글로벌 총 6개사
TF2팀	생명공학 분야 기술 보호 가이드 수립	삼성바이오로직스, 셀트리온, 메디톡스, SK바이오사이언스, 한국비엔씨, 파마리서치바이오 총 6개사

□ 실무자 회의 개최

회차	TF1팀		TF2팀	
1	일시	'21.4.8(목) 10:00	일시	'21.4.8(목) 14:00
	주요 내용	TF1팀 구성 및 활동 계획 협의	주요 내용	가이드라인 방향성 및 향후 일정 논의
2	일시	'21.4.27(화) 14:00	일시	'21.5.13(목) 14:00
	주요 내용	국가핵심기술 신청 범위 논의	주요 내용	가이드라인의 세부 주제 선정 및 향후 추진 일정 논의
3	일시	'21.5.13(목) 14:00	일시	'21.6.17(목) 14:00
	주요 내용	국가핵심기술 신청 범위 논의 결과 협의	주요 내용	인력관리 가이드(案) 논의
4	일시	'21.6.17(목) 14:00	일시	'21.7.22(목) 10:00
	주요 내용	파트너사 선정, 검증 방법 논의 및 기술 유출 보호 대책 현황 논의 계획 공유	주요 내용	신규 TF팀 가입사 소개 및 가이드(案) 보완 논의
5	일시	'21.7.22(목) 14:00	일시	'21.8.26(목) 10:00
	주요 내용	국가핵심기술 수출 시스템의 기준 논의	주요 내용	가이드(案) 세부사항 논의 (회원사 별 의견 수렴 등)
6	일시	'21.8.26(목) 14:00	일시	'21.10.5(화) 14:30
	주요 내용	파트너사 선정 프로세스 및 수출 신고 프로세스 논의	주요 내용	가이드(案) 세부사항 논의 (사전 조사 평가지표 체크 등)
7	일시	'21.10.5(화) 9:30	-	
	주요 내용	파트너사 선정 기준 및 기밀 유지 조항 표준화 논의		

□ 2021년도 생명공학 분야 산업보안협의회 성과발표회

- (일시) '21. 11. 4(목) 14:00
- (참석자) 국가정보원 산업기밀보호센터, 산업통상자원부, 한국바이오협회, 생명공학 전문위원회 관계자 및 생명공학 분야 산업보안협의회 12개 기업 임원진, 실무자
- (주요 내용) 산업보안협의회 운영 결과, 생명공학 분야 기술보호 가이드라인 진행 상황 보고 및 최종 의견 수렴 등

# 목 차

## 제1부

### 국가핵심기술의 내용을 포함하는 국제공통기술문서 (Common Technical Document, CTD)의 수출 승인 판단 기준 가이드라인

제1장 개요	3
제1절 배경 및 목적	3
제2절 용어 정의	3
1. 국가핵심기술	3
2. 국가핵심기술 수출 신고/승인	4
3. 중요 변경	4
4. 기밀정보	4
5. WEB을 통해 구현된 시스템	4
제2장 국가핵심기술 수출 신고/승인 절차, 신청 기준 및 요건	5
제1절 국가핵심기술 수출 신고/승인의 절차	5
1. 국가핵심기술 수출 신고	5
2. 국가핵심기술 수출 승인	6
제2절 국가핵심기술 수출 신고/승인 신청 기준	7
1. 신규 신고/승인 신청 기준	7
2. 재신고/재승인 신청 기준	7
제3절 국가핵심기술 수출 신고/승인 신청 요건	9
1. 요건 1: 국가핵심기술 수출 신고서 또는 국가핵심기술 수출 승인 신청서	9
2. 요건 2: 국가핵심기술의 매각 또는 이전 계약서	9
3. 요건 3: 국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항	9
4. 요건 4: 국가핵심기술의 용도와 성능을 표시하는 기술자료	10
5. 요건 5: 국가핵심기술의 제공 조건과 방법	10
6. 요건 6: 국가핵심기술을 사용한 관련 제품의 시장 규모와 경쟁력 수준	10
7. 요건 7: 국가로부터 지원받은 연구개발비에 관한 자료	10

제3장 체크리스트 .....	11
제1절 체크리스트 1 : 국가핵심기술의 매각 또는 이전 계약서에 반영 필요한 표준 문구 .....	11
제2절 체크리스트 2 : 국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항 .....	13
제3절 체크리스트 3 : 국가핵심기술의 용도와 성능을 표시하는 기술자료 .....	16
제4절 체크리스트 4 : 국가핵심기술의 제공 조건과 방법 .....	17
제4장 부록 .....	18
부록 [1] 산업기술의 유출방지 및 보호에 관한 법률 (약칭: 산업기술보호법) .....	18
부록 [2] 산업기술의 유출방지 및 보호에 관한 법률 (약칭: 산업기술보호법) .....	19
부록 [3] 산업기술의 유출방지 및 보호에 관한 법률 시행규칙 (약칭: 산업기술보호법 시행규칙) ..	21
부록 [4] 산업기술의 유출방지 및 보호에 관한 법률 시행령 (약칭: 산업기술보호법 시행령) .....	22
부록 [5] <b>PLEDGE OF CONFIDENTIALITY 기밀유지 서약서</b> .....	<b>23</b>
부록 [6] Checklist for Partnering Verification (파트너사 선정 체크리스트) .....	27

## 제2부

### 국가핵심기술 인력관리 가이드(案)

제1장 총 칙	31
제1조(목적)	31
제2조(적용범위)	31
제2장 인사	31
제3조(사규 준수 의무)	31
제4조(법규 준수 의무)	31
제3장 출입	32
제5조(사업장 출입)	32
제6조(출입 관리)	32
제4장 정보관리	33
제7조(보안등급 분류)	33
제8조(보안등급 별 관리)	34
제5장 네트워크, PC	35
제9조(네트워크 사용)	35
제10조(사외접속)	36
제11조(패스워드 관리)	36
제12조(업무PC 사용)	36
제13조(인터넷, 메일, 메신저, 협업 도구 사용)	37
제14조(이동식 저장매체 사용)	38
제15조(클린데스크)	38
제16조(예외 절차)	38
제6장 업무 수행	39
제17조(출력문서 관리)	39
제18조(업무 회의, 출장)	40
제19조(외부인원 관리)	40

제20조(보안 교육) .....	42
제21조(부서 보안) .....	42
<b>제7장 사고대응 및 상벌</b> .....	<b>46</b>
제22조(보안사고 대응) .....	46
제23조(보안우수자 및 위반자의 조치 및 징계) .....	47
<b>제8장 퇴사</b> .....	<b>48</b>
제24조(퇴사 시 의무) .....	48
[별첨 1] 관련 기관별 역할 .....	49
[별첨 2] 국가핵심기술 등의 비밀유지 및 경업금지 서약서 .....	50
[별첨 3] 비밀유지 서약서 .....	51
[별첨 4] 핵심기술 식별 및 관리 프로세스(예시) .....	53
[별첨 5] 핵심기술정보 Life-Cycle(예시) .....	53
[별첨 6] 핵심기술 유출 실태와 원인분석 .....	54
[별첨 7] 핵심기술 유출 대응 절차(예시) .....	56



# 제1부

국가핵심기술의 내용을 포함하는  
국제공통기술문서  
(Common Technical Document, CTD)의  
수출 승인 판단 기준 가이드라인



# 제1장 개요

## 제1절 배경 및 목적

국가핵심기술 지정 등에 관한 고시 (산업통상자원부 고시 제2021-130호)에 지정된 국가핵심기술의 내용을 포함하는 국제공통기술문서 (Common Technical Document, CTD)의 해외 반출 시에는, 산업통상자원부 (이하, 산자부)의 국가핵심기술 수출 승인이 필요함에 따라, 본 가이드에서는 수출 신고/승인 신청의 기준 및 요건을 제시하고자 한다.

## 제2절 용어 정의

### 1. 국가핵심기술

국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장 잠재력이 높아 해외로 유출될 경우에 국가의 안전 보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술로서 「산업기술의 유출방지 및 보호에 관한 법률」 제9조 <sup>부록</sup> [1]에 따라 지정된 산업기술을 의미한다.

국가핵심기술 지정 등에 관한 고시 (산업통상자원부 고시 제2021-130호, 2021.7.14)에 따르면 생명공학 분야에는 총 4 개의 산업기술이 국가핵심기술로 지정되었다. (표 1-1)

〈표 1-1〉 생명공학 분야의 국가핵심기술

1	항체 대규모 발효정제 기술 (1만 리터급 이상의 동물세포 발현정제 공정기술)
2	보툴리눔 독소제제 생산기술 (보툴리눔 독소를 생산하는 균주 포함)
3	원자현미경 제조기술 (True non-contact mode 기술, Narrow Trench 측정기술, 30nm급 이하 반도체소자 3차원 분석기술, 300mm 이상의 대면적 시료 나노 계측기술, SPM 융합기술)
4	바이오마커 고정화 기술을 응용한 감염질환용 다중 면역 분석 시스템 기술 (3종 이상, 민감도 및 특이도 95% 이상 성능 구현)

## 2. 국가핵심기술 수출 신고/승인

국가핵심기술의 수출은 「산업기술의 유출방지 및 보호에 관한 법률」 제 11조 <sup>부록 2</sup>에 따라, 국가핵심기술 수출 신고 또는 수출 승인의 절차 진행이 필요하다.

관련 상세 절차 및 요건은 산업보안 정보도서관 (<http://www.is-portal.net/tech01>) 및 본 가이드의 2.3항 에서 확인 가능하다.

## 3. 중요 변경

중요 변경은 '생물의약품의 제조방법 변경에 따른 비교동등성 평가 가이드라인 (2019)'의 [별첨] 기준으로 중요로 구분된 변경 중 공정밸리데이션 자료를 요구하는 변경을 의미한다.

발생한 변경 사항의 수준이 불명확한 경우, 글로벌 (미국, 유럽, 캐나다, 등) 변경 가이드라인의 공정 밸리데이션을 요구하는 Major variation의 기준을 참고하여 결정할 수 있다.

## 4. 기밀정보

국가핵심기술과 관련된 정보를 포함한 기밀로 간주되는 모든 형태의 정보를 의미하며, 공개 당사자가 수령 당사자에게 제공한 모든 정보를 의미한다.

## 5. WEB을 통해 구현된 시스템

인터넷 환경에서 웹 표준 기반을 통하여 구현된 시스템을 의미한다.

## 제1절 국가핵심기술 수출 신고/승인의 절차

## 1. 국가핵심기술 수출 신고

수출 주체 (업체)가 「산업기술보호법」 제2조, 동법 시행령 제13조의 2에 따라 국가핵심기술으로 판정된 기술 (관련: 가이드라인 2.2항)을 국가로부터 연구 개발비를 지원받지 않고 개발한 경우, 「산업기술보호법」에 의거 해당 기술의 수출을 아래와 같은 절차를 통해 산업통상자원부 장관에게 신고 해야 한다.

순서	단계	주체	근거 및 참고사항
1	수출 신고	수출 주체 (업체)	<ul style="list-style-type: none"> <li>• 「산업기술보호법」 제11조 및 동법 시행령 제16조</li> <li>• 가이드라인 2.3항</li> </ul>
	↓		
2	접수	산업통상자원부	
	↓		
3	사전조사	정보수사기관	
	↓		
4	심의 1	생명공학분야 산업기술보호 전문위원회	<ul style="list-style-type: none"> <li>• 「산업기술보호법 시행령」 제16조에 따른 수출 신고 사항</li> <li>• 사전조사 결과</li> </ul>
	↓		
5	결과 통보 <sup>1)</sup>	산업통상자원부	<ul style="list-style-type: none"> <li>• 「산업기술보호법 시행령」 제16조</li> </ul>

<sup>1)</sup> 접수일로부터 15일 내에 검토 결과를 서면으로 알리고, 심각한 영향을 줄 수 있다고 판단되는 경우에는 통보일로부터 30일 이내에 관계 중앙행정기관과 협의한 후 위원회 심의를 거쳐 수출 중지, 금지, 원상회복 등의 조치를 명할 수 있음. 다만, 해당 국가핵심기술에 대하여 기술심사 (사전조사, 심의, 등)가 따로 필요한 경우에는 이에 걸리는 일수는 산입하지 아니함

## 2. 국가핵심기술 수출 승인

수출 주체 (업체)가 「산업기술보호법」 제2조, 동법 시행령 제13조의 2에 따라 국가핵심기술으로 판정된 기술 (관련: 가이드라인 2.2항)을 국가로부터 연구 개발비를 지원받아 개발한 경우, 「산업기술보호법」에 의거 아래와 같은 절차를 통해 산업통상자원부 장관으로부터 수출 승인 얻은 후 수출을 진행 해야 한다.

순서	단계	주체	근거 및 참고사항
1	수출 승인 신청	수출 주체 (업체)	<ul style="list-style-type: none"> <li>• 「산업기술보호법」 제11조 및 동법 시행령 제15조</li> <li>• 가이드라인 2.3항</li> </ul>
	↓		
2	접수	산업통상자원부	
	↓		
3	사전조사	정보수사기관	
	↓		
4	심의 1	생명공학분야 산업기술보호 전문위원회	<ul style="list-style-type: none"> <li>• 「산업기술보호법 시행령」 제15조에 따른 수출 승인 사항 검토</li> <li>• 사전조사 결과</li> </ul>
	↓		
5	심의 2	산업기술보호위원회	<ul style="list-style-type: none"> <li>• 「산업기술보호법 시행령」 제15조에 따른 수출 승인 사항 검토</li> <li>• 전문위원회 검토 결과</li> </ul>
	↓		
6	결과 통보 <sup>1), 2)</sup>	산업통상자원부	• 「산업기술보호법 시행령」 제15조

1) 접수일로부터 45일 내에 위원회의 심의를 거쳐 그 결과를 서면으로 알려야 함. 다만, 해당 국가핵심기술에 대하여 기술심사 (사전조사, 심의 등)가 따로 필요한 경우에는 이에 걸리는 일수는 미포함

2) 승인의 유효기간 설정, 수출실적의 제출, 입증서류의 제출 등에 관하여 필요한 조건을 붙일 수 있음

## 제2절 국가핵심기술 수출 신고/승인 신청 기준

### 1. 신규 신고/승인 신청 기준

국가핵심기술의 내용이 포함되는 의약품국제공통기술문서(Common Technical Document, 이하 CTD) 섹션 (Section) (표 2-1)이 해외로 수출되는 경우에는 각 수출 대상 국가와 해외 파트너사 대상으로 국가핵심기술 수출 신고/승인 신청을 진행해야 한다.

〈표 2-1〉 국가핵심기술 수출 신고/승인, 재신고/재승인 신청 대상 CTD 섹션

Common Technical Document		선정 사유
Module 2	Module 3	
2.3.S.2	3.2.S.2.2 Description of Manufacturing Process and Process Controls	제조공정 정보 포함
	3.2.S.2.3 Control of Materials	제조공정에 쓰이는 원료 정보 포함
	3.2.S.2.4 Controls of Critical Steps and Intermediates	제조공정 파라미터 정보 포함
	3.2.S.2.5 Process Validation and/or Evaluation	제조공정 검증 정보 포함
	3.2.S.2.6 Manufacturing Process Development	제조공정 개발 경위 포함
2.3.P.2	3.2.P.2.3 Manufacturing Process Development	제조공정 개발 경위 포함
2.3.P.3	3.2.P.3.2 Batch Formula	완제의 원료약품 및 그 분량 정보 포함
	3.2.P.3.3 Description of Manufacturing Process and Process Controls	제조공정 정보 포함
	3.2.P.3.4 Controls of Critical Steps and Intermediates	제조공정 파라미터 정보 포함
	3.2.P.3.5 Process Validation and/or Evaluation	제조공정 검증 정보 포함
2.3.A.1 <sup>1)</sup>	3.2.A.1 Facilities and Equipment	기기, 도면 정보 포함

<sup>1)</sup> 3.2.A.1의 경우 기기, 설비에 대한 정보로 제조 공정의 직접적인 정보 미포함에 따라 재신고/재승인 대상에서 제외

### 2. 재신고/재승인 신청 기준

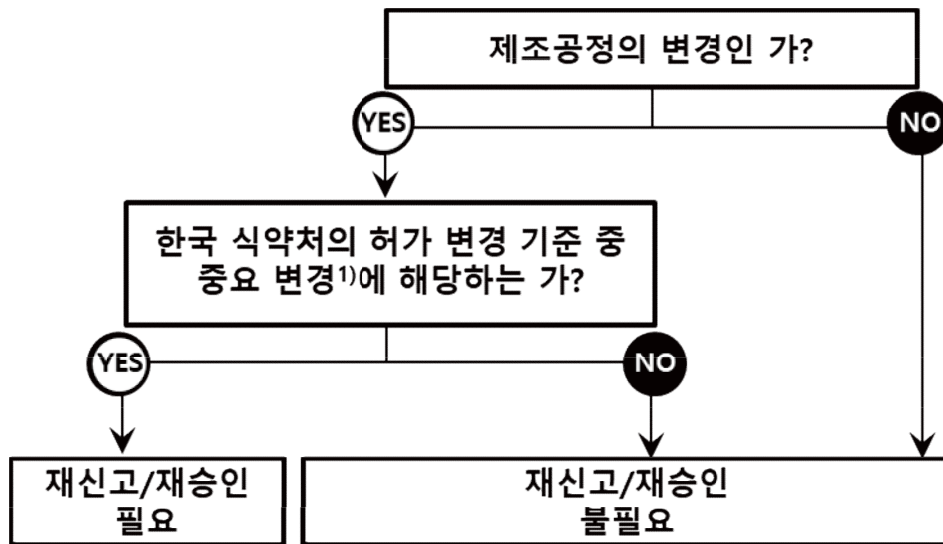
국가핵심기술 수출 신고/승인 이후, 수출 대상 국가 혹은 해외 파트너사의 추가/변경의 경우와 신고/승인 대상 CTD 섹션에 중요 변경이 있는 경우에는 국가핵심기술 수출 재신고/재승인 신청이 필요하다. 신고/승인 대상 CTD 섹션의 중요 변경의 기준은 포함된 내용 중 '생물의약품의 제조방법 변경에 따른 비교동등성 평가 가이드라인 (2019)'의 [별첨] 기준으로 중요로 구분된 변경 내용 중 공정밸리데이션 자료를 요구하는 변경이 제조 공정에 적용되었는지 여부이며, 이는 표 2-2에 요약되어있다.

〈표 2-2〉 국가핵심기술 수출 재신고/재승인 신청 대상

Common Technical Document		재신고/재승인 신청 기준
Module 2	Module 3	
2.3.S.2	3.2.S.2.2 Description of Manufacturing Process and Process Controls	3.2.S.2.2의 변경으로 인한 수정 발생 시
	3.2.S.2.3 Control of Materials	
	3.2.S.2.4 Controls of Critical Steps and Intermediates	
	3.2.S.2.5 Process Validation and/or Evaluation	
	3.2.S.2.6 Manufacturing Process Development	
2.3.P.2	3.2.P.2.3 Manufacturing Process Development	3.2.P.3.3의 변경으로 인한 수정 발생 시
2.3.P.3	3.2.P.3.2 Batch Formula	공정 절차의 중요 변경 <sup>1)</sup> 발생 시
	3.2.P.3.3 Description of Manufacturing Process and Process Controls	
	3.2.P.3.4 Controls of Critical Steps and Intermediates	
	3.2.P.3.5 Process Validation and/or Evaluation	

1) 중요 변경은 '생물의약품의 제조방법 변경에 따른 비교동등성 평가 가이드라인 (2019)'의 [별첨] 기준으로 중요로 구분된 변경 중 공정밸리데이션 자료를 요구하는 변경  
 발생한 변경 사항의 수준이 불명확한 경우, 해외규제기관의 변경규정의 공정밸리데이션을 요구하는 주요변경 (Major variation)의 기준을 참고하여 결정 가능

또한, 재신고/재승인 신청 진행 여부는 그림 2-1의 decision tree에 따라 결정할 수 있다.



1) 중요 변경은 '생물의약품의 제조방법 변경에 따른 비교동등성 평가 가이드라인 (2019)'의 [별첨] 기준으로 중요로 구분된 변경 중 공정밸리데이션 자료를 요구하는 변경  
 발생한 변경 사항의 수준이 불명확한 경우, 해외규제기관의 변경규정의 공정밸리데이션을 요구하는 주요변경 (Major variation)의 기준을 참고하여 결정 가능

〈그림 2-1〉 국가핵심기술 수출 재신고/재승인 신청 decision tree



### 제3절 국가핵심기술 수출 신고/승인 신청 요건

국가핵심기술 수출 신고/승인 신청을 위해서는 산업기술의 유출방지 및 보호에 관한 법률 시행규칙 제2조 <sup>부록 [3]</sup>와 산업기술의 유출방지 및 보호에 관한 법률 시행령 제15조 <sup>부록 [4]</sup>에 따라, 신청서와 첨부서류 (표 2-3) 제출이 필요하다.

〈표 2-3〉 국가핵심기술 수출 신고/승인 신청 요건

번호	요건	상세 정보
1	국가핵심기술 수출 신고서 또는 국가핵심기술 수출 승인 신청서	2.3.1항
2	국가핵심기술의 매각 또는 이전 계약서(임시계약서 포함)	2.3.2항
3	국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항	2.3.3항
4	국가핵심기술의 용도와 성능을 표시하는 기술자료	2.3.4항
5	국가핵심기술의 제공 조건과 방법	2.3.5항
6	국가핵심기술을 사용한 관련 제품의 시장 규모와 경쟁력 수준	2.3.6항
7	국가로부터 지원받은 연구개발비에 관한 자료 <sup>1)</sup>	2.3.7항

1) 국가핵심기술수출 승인 신청의 경우에 한하여 요구되는 요건

각 요건에 포함 필요 사항은 하위 항에 설명되어 있다.

#### 1. 요건 1: 국가핵심기술 수출 신고서 또는 국가핵심기술 수출 승인 신청서

산업보안 정보도서관 사이트의 국가핵심기술- 수출승인 신청·신고 항에서 조회하여 작성 후 제출이 필요하다.

#### 2. 요건 2: 국가핵심기술의 매각 또는 이전 계약서

국가핵심기술의 매각 또는 이전 계약서에는, 3.1항 (**체크리스트 1 : 국가핵심기술의 매각 또는 이전 계약서에 반영 필요한 표준 문구**)에 제시된 보안을 위한 표준 조항을 포함하여 계약을 체결해야 한다.

국가핵심기술 수출 신고/승인 신청, 재신고/재승인 신청 시에는 3.1항에 표준 조항 포함 여부를 표기하여 계약서와 함께 제출해야 한다.

#### 3. 요건 3: 국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항

신규 국가핵심기술의 매입자 또는 이전받으려는 자 (파트너사) 선정 시, 3.2항 (**체크리스트 2 : 국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항**)의 기준을 바탕으로 후보군의 국가핵심기술 취급에 대한 적정성을 판단하여 최종 파트너를 선정한다.

국가핵심기술 수출 신고/승인 신청, 재신고/재승인 신청 시에는 3.2항\*에 파트너사에 관한 정보를 작성하여 제출해야 한다.

\* 예외 사항: 3.2항 중 파악 불가의 정보가 있는 경우, 대체할 수 있는 정보로 파트너사의 신뢰성 검증 결과를 제출할 수 있다.

#### 4. 요건 4: 국가핵심기술의 용도와 성능을 표시하는 기술자료

2.2.1항에 제시된 국가핵심기술 수출을 위한 국가핵심기술 수출 신고/승인 신청, 재신고/재승인 신청 시에는, **3.3항 (체크리스트 3 : 국가핵심기술의 용도와 성능을 표시하는 기술자료)**에 신청하는 문서를 표기하여 해당 기술문서와 함께 제출해야 한다.

#### 5. 요건 5: 국가핵심기술의 제공 조건과 방법

국가핵심기술을 해외에 제공하기 위해서는 아래에 제시된 사항을 고려하여 국가핵심기술 수출을 위한 시스템의 구축이 필수적이다.

〈표 2-4〉 국가핵심기술 해외 수출을 위한 시스템의 조건

번호	요건
1	상호 합의된 파트너사 및 지정된 제3자만 열람할 수 있도록 권한 부여 및 변경/회수 기능 보유
2	제공하는 기술자료의 유출을 대비하여, 기술자료의 열람 현황 및 내역에 대한 추적(Tracking) 기능을 보유
3	기술자료 열람 시, 권한 및 용도에 따라 저장/인쇄 등에 대한 제한 기능 보유

국가핵심기술을 수출을 위한 국가핵심기술 수출 신고/승인 신청, 재신고/재승인 신청 시에는 **3.4항 (체크리스트 4 : 국가핵심기술의 제공 조건과 방법)**에 신청하는 문서를 표기하여 국가핵심기술 제공 조건과 방법에 대한 정보를 제출해야 한다.

#### 6. 요건 6: 국가핵심기술을 사용한 관련 제품의 시장 규모와 경쟁력 수준

국가핵심기술을 수출하고자 하는 국가에 해당 기술의 시장 규모에 대한 정보의 제출이 필요하다.

#### 7. 요건 7: 국가로부터 지원받은 연구개발비에 관한 자료

국가핵심기술 수출 승인 신청에만 요구되는 요건으로, 국가에서 지원받은 연구개발비에 대한 자료 제출이 필요하다.

## 제1 절 체크리스트 1 : 국가핵심기술의 매각 또는 이전 계약서에 반영 필요한 표준 문구

번호	분류	표준 문구	포함 여부	비고 <sup>1)</sup>
1	보안(기밀조항) 조항 : Limited Use	The RECIPIENT may use the CONFIDENTIAL INFORMATION including national core technology only for the PURPOSE during the term of this AGREEMENT, and shall not use it for any other purpose without the DISCLOSER's prior written consent. [파트너 사는 계약기간 동안만 국가핵심기술을 포함한 기밀정보를 사용할 수 있으며, 제공하는 자의 사전서면동의 없이 다른 목적으로 사용해서는 안 된다.]		
2	계약 만료 시 회수/폐기 조항 : Return	Each PARTY acknowledges that all of the CONFIDENTIAL INFORMATION including national core technology shall remain the property of the DISCLOSER. Upon the request by the DISCLOSER, the RECIPIENT shall return to the DISCLOSER or destroy or delete all of the CONFIDENTIAL INFORMATION including its copies and reproduction as well as electronic media, except the RECIPIENT may retain one (1) copy of such CONFIDENTIAL INFORMATION solely for record purposes. [국가핵심기술을 포함한 기밀정보는 제공하는 자의 요청에 따라 제공한 자에게 반환되거나 복사 및 복제를 포함한 모든 기밀정보 (전자매체 포함)를 파기 또는 삭제해야 한다. 단, 수신자는 기록 목적으로만 기밀정보의 사본 1부를 유지할 수 있다.]		
3	국가핵심기술 취급 담당자에 대한 개인별 보안서약서 조항	아래의 기준을 바탕으로, 회원사별로 법무팀 검토 후 파트너사 개인별 서약서 징구 1) 원칙: 국가핵심기술 관련 문서를 취급하는 모든 인원들로부터, 기밀유지에 대한 서명 수령 <sup>2)</sup> 2) 원칙: 개인별 보안서약서에 별첨 (Appendix)로 국가핵심기술 관련 문서를 취급하는 모든 인원의 이름, 직책 등 정보를 기재하고/추가적으로 업데이트하여 관리하거나 대표자 서명으로 대체 가능		

번호	분류	표준 문구	포함 여부	비고 <sup>1)</sup>
4	보안 위반시 행동 조항: Remedies	<p>Each party understand and acknowledge that any disclosure or misappropriation of any of the CONFIDENTIAL INFORMATION in violation of this AGREEMENT may cause the DISCLOSER irreparable harm, the amount of which may be difficult to ascertain and, therefore, agrees that the DISCLOSER shall have the right to apply to a court of competent jurisdiction for an order restraining any such further disclosure or misappropriation and for such other relief as the DISCLOSER deems appropriate. Such right of the DISCLOSER shall be exercisable in addition to the remedied otherwise available to the DISCLOSER at law or in equity</p> <p>[각 당사자는 본 계약을 위반하여 기밀정보의 공개 또는 남용이 제공한 자에게 피해를 줄 수 있음을 이해하고 인정하며, 그 금액은 확인이 어렵기 때문에, 공개자가 민.형사상의 책임을 청구할 수 있으며, 제공한 자가 추가공개 또는 남용을 금지하는 명령과 적절하다고 판단하는 구제를 관할법원에 신청할 수 있음에 동의한다.]</p>		

1) 위의 표준 문구의 의미를 포함하는 대체 문구로도 활용할 수 있으나 해당 내용에 대해서는 비교에 기술하여 전문위에서 소명 필요

2) 4항 부록 [5]의 예시를 회사 및 국가의 현황에 맞춰 활용 가능

## 제2절

### 체크리스트 2 : 국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항

항목	조사 예시번호	확인 결과 <sup>1)</sup>	비고 <sup>2)</sup>
1) 회사소개서를 통한 재무 건정성/신용도 조사			
- 조사 항목			
1	회사연혁	<ul style="list-style-type: none"> <li>• 설립연도 확인</li> <li>• 그룹계열사 분사 확인</li> </ul>	
2	재무 건정성 (매출액)	<ul style="list-style-type: none"> <li>• 3~5년 매출 안정성 및 성장률 확인</li> <li>• IR 자료확인 가능한 경우 확인</li> </ul>	
3	사업경험	<ul style="list-style-type: none"> <li>• 에스테틱 사업 (필러, 화장품 등) 경험 유무 확인 (년수는 참고)</li> <li>• 현지 네트워크 보유현황 확인</li> <li>• 시장 이해도 확인 (시장규모, 경쟁사 현황 등)</li> <li>• 국내외 기업과의 거래 이력</li> </ul>	
4	대표자	<ul style="list-style-type: none"> <li>• 대표자 이름</li> <li>• 연혁 확인</li> </ul>	
5	직원 수	<ul style="list-style-type: none"> <li>• 에스테틱 사업 영업 활용 인원 확인 (기능/업무별 조직 인원 구성 여부 확인)</li> </ul>	
6	사업자등록증 유무	<ul style="list-style-type: none"> <li>• 사업자등록증 확인</li> </ul>	
7	신용도 조사	<ul style="list-style-type: none"> <li>• 제3의 신용기관 신용조사를 통해 확인 (예시: 한국무역보험공사 기준 신용등급 확인 (보험가능 등급 이상))</li> </ul>	
- 선정 제외 고려사항			
1	신용등급 문제 이력 보유 여부 현지 코트라를 통한 평판 및	<ul style="list-style-type: none"> <li>• 보험 가입 불가</li> </ul>	
2	정보 확인 결과 범법 행위 이력 보유 여부	<ul style="list-style-type: none"> <li>• 불법 행위, 파산 등 대표 또는 회사의 범법행위</li> </ul>	
3	요청사항에 대해 특별한 사유없이 비협조적인지 여부	<ul style="list-style-type: none"> <li>• 재무 관련 자료, 회사연혁, 매출 관련, 회사 사업 현황 등</li> </ul>	

항목	조사 예시번호	확인 결과 <sup>1)</sup>	비고 <sup>2)</sup>
<b>2) 보안계약서 체결 (CDA 체결 必)</b>			
<b>- 조사 항목</b>			
1	계약서 체결진행 (CDA)	• 국가핵심기술 기밀유지 내용이 포함된 CDA 체결	
<b>3) 제약 또는 관련산업(에스테틱) 제품 인허가 역량 확인</b>			
<b>- 조사 항목</b>			
1	해외 제약제품/에스테틱 제품 인허가 경험 보유 여부	<ul style="list-style-type: none"> <li>• 의약품 및 에스테틱 인허가 경험 확인</li> <li>• 허가 절차에 대한 이해도 검증 필요</li> </ul>	
2	자체 허가팀 또는 CRO (대행업체) 보유 여부	<ul style="list-style-type: none"> <li>• 자체 인허가 조직 보유</li> <li>• CRO 소개서 및 홈페이지 확인</li> <li>• CRO의 임상/허가 진행 이력 확인</li> </ul>	
<b>- 선정 제외 고려사항</b>			
1	RA 인허가 역량 미보유	<ul style="list-style-type: none"> <li>• 허가 관련 지식, 경험, 자원, 규제기관과의 관계가 부족하지 확인</li> <li>• 내부역량 부족시, 외부의 자원을 통해 보완하여 예외적으로 확인 및 진행</li> </ul>	
<b>4) 우려 국가/기업 여부 확인</b>			
<b>- 조사 항목</b>			
1	기존 우려 국가/업체에 대한 정보 파악	• 우려 국가/ 업체에 대한 정보 파악	
<b>- 선정 제외 고려사항</b>			
1	우려 업체 여부 확인 (보안의 이슈, 이전 경험이나 기타 사유로 국가핵심기술의 공유가 어렵다고 판단/확인되는 기업)	<ul style="list-style-type: none"> <li>• 국가의 정치적, 경제적 상황에 대한 불투명한 부분 등을 서신 등으로 확인/소명</li> <li>• 미국 상무부 제재국가에 포함되는지 참고하여 의사결정에 활용</li> </ul>	

항목	조사 예시번호	확인 결과 <sup>1)</sup>	비고 <sup>2)</sup>
<b>5) 파트너사 생산시설 보유 유무</b>			
<b>- 조사 항목</b>			
1	생산시설 보유 여부	<ul style="list-style-type: none"> <li>• 거래사의 생산시설 보유 여부 확인</li> <li>• 생산시설 보유 시, 생산 가능 제품 확인</li> </ul>	
<b>- 선정 제외 고려사항</b>			
1	생산시설 보유 및 경력/계획	• 국가핵심기술을 이용한 생산 계획이 있거나 생산 경험 있는 거래자	
<b>6) 국가핵심기술 취급 파트너/CRO 계열사 현황 확인 (상기 내용에 대해, 더블체크)</b>			
<b>- 조사 항목</b>			
1	국가핵심기술 취급 파트너/CRO 계열사 현황 확인	<ul style="list-style-type: none"> <li>• 파트너사 및 CRO (해당하는 계열사)에 대한 회사소개서 요청</li> <li>• 파트너사에서 맺은 CRO의 계약서 (기 체결한 경우 해당하며, 비밀유지조항/영업비밀 부분에 대한 공유 필수)</li> </ul>	

1) 파트너사 검증 시, 4항 부록 [6]의 예시를 활용하여 조사 진행 가능

2) 위의 각 항목을 확인할 때, 대체 가능한 정보를 활용하여서도 소명 가능하나 해당 내용에 대해서는 비교에 기술하여 전문위에서 소명 필요

### 제3절

## 체크리스트 3 : 국가핵심기술의 용도와 성능을 표시하는 기술자료

번호	국가핵심기술 (Common Technical Document)	신청 여부	비고
1	2.3.S.2.2 Description of Manufacturing Process and Process Controls		
2	2.3.S.2.3 Control of Materials		
3	2.3.S.2.4 Controls of Critical Steps and Intermediates		
4	2.3.S.2.5 Process Validation and/or Evaluation		
5	2.3.S.2.6 Manufacturing Process Development		
6	2.3.P.2.3 Manufacturing Process Development		
7	2.3.P.3.2 Batch Formula		
8	2.3.P.3.3 Description of Manufacturing Process and Process Controls		
9	2.3.P.3.4 Controls of Critical Steps and Intermediates		
10	2.3.P.3.5 Process Validation and/or Evaluation		
11	2.3.A.1 Facilities and Equipment		
12	3.2.S.2.2 Description of Manufacturing Process and Process Controls		
13	3.2.S.2.3 Control of Materials		
14	3.2.S.2.4 Controls of Critical Steps and Intermediates		
15	3.2.S.2.5 Process Validation and/or Evaluation		
16	3.2.S.2.6 Manufacturing Process Development		
17	3.2.P.2.3 Manufacturing Process Development		
18	3.2.P.3.2 Batch Formula		
19	3.2.P.3.3 Description of Manufacturing Process and Process Controls		
20	3.2.P.3.4 Controls of Critical Steps and Intermediates		
21	3.2.P.3.5 Process Validation and/or Evaluation		
22	3.2.A.1 Facilities and Equipment		



## 제4절 체크리스트 4 : 국가핵심기술의 제공 조건과 방법

번호	확인 필요 항목	확인 결과	비고 <sup>1)</sup>
<b>제공 조건</b>			
1	국가핵심기술정보를 다루는 사용자 PC에 대한 적절한 보안 조치 여부 (사용자의 모든 행위는 기록되어 추후 확인될 수 있어야 함)		
2	국가핵심기술을 제공 주체와 보안에 대한 계약 체결 여부 (2.2.1항 중 보안에 대한 계약 체결 필요)		
<b>국가핵심기술 제공 방법: 국가핵심기술의 반출 시, 보안 유지를 위해 사용되는 시스템 정보</b>			
1	시스템이 WEB을 통하여 구현되었는지 여부		
2	시스템의 문건을 전달받는 사용자의 계정 권한에 대한 통제 가능 여부 (예시: 문서에 대한 접근권한, 조회, 다운로드 등)		
3	시스템 사용자의 행위가 기록되어 추후 확인 가능한지 여부 (예시: 문서에 대한 접근권한, 조회, 다운로드 등)		

1) 위의 각 항목을 확인할 때, 대체 가능한 정보를 활용하여서도 소명 가능하나 해당 내용에 대해서는 비교에 기술하여 전문위에서 소명 필요

부록 [1]

산업기술의 유출방지 및 보호에 관한 법률 (약칭: 산업기술보호법)

[시행 2021. 4. 1.] [법률 제17163호, 2020. 3. 31., 타법개정]

- 제9조 (국가핵심기술의 지정·변경 및 해제 등)** ①산업통상자원부장관은 국가핵심기술로 지정되어야 할 대상기술(이하 이 조에서 “지정대상기술”이라 한다)을 선정하거나 관계 중앙행정기관의 장으로부터 그 소관의 지정대상기술을 선정·통보받은 경우에는 위원회의 심의를 거쳐 국가핵심기술로 지정할 수 있다. 이 경우 산업통상자원부장관이 선정한 지정대상기술이 다른 중앙행정기관의 장의 소관인 경우에는 위원회 심의 전에 해당 중앙행정기관의 장과 협의를 거쳐야 한다. <개정 2008. 2. 29., 2013. 3. 23., 2015. 1. 28.>
- ②산업통상자원부장관 및 관계 중앙행정기관의 장은 지정대상기술을 선정함에 있어서 해당기술이 국가안보 및 국민경제에 미치는 파급효과, 관련 제품의 국내외 시장점유율, 해당 분야의 연구동향 및 기술 확산과의 조화 등을 종합적으로 고려하여 필요최소한의 범위 안에서 선정하여야 한다. <개정 2015. 1. 28.>
- ③산업통상자원부장관은 국가핵심기술의 범위 또는 내용의 변경이나 지정의 해제가 필요하다고 인정되는 기술을 선정하거나 관계 중앙행정기관의 장으로부터 그 소관의 국가핵심기술의 범위 또는 내용의 변경이나 지정의 해제를 요청받은 경우에는 위원회의 심의를 거쳐 변경 또는 해제할 수 있다. 이 경우 산업통상자원부장관이 선정한 기술이 다른 중앙행정기관의 장의 소관인 경우에는 위원회 심의 전에 해당 중앙행정기관의 장과 협의를 거쳐야 한다. <개정 2008. 2. 29., 2013. 3. 23., 2015. 1. 28.>
- ④산업통상자원부장관은 제1항의 규정에 따라 국가핵심기술을 지정하거나 제3항의 규정에 따라 국가핵심기술의 범위 또는 내용을 변경 또는 지정을 해제한 경우에는 이를 고시하여야 한다. <개정 2008. 2. 29., 2013. 3. 23.>
- ⑤위원회는 제1항 및 제3항의 규정에 따라 국가핵심기술의 지정·변경 또는 해제에 대한 심의를 함에 있어서 지정대상기술을 보유·관리하는 기업 등 이해관계인의 요청이 있는 경우에는 대통령령이 정하는 바에 따라 의견을 진술할 기회를 주어야 한다.
- ⑥ 대상기관은 해당 기관이 보유하고 있는 기술이 국가핵심기술에 해당하는지에 대한 판정을 대통령령으로 정하는 바에 따라 산업통상자원부장관에게 신청할 수 있다. <신설 2011. 7. 25., 2013. 3. 23.>
- ⑦제1항 및 제3항의 규정에 따른 국가핵심기술의 지정·변경 및 해제의 기준·절차 그 밖에 필요한 사항은 대통령령으로 정한다. <개정 2011. 7. 25.>

## 부록 [2]

### 산업기술의 유출방지 및 보호에 관한 법률 (약칭: 산업기술보호법)

[시행 2021. 4. 1.] [법률 제17163호, 2020. 3. 31., 타법개정]

**제11조(국가핵심기술의 수출 등)** ①국가로부터 연구개발비를 지원받아 개발한 국가핵심기술을 보유한 대상기관이 해당국가핵심기술을 외국기업 등에 매각 또는 이전 등의 방법으로 수출(이하 “국가핵심기술의 수출”이라 한다)하고자 하는 경우에는 산업통상자원부장관의 승인을 얻어야 한다. <개정 2008. 2. 29., 2013. 3. 23.>

②산업통상자원부장관은 제1항의 규정에 따른 승인신청에 대하여 국가핵심기술의 수출에 따른 국가안보 및 국민경제적 파급효과 등을 검토하여 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 승인할 수 있다. <개정 2008. 2. 29., 2013. 3. 23.>

③제1항의 규정에 따라 승인을 얻은 국가핵심기술이 「대외무역법」 제19조제1항의 기술인 경우에는 같은 조 제2항에 따라 허가를 받은 것으로 보며, 「국방과학기술혁신 촉진법」 제2조제2호에 따른 국방과학기술 및 「방위사업법」 제34조에 따른 방산물자인 경우에는 「방위사업법」 제57조제2항에 따라 허가를 받은 것으로 본다. 이 경우 산업통상자원부장관은 사전에 관계중앙행정기관의 장과 협의를 하여야 한다. <개정 2008. 2. 29., 2011. 7. 25., 2013. 3. 23., 2020. 3. 31.>

④제1항의 규정에 따른 승인대상 외의 국가핵심기술을 보유·관리하고 있는 대상기관이 국가핵심기술의 수출을 하고자 하는 경우에는 산업통상자원부장관에게 사전에 신고를 하여야 한다. <개정 2008. 2. 29., 2013. 3. 23.>

⑤산업통상자원부장관은 제4항의 신고대상인 국가핵심기술의 수출이 국가안보에 심각한 영향을 줄 수 있다고 판단하는 경우에는 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 국가핵심기술의 수출중지·수출금지·원상회복 등의 조치를 명할 수 있다. <개정 2008. 2. 29., 2013. 3. 23.>

⑥제4항의 신고대상 국가핵심기술의 수출을 하고자 하는 자는 해당국가핵심기술이 국가안보와 관련되는지 여부에 대하여 산업통상자원부장관에게 사전검토를 신청할 수 있다. <개정 2008. 2. 29., 2013. 3. 23.>

⑦산업통상자원부장관은 국가핵심기술을 보유한 대상기관이 제1항의 규정에 따른 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술의 수출을 한 경우 또는 제4항의 규정에 따른 신고대상 국가핵심기술을 신고하지 아니하거나 허위로 신고하고 국가핵심기술의 수출을 한 경우에는 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 위원회에 보고한 후 위원회의 심의를 거쳐 해당국가핵심기술의 수출중지·수출금지·원상회복 등의 조치를 명령할 수 있다. <개정 2008. 2. 29., 2013. 3. 23.>

⑧위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대상기관의 의견을 청취할 수 있다.

1. 제2항의 규정에 따른 승인신청에 대한 심의
2. 제5항의 규정에 따른 국가안보에 심각한 영향을 주는 국가핵심기술의 수출중지·수출금지·원상회복 심의

3. 제7항의 규정에 따른 미승인 또는 부정승인 및 미신고 또는 허위신고 등에 대한 국가핵심기술의 수출중지·수출금지·원상회복 심의

⑨산업통상자원부장관은 제1항의 규정에 따른 승인 또는 제4항의 규정에 따른 신고와 관련하여 분야별 전문위원회로 하여금 검토하게 할 수 있으며 관계중앙행정기관의 장 또는 대상기관의 장에게 자료제출 등의 필요한 협조를 요청할 수 있다. 이 경우 관계 중앙행정기관의 장 및 대상기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다. <개정 2008. 2. 29., 2013. 3. 23.>

⑩제1항의 승인, 제4항의 신고, 제5항 및 제7항의 수출중지·수출금지·원상회복 등의 조치 및 절차 등에 관하여 세부적인 사항은 대통령령으로 정한다.

⑪제6항의 규정에 따른 국가핵심기술이 국가안보와 관련되는지 여부에 대한 사전검토의 신청에 관하여 필요한 사항은 대통령령으로 정한다.

**부록 [3]**

**산업기술의 유출방지 및 보호에 관한 법률 시행규칙 (약칭: 산업기술보호법 시행규칙)**

[시행 2020. 2. 21.] [산업통상자원부령 제361호, 2020. 2. 21., 일부개정]

**제2조(국가핵심기술 수출승인신청서)** 산업기술의 유출방지 및 보호에 관한 법률 시행령 제15조제1항에 따른 국가핵심기술 수출승인신청서는 별지 제2호서식에 따른다. 〈개정 2012. 1. 25.〉

## 부록 [4]

### 산업기술의 유출방지 및 보호에 관한 법률 시행령 (약칭: 산업기술보호법 시행령)

[시행 2021. 1. 5.] [대통령령 제31380호, 2021. 1. 5., 타법개정]

**제15조(국가핵심기술의 수출승인 신청 등)** ①법 제11조제1항에 따라 국가핵심기술의 수출을 승인받으려는 대상기관은 산업통상자원부령으로 정하는 국가핵심기술 수출승인신청서에 다음 각 호의 서류를 첨부하여 산업통상자원부장관에게 제출하여야 한다. <개정 2008. 2. 29., 2013. 3. 23.>

1. 국가핵심기술의 매각 또는 이전 계약서(임시계약서를 포함한다)
2. 국가핵심기술의 매입자 또는 이전받으려는 자에 관한 사항
3. 국가핵심기술의 용도와 성능을 표시하는 기술자료
4. 국가핵심기술의 제공 조건과 방법
5. 국가핵심기술을 사용한 관련 제품의 시장 규모와 경쟁력 수준
6. 국가로부터 지원받은 연구개발비에 관한 자료

②제1항에 따른 신청을 받은 산업통상자원부장관은 접수일부터 45일 이내에 관계 중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 그 결과를 신청인에게 서면(전자문서를 포함한다)으로 알려야 한다. 다만, 승인을 신청한 국가핵심기술에 대하여 기술심사가 따로 필요한 경우에는 이에 걸리는 일수(日數)는 본문에 따른 기간에 산입(算入)하지 아니한다. <개정 2008. 2. 29., 2013. 3. 23., 2015. 4. 28.>

③산업통상자원부장관은 법 제11조제2항에 따라 승인할 때에는 승인의 유효기한 설정, 수출실적의 제출, 입증서류의 제출 등에 관하여 필요한 조건을 붙일 수 있다. <개정 2008. 2. 29., 2013. 3. 23.>

## 부록 [5]

※ 아래의 양식은 한국의 산업기술의 유출방지 및 보호에 관한 법률(산업기술보호법)에 의거하여 국가핵심기술로 지정한 기술을 엄격히 기밀로 보호하고 유출을 예방하기 위하여 기업의 차원을 넘어서 국가핵심기술 정보를 다루는 개개인을 대상으로 책임과 의무 이행 및 약속을 확약 받는 “기밀유지 서약서”이다. 다만, 문서의 성격상 개인을 식별할 수 있는 민감한 개인정보를 포함하고기 때문에 이는 개인정보와 관련한 국가별 법/제도적 상황과 국/내외 회사 내규 등의 입장을 고려하여 수정하거나 다른 방법으로 대체될 수 있다.  
(예시 항목: 개인정보 처리 주체인 소속 회사 연락처, 개인정보의 해외 이전 사실·이전의 적정성, 보호 수단 정보 제공, 정보주체의 개인정보 접근권, 정보주체의 개인정보에 대한 정정 및 삭제권·반대권, 프로파일링 등 자동화된 의사결정의 대상이 되지 않을 권리 등)

- 아 래 -

## PLEDGE OF CONFIDENTIALITY

### 기밀 유지 서약서

Name 성명	
Company 소속 회사	
Department/Position 소속부서/지위	
Contact (Email/Phone number) 연락처 (이메일/전화번호)	

I hereby pledge my observance of the below obligations when carrying out any work related to “00000 Project” (hereinafter referred to as “Target Project”).

본인은 “00000사업” (이하 “목적사업”)에 관한 업무를 수행함에 있어 다음 사항을 준수할 것을 서약한다.

This “Pledge of Confidentiality”(hereinafter referred to as “Pledge”) becomes effective on MM DD, YYYY (hereinafter referred to as the “Effective Date”)

본 “기밀 유지계약 서약서”(이하 “서약서”)는 0000년 00월 00일 (이하 효력 일자)로부터 유효하다.

1. I acknowledge and agree that, in connection with my participation in the Target Project, I may acquire, use and become aware of all of the below information provided for carrying out the work related to the Target Project (hereinafter “Confidential Information”), and acknowledge that it is confidential and proprietary information of which security must be maintained during the execution of the Target Project and even after the Target Project is terminated.

본인은 목적사업에 관한 업무의 수행을 위하여 제공되는 하기의 모든 정보(이하 “기밀정보”)를 획득, 사용 및 숙지하고, 목적사업 수행 중이나 목적사업 종료 후에도 보안을 유지해야 하는 기밀임을 인정한다.

- a) I acknowledge and agree that Confidential Information refers to all types of information provided by written, oral, electronic transmission or other methods, irrespective of its intangibility and recording type, which includes, without limitation, know-how, technology, process, drawings, designs, blueprints, ideas, specification, data, business information and management information with respect to the Target Project, and any information defined as Confidential Information under the mutual confidentiality agreement between the employer company and 0000 (소속회사 Full name). (hereinafter "0000 (소속 회사 줄임 명칭)").

본인은 기밀정보가 목적사업과 관련하여 서면, 구두, 전자적 방법에 의한 전송 또는 기타의 방법으로 제공하는 모든 노하우, 기술, 공정, 도면, 설계, 디자인, 아이디어, 사업정보, 경영정보 등 일체의 정보, 또는 0000 (소속회사)와/과 고용인 사이에 체결한 비밀유지계약서상 정의한 기밀정보로서 유·무형의 여부 및 그 기록 형태를 불문한다는 것을 인정하고 동의한다.

- b) I acknowledge and agree that reports and outputs produced using Confidential Information during the execution of the Target Project are also included in Confidential Information.

본인은 목적사업을 수행하는 중 기밀정보를 이용하여 생산되는 보고서 및 산출물도 기밀정보에 포함된다는 것을 인정하고 동의한다.

- c) I acknowledge and agree that among Confidential Information, certain types of information (Common Technical Document CTD, etc.) related to the production technology of botulinum toxin preparations including strains that produce botulinum toxin is designated as an important national core technology pursuant to the Korean Act on Prevention of Divulgence and Protection of Industrial Technology (hereinafter "National Technology Protection Act"), as it is regarded as an important industrial technology by the Ministry of Trade, Industry and Energy of the Republic of Korea. Confidential Information of the national core technology is an important matter for the Target Project and the Republic of Korea, and all applicable security regulations must be complied with regardless of time and place.

본인은 본 기밀정보 가운데 보툴리눔 독소를 생산하는 균주를 포함하는 보툴리눔 독소 제제 생산기술과 관련된 특정 정보(국제공통기술문서 CTD 등)는 대한민국의 산업통상자원부에서 중요한 산업기술로서 한국의 산업기술의 유출방지 및 보호에 관한 법률 (이하 “산업기술보호법”)에 의거하여 국가핵심기술로 지정하고 있는 것을 인정하고 동의한다. 해당 국가핵심기술의 기밀정보는 목적사업



및 대한민국 국가의 중요한 사항이며 시간과 장소에 구애됨이 없이 제반 보안규정을 준수해야 한다.

2. I agree to keep Confidential Information strictly not to use for any purpose, unless otherwise provided herein, and to access to Confidential Information during the execution of the Target Project or even after the Target Project is terminated.

본인은 기밀정보를 엄격하게 기밀로 유지하고 여기 달리 규정하지 않는 한 어떤 목적으로도 사용하지 않으며, 목적사업 수행 중이나 목적사업 종료 후에도 기밀 유지, 사용금지 및 기밀정보 접근의 관리에 대한 책임과 의무가 있다.

3. I agree not to leak, divulge, or disclose Confidential Information to any third party other than for the mutually agreed business purpose during the execution of the Target Project.

본인은 목적사업을 수행하는 동안 협의된 업무 목적 이외에 어떠한 제3자에게도 기밀정보를 유출, 누설하거나 공개하지 아니한다.

4. I agree and acknowledge that any unauthorized disclosure or divulgence of Confidential Information to a third party intentionally or negligently without prior written consent shall constitute a breach of this Agreement and may result in a violation of the National Technology Protection Act.

본인은 공개당사자의 사전 서면 동의 없이 기밀정보를 고의 또는 과실로 제3자에게 공개, 제공 또는 누설한 경우 본 계약 위반에 해당하고, 나아가 산업기술보호법에 저촉될 수 있음을 인정한다.

5. I pledge to accept any punishment or disadvantage including legal liability arising out of or in connection with the breach of this confidentiality pledge and violation of the National Technology Protection Act.

본인은 본 계약 위반 및 산업기술보호법 위반으로 인하거나 관련하여 발생하는 모든 손해에 대하여 책임을 지고, 법적 책임을 포함하여 어떠한 처벌 및 불이익도 감수할 것을 서약한다.

6. I hereby consent to 0000(소속회사) retaining and using my personal information only for the Target Project during the period of maintaining confidentiality and security on the premise that I can withdraw my consent freely at any time.

본인은 개인정보의 수집 및 이용에 대한 동의를 언제든지 자유롭게 철회할 수 있음을 전제로 0000(소속 회사)이/가 기밀보안 유지 기간 동안 오직 목적사업을 위하여 본인의 개인정보를 보유하고 이용하는 것에 동의한다.

수집 개인정보 항목 (personal information items to be collected)	수집·이용 목적 (Purpose of Collection and Use)	개인정보의 보유 및 이용기간 (Retention and use period of personal information)
성명, 소속회사, 소속부서, 직위, 연락처(이메일, 전화번호) Name, Company, Department, Position, Contact (Email, Phone number)	목적사업 관련 계약 체결, 기밀정보 제공, 본 협약서에 서명한 모든 협약 실무자에게 공지사항 전달 Conclusion of a contract related to the Target Project, Provision of Confidential Information, Notification to anyone who signed this Pledge convention practitioner-	본 계약 효력 일자부터 목적사업의 비밀유지기간 종료 일자 까지 From the Effective Date of this Pledge to the end of the confidentiality period of the Target Project

7. I acknowledge and agree that I have read this Pledge carefully and pledge observation hereof faithfully.

본인은 본 서약서를 상세히 읽어 보았음을 확인하고, 이를 성실히 준수할 것을 서약한다.

MM/DD/YYYY

DATE

Name

Signature

## 부록 [6] Checklist for Partnering Verification

### 파트너사 선정 체크리스트

※ 아래의 양식은 한국의 산업기술의 유출방지 및 보호에 관한 법률(산업기술보호법)에 의거하여 국가핵심기술로 지정한 기술을 수출할 파트너사의 신뢰성 검토용 조사 항목 예시이다. 본 가이드라인 3.2항의 조사를 진행할 때, 국/내외 회사 내규 등의 입장을 고려하여 수정하여 활용하거나 대체될 수 있다.

- 아 래 -

Checklist for Partnering Verification			
<b>1. General information</b>			
1-1.	Name of Company	.	
1-2.	Country	.	
1-3.	Name of Representative	.	
1-4.	Main shareholder/shareholder of the Company	.	
1-5.	Sales Volume of the Company	.	
1-6.	1-6-1.	Total number of employee	.
	1-6-2.	The number of employees in the R&D department	.
1-7.	Main product of the company	.	
1-8.	Possession of main/key technology (e.g. Manufacturing, sales, or Regulatory service)	.	
1-9.	Responsible team who receipts the CTD* (* Common Technical Document)	.	
1-10.	Overseas/Domestic offices or Subsidiary company	.	
1-11.	Level of credibility	.	
1-12.	Business partnership with Domestic/Foreign companies	.	
1-13.	Business license or Certificate issued from the country	.	
※ Please provide information for 1-1 to 1-13.			
1-14.	Official name of the national MOH and its abbreviation (e.g.; Ministry of Food and Drug Safety of Republic of Korea, MFDS)	.	
1-15.	Do you have any product registered and marketed in your country? If yes, please provide the relevant classification of product. (e.g.; Biologicals)	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:	
1-16.	Does your company have a Regulatory Affairs team? If yes, please provide the information of personnel in charge.	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:	
1-17.	Does your company have a contract with any related	<input type="checkbox"/> Yes /Comment:	

**Checklist for Partnering Verification**

	agency (e.g., CRO(Contract Research Organization, testing institutes) for handling technical document?	<input type="checkbox"/> No /Comment:
1-17-1.	If you have a contract with the agency, have you signed a Confidentiality Agreement with the agency?	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:
1-17-2.	If you have a contract with the agency, please provide information for 1-1 to 1-13.	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:

**2. Production line confirmation**

2-1.	Do you have any production line for manufacturing product for human uses? If yes, please provide the brief information. (e.g.; Injection)	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:
2-2.	Have you produced any toxin product before in your manufacturer?	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:
2-3.	Do you have any plan for manufacturing toxin product in your manufacturer?	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:

**3. Confidential information and Security**

3-1.	Under the governing law in Korea, the information of botulinum toxin including strain has been designated as a "National Core Technology". Accordingly, do you agree to be provided after being reviewed and approved by MOTIE* ? (*Ministry of Trade, Industry, and Energy)	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:
3-2.	Do you check and understand the terms of the Confidentiality Agreement?	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:
3-3.	Do you agree to apply the COMPANY's internal security system to deliver the document, if necessary?	<input type="checkbox"/> Yes /Comment: <input type="checkbox"/> No /Comment:

Date:

\_\_\_\_\_

Name/ Position

\_\_\_\_\_

Signature:

\_\_\_\_\_

# 제2부

국가핵심기술 인력관리 가이드(案)



## 제1장 총 칙

### 제1조(목적)

본 '국가핵심기술 인력관리 가이드'는 국가핵심기술 보유 기업의 사업 경쟁력 확보 및 강화를 위하여 준수해야 하는 기본 원칙을 구성되었으며 필요시 현장 보안 업무 수행을 위한 참고 가이드를 활용하는데 목적이 있다.

### 제2조(적용 범위)

국가핵심기술보호 범위는 핵심기술 및 인력 분류 및 정의 → 보호조치 → 실태점검 등 전 단계에서 수행 중 혹은 그 결과로 도출된 결과물을 보호하고 유출을 방지하는 제반 활동 전체를 의미한다. 생명공학분야 국가핵심기술 보유 기업에서 진행되는 기술 보호 활동 및 조치를 위해서 본 가이드의 내용을 참고해야 한다.

## 제2장 입사

### 제3조(사규 준수 의무)

국가핵심기술에 대한 보호 등급의 부여와 보안관리 규정을 제정하고 준수하여야 한다.

1. 국가핵심기술 관리책임자 및 보안 전담 인력의 지정
2. 국가핵심기술 보호구역의 통신시설과 통신수단에 대한 보안
3. 국가핵심기술 관련 정보의 처리 과정과 결과에 관한 자료의 보호
4. 국가핵심기술을 취급하는 전문인력의 구분 및 관리
5. 국가핵심기술을 취급하는 전문인력에 대한 보안 교육 실시
6. 국가핵심기술 유출 사고에 대한 대응체계 구축

### 제4조(법규 준수 의무)

국가핵심기술을 보유 관리하고 있는 대상 기관의 장은 국가핵심기술의 유출을 방지하기 위하여 다음 각 호에 따른 조치를 하여야 한다.

1. 보호구역의 설정, 출입, 허가 또는 출입 시 휴대품 검사
2. 국가핵심기술을 취급하는 전문인력의 이직 관리 및 비밀유지 등에 관한 계약 체결
3. 그 밖에 국가핵심기술 유출 방지를 위하여 대통령령으로 정하는 사항

## 제3장 출입

### 제5조(사업장 출입)

사업장 출입인력은 사업장 내에서 반드시 사원증을 패용해야 하며, 승인된 지역에 한하여 출입한다. 사업장 출입인력은 지급받은 사원증(출입증)을 타인에게 대여·판매·증여할 수 없으며, 분실한 경우 즉시 정보보호부서에 신고한다. 임직원은 퇴직 시 사원증을 반납하여야 한다

내방객 출입을 신청한 임직원은 내방객에게 정보보호규정 및 절차, 영업비밀보호 정책준수 등 정보보호 관련사항을 사전에 주지시키고, 사내에서는 승인된 지역에 한하여 출입할 수 있도록 관리한다

출입 승인자(부서장 등)는 내방객과 방문목적 등을 확인하여 회사 업무목적에 부합하는 경우에 한하여 출입을 승인한다.

내방객과 회의 등의 업무협의를 사무실 별도의 접견실에서 실시한다.

### 제6조(출입 관리)

#### 1. 출입 통제

- (1) 임직원 등은 사내에서 출입 권한을 설정하여야 한다.
- (2) 물리 보안담당자는 출입하는 자의 출입 권한을 확인하여 미소지자에 대해서는 출입을 통제하여야 한다.

#### 2. 출입증 관리·회수·반납

- (1) 출입증의 제작, 교부, 출입권한 부여, 회수 및 폐기 등의 전반적인 관리는 보안담당자가 담당한다.
- (2) 출입증이 분실 또는 훼손되지 않도록 관리하여야 한다.
- (3) 출입증을 분실한 경우, 보안담당자에게 즉시 통보하여 새로운 출입증을 재발급받아야 한다.
- (4) 보안담당자는 분실, 반납 및 폐기 처리된 출입증의 출입 권한을 제거해야 한다.
- (5) 보안담당자는 출입증의 관리실태를 연 1회 이상 점검하여야 하며, 점검 결과를 보안책임자에게 제출하여야 한다.
- (6) 모든 임직원은 퇴사 시 출입증을 반납하여야 한다.

#### 3. 출입증 대여 금지

- (1) 출입증은 타인에게 대여하거나 양도할 수 없다.
- (2) 타인의 출입증을 패용한 경우, 보안담당자는 해당 직원의 출입증을 즉시 회수하여야 한다.



## 제4장 정보관리

### 제7조(보안등급 분류)

1. 국가핵심기술 관련 문서는 비밀등급을 분류하여 관리하여야 한다.
2. 비밀등급의 분류는 문서 내용의 중요도와 민감도에 따라 등급을 결정하는 것으로, 국가핵심기술 보유기업 내 모든 문서 및 데이터 등 자산에 대한 비밀등급 기준을 정하고, 등급에 따라서 비밀의 보관, 수발, 취급인가자 등 관리방법을 달리하여야 한다.
3. 일반적인 분류는 다음과 같으며 각 회사별 환경에 맞게 운영한다.
  - (1) 보안문서 등급 분류 책임
    - 1) 보안문서의 분류는 최초로 문서를 생산한 작성(기안)자가 분류한다.
    - 2) 등급의 조정권한은 결재권을 가진 부서장 또는 관리책임자에게 있다.
    - 3) 고의 또는 실수로 보안문서로 미 지정 하거나 오 분류하는 경우에 대한 책임은 결재권을 가진 해당 부서(팀)장에게 있다.
  - (2) 보안문서 등급분류 기준(안)
    - 1) 보안문서의 등급분류 시 회사에 맞는 보안문서 분류기준에 의거 세부 분류지침 등급을 결정하여야 한다.
    - 2) 분류기준에 해당 사항이 없는 경우 세부 분류지침과 관계없이 보안문서로 지정을 제외한다.
    - 3) 문서의 내용이 보안문서와 일반문서가 혼재되어 있는 경우 상위등급의 내용으로 보안문서로 등급을 지정하여야 한다.
4. 보안문서의 등급 분류 시 아래와 같은 기준을 참조하여 분류기준에 해당되는 경우 <표> 등급분류 예시의 세부 분류지침에 따라 등급을 결정해야 한다.
  - (1) 극비: 심각한 국가적인 손실을 야기하는 사항 또는 타국가에 유출될 경우 막대한 손해를 초래하는 문건
    - 1) 국내외 미공개 기술정보
    - 2) 회사 수익에 절대적 영향을 미칠 정보
    - 3) 동종업계 절대적 우위를 확보할 정보 (신규 사업계획, 상품개발계획 등)
  - (2) 비밀: 사외로 유출 또는 누설될 경우 회사 중요정책의 효율적 집행에 지장 및 경제적 손실을 가져올 수 있는 문건
    - 1) 동종업계 상대적 우위를 확보할 정보
    - 2) 중장기 전략에 관한 주요 정보
    - 3) 제조원가, 주요 분석 자료 (전사 조직도, 제품 및 부품 설계도면 등)
  - (3) 대외비: 중요한 비밀은 아니지만 사외로 유출될 경우 회사의 손실을 초래할 수 있는 문건
    - 1) 극비, 비밀 이외 주요 정보
    - 2) 관련 직원 이외 공개가 제한되는 정보 (협력사 정보, 생산 관련 자료 등)

5. 문서의 내용이 보안문서와 일반문서가 혼재되어 있는 경우 상위등급의 내용으로 문서의 등급을 지정하여야 한다.

〈표〉 등급분류 예시

구분	분류기준	세부 분류지침
극비 (TOP SECRET)	회사 경영에 심각한 영향을 미치는 사항 경쟁사나 이해관계자에게 이용되어 회사에 막대한 손해를 초래하는 사항	경영정책 회의록 중장기 경영계획 신규사업계획 신기술 개발계획 상품개발 및 출시계획 중요 경영분석자료
비밀 (SECRET)	회사 중요정책의 효율적 집행에 지장 및 경제적 손실을 가져올 수 있는 사항	전사 조직도 인원 현황 및 급여체계 제품 및 부품의 설계도면 각종 재무제 표관련 자료 및 현황 중요 회의록 제품성능 및 품질 관련보고서 고객정보 시장조사 자료 가격결정 자료
대외비 (RESTRICTED)	사외로 유출될 경우 회사에 손실을 초래할 수 있는 사항	각종 규정, 표준 계약서류 업무계획 생산 및 판매계획 각종 프로젝트성 업무 협력 업체 정보 주요 직위자 인사자료 사내 건물 설계도 및 레이아웃 제조원가 등 생산관련자료

**제8조(보안등급 별 관리)**

1. 국가핵심기술 관련 문서는 분류된 보안등급(극비, 비밀, 대외비)에 따라 접근통제, 보호구역 지정 및 보관 열람 승인 절차 등 적절한 보호조치를 취하여 관리하여야 한다.
2. 국가핵심기술 관련 문서는 적절한 위치에 해당하는 등급에 대해 명확히 표기하여야 한다.
3. 국가핵심기술 관련 문서에 대한 접근권한은 최고경영진과 관련 부서의 결재권자의 승인을 모두 득할 경우에만 부여되며, 각 등급별 권한 보유자에 대한 기록을 항상 최신으로 유지해야 한다.
4. 접근권한이 없는 비인가자의 국가핵심기술 관련 문서 열람은 원칙적으로 엄격히 금지하나, 연구개발 또는 업무적 필요성에 의한 열람이 필요할 경우, 최고경영진 및 결재권자의 승인을 득하여 1개월 이내의 기간 동안 한시적으로 허용한다.
5. 접근권한이 없는 비인가자의 국가핵심기술 관련 문서 열람이 1개월을 초과할 경우, 최고경영진과 관련 부서의 결재권자의 재승인을 득하여야 한다.

## 제5장 네트워크, PC

### 제9조(네트워크 사용)

1. 국가핵심기술 관련 자료 보호를 위해 내부망과 인터넷망을 분리·운영하여야 한다.  
내부망과 인터넷망을 분리·운영하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
  - (1) 침입 차단·탐지시스템 설치 등 비(非)인가자 침입 차단대책
  - (2) 네트워크 접근관리시스템 설치 등 비(非)인가 장비의 내부망 접속 차단대책
  - (3) 내부망 정보시스템의 인터넷 접속 차단 대책
  - (4) 내부망과 인터넷망 간 안전한 자료전송 대책
2. 시스템에 부여되는 IP주소를 체계적으로 관리하여야 하며 비(非)인가자로부터 내부망을 보호하기 위하여 네트워크 주소변환기(NAT)를 이용하여 사설 IP주소 체계를 구축·운영하여야 한다. 또한 IP주소별로 시스템 접속을 통제하여 비(非)인가 기기에 의한 내부망 접속을 차단하여야 한다.
3. 분리된 내부망과 인터넷망 간 자료전송을 위한 접점이 불가피한 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
  - (1) 침입 차단·탐지시스템 설치·운영
  - (2) 내부망과 인터넷망 간 접점 최소화
  - (3) 내부망과 인터넷망 간 일방향 전송장비 등을 이용한 자료전송체계를 구축·운영하고 원본파일은 3개월 이상, 전송기록은 6개월 이상 유지
  - (4) 정기적으로 전송실패 기록을 확인하고 악성코드 유입 여부 등 점검
  - (5) 내부망 자료를 인터넷망으로 전송할 경우 보안담당자 혹은 결재권자의 사전 또는 사후 승인 절차 마련
4. 보안담당자는 침입 차단·탐지시스템, 스위치·라우터 등 정보통신망 구성 또는 정보보안 정책 전반에 영향을 미치는 보안·네트워크 장비를 설치·운영하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
  - (1) 물리적으로 안전한 장소에 설치하여 비(非)인가자의 무단접근 통제
  - (2) 콘솔에서 관리함을 원칙으로 하되, 다음 항목의 경우 지정 단말기를 통한 접속 관리 허용
    - ① 장비 관리자의 접속
    - ② 장비 담당 벤더사 혹은 유지보수 업체 작업장소에서의 접속
  - (3) 시스템관리자는 로그기록을 1년 이상 유지하여야 하고 비(非)인가자의 접속 여부를 정기적으로 점검하여 그 결과를 보안담당자에게 통보하여야 한다.
  - (4) 시스템관리자는 침입차단·탐지시스템의 침입차단·탐지규칙의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검·갱신하여야 한다.

## 제10조(사외접속)

1. 사외 네트워크를 통한 내부 시스템 접속은 원칙적으로 금지하나, 업무 목적상 접속이 필요할 경우, 적절한 보안대책 수립 및 정보보안 담당 부서장(CISO)과 관련 업무의 부서장의 승인 승인을 받은 대상에 한정하여 예외적으로 허용한다.
2. 사외 네트워크를 이용한 내부시스템 접속을 위해 반드시 다음의 보안대책을 수립한다.
  - (1) 접속 계정 신청 및 발급 절차 수립, 관련 기록 일정 기간 보존
  - (2) 허용 대상별 접속이 필요한 최소한의 시스템에 대해서만 접속 허용
  - (3) 전용선, VPN (가상사설망) 등 암호화 및 인증이 충분히 확보된 수단을 통해 접속
  - (4) ID/PW 입력 이외에 모바일 OTP, 휴대전화 인증 등 다중 인증체계를 구축
  - (5) VPN 접속, 업무용 응용 프로그램 로그인 등의 계정을 통합 관리함으로써 사용자 접속 이력 및 행위 추적성 확보

## 제11조(패스워드 관리)

임직원은 정보시스템 사용 시 아래와 같은 패스워드 기준을 준수해야 한다.

- a. 8자리 이상의 알파벳 대문자와 소문자, 특수문자, 숫자 중 3종류 이상 또는 10자리 이상의 알파벳 대소문자, 특수문자 중 2종류로 구성된 문자열로 생성
- b. Null 및 디폴트 패스워드, 사용자명 등 추정 가능 패스워드 사용금지
- c. 개인 신상정보(전화번호, 주민등록번호, 생년월일 등)와 관련된 패스워드 사용금지
- d. 동일숫자, 문자의 4회 이상 반복 및 키보드 자판의 연속문자 사용금지
- e. 6개월마다 패스워드 변경 등

## 제12조(업무PC 사용)

- ① 정보보호부서는 해킹, 정보유출 방지를 위하여 PC 보안기준을 수립하고 아래의 보안대책이 적용된 PC에 한해 회사 내부망에 연결되도록 관리해야 한다.
- ② 정보보호부서는 PC의 운영체제 및 PC에 설치된 정품 소프트웨어에 대하여 최신의 보안 업데이트가 유지될 수 있도록 PMS(패치 관리시스템)를 운영해야 한다.
- ③ 정보보호부서는 PC 보안프로그램에 아래의 기능을 적용해야 한다.
- ④ 정보보호부서는 PC 보안프로그램에 대한 예외 처리 현황을 관리하고 정기적으로 점검하여 보안 예외를 최소화해야 한다.
- ⑤ 정보보호부서는 사용PC에 대하여 실사용자와 일치되도록 관리해야 한다.
- ⑥ 정보보호부서는 외부 인원이 사내에서 프로젝트와 같은 공동 업무수행이 필요한 경우 전용PC 등을 별도 지급하거나 반입된 PC는 임직원이 사용하는 PC와 동일한 보안 수준으로 관리해야 한다.
- ⑦ 정보보호부서는 승인되지 않은 개인정보가 임직원 PC에 저장되지 않도록 정기 점검 또는 점검 툴 등을 통해 통제해야 한다.

## 제13조(인터넷, 메일, 메신저, 협업 도구 사용)

### [전자메일 사용]

- ① 임직원은 전자메일 사용 시 아래 사항을 준수해야 한다.
  - a. 업무목적으로 전자메일 사용시 회사 업무메일시스템을 사용
  - b. 외부 메일시스템은 업무 목적 사용금지
  - c. 업무용 메일을 외부로 발신하는 경우 회사의 승인 필요
- ② 메일을 통한 악성코드 감염 예방을 위해 아래 사항을 준수해야 한다.
  - a. 출처가 불분명한 메일은 개봉 시 주의
  - b. 메일 내 첨부파일, URL 및 게시물 등 의심스러운 경우에는 클릭 금지
- ③ 회사 통신망을 통해 이루어지는 메일 관련 모든 수발신 내용은 회사의 소유물이며 회사가 보관하는 공식 기록의 일부임을 인식해야 한다.

### [인터넷 사용]

- ④ 임직원은 사내 통신망 및 인터넷 사용시 다음 사항을 포함하여 회사에 손실을 초래하는 행위를 하지 않아야 한다.
  - a. 악성코드를 유포시키는 행위 금지
  - b. 회사 정보자산 무단 전송 금지
  - c. 회사 및 임직원 비방, 집단행동 선동 및 범죄행위 모의 금지
- ⑤ 임직원은 회사 통신망 및 인터넷을 이용하여 회사의 명예를 실추시킬 수 있는 아래의 사이트 접속을 금지한다.
  - a. 불건전 사이트: 음란, 폭력, 도박 등 반사회적 사이트
  - b. 비업무 사이트: 게임, 영화, 만화, 증권 등 업무와 무관한 사이트
- ⑥ 임직원은 외부로 자료 전송시 회사가 지정한 방법을 사용해야 한다.
  - a. 회사 업무 메일시스템 또는 외부 자료전송시스템 등을 이용
  - b. 블로그, 게시판, 외부메일 등 이용금지
- ⑦ 임직원은 회사 통신망 또는 IT자산을 통해 개인적인 용도로 외부 클라우드 서비스 사용을 금지하며, 업무상 사용이 필요한 경우 정보보호부서 승인 후 아래 사항을 준수해야 한다.
  - a. 개인정보를 포함한 대외비 이상의 정보는 암호화 저장
  - b. 계정 공유 금지 및 안전한 비밀번호 설정
- ⑧ 임직원이 SNS를 사용하는 경우 아래 사항을 준수해야 한다.
  - a. 업무 관련 사항 외부 유포 금지
  - b. 게시되는 글, 사진, 동영상 등은 저작권법 준수

#### 제14조(이동식 저장매체 사용)

이동식 저장매체란 HDD, SSD, USB 메모리, 광학 기록매체, 촬영기기(드론 등), PC, 태블릿 등 정보자산을 저장할 수 있는 모든 매체를 말한다.

사전에 승인받지 않은 보조 저장매체 및 휴대용 전산장비의 PC 접속을 통제하여야 한다. 또한 생산라인 반입 PC 및 저장매체 대상 악성코드 검사 절차 운영하여야 한다.

#### 제15조(클린데스크)

임직원은 책상 위에 노트북을 방치해서는 안 되며, 반드시 잠금장치를 하거나 책상 서랍, 캐비닛 등에 잠금 보관해야 한다.

임직원은 퇴근 전 모든 PC 전원을 OFF해야 한다. 단, 업무상 필요한 경우 별도의 예외 표시가 필요하다.

임직원은 퇴근 시 책상 등 업무공간을 안전하게 정리해야 한다.

- a. 책상 위에 문서방치 금지
- b. 대외비 이상 자료(저장매체 또는 출력물 형태) 잠금 보관
- c. 프린터, 세절기, 휴지통, 화물 E/V 주변 등 자료방치 금지
- d. 서랍이나 캐비닛은 모두 잠그기
- e. 저장매체나 개발 관련 제품(샘플 시료 등) 등 무단 방치 금지 등

퇴근 이후 보안상태 확인을 위해 불시 보안점검이 진행될 수 있으므로 보안규정 위반으로 적발되지 않도록 평상시 철저히 관리해야 한다.

#### 제16조(예외 절차)

① 보안담당자는 네트워크, PC의 보안시스템의 예외 절차를 보안 정책에 따라 관리하고, 예외 절차사용자에 대하여 최소한의 권한으로 부여하여 관리하여야 한다. 다음의 경우에 예외 사항으로 한다.

1. 외부로 전자파일을 메일로 전달하는 경우에는 보안담당자의 개별 승인을 받아야 한다. 이때 전달하는 문서의 보안성을 확인하고, 가급적 회수 조치하여야 한다.
2. 개인정보취급자가 P2P 및 웹하드 사이트 접속 시 책임자 승인을 거쳐 특정기간 동안만 허용한다.
  - 가. 신청사유의 타당성 검토한다.
  - 나. 예외 정책에 따른 보안성 검토 및 보완대책 마련한다.
  - 다. 예외정책 만료여부 및 예외 사용에 대한 모니터링 등을 실시한다.
3. 상용 전자우편을 이용한 업무자료 송수신을 하여서는 아니 된다. 단, 외부인은 원칙적으로 사내 E-mail을 사용할 수 없으며, 예외의 경우 그 이유를 문서화한다. 단, 특별히 기밀성을 요하는 정보가 있을 경우 E-mail을 통해 전송되어야 한다면 사내 승인된 소프트웨어와 알고리즘을 사용하여 지정 수신인만 읽을 수 있도록 암호화한다.
4. 서버에 접속한 후 사용자나 다른 시스템으로부터 일정시간(10분 이하) 동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시키는 것을 원칙으로 한다. 단, 개발 업무나 서버 운영상 필요성이 인정되는 경우 예외로 할 수 있다.

5. 정보시스템, 모바일기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보 유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 따라야 한다.

가. 반출입 통제 대상 : 정보시스템(서버, 네트워크 장비 등), 모바일기기(노트북, 스마트패드, 스마트폰 등), 저장매체(HDD, SSD, USB메모리, 외장하드디스크, CD/DVD, 테이프 등) 등

나. 반출입 통제 절차 : 보호구역 출입통제 책임자 사전승인, 반출입 관리대장 기록, 반출입 기기에 대한 보안점검 수행(백신설치 여부, 보안업데이트 여부, 악성코드 감염 여부, 보안스티커 부착 여부, 중요정보 유출 여부 등), 반출입 내역 주기적 검토 등

다. 반출입 관리대장에는 다음의 사항을 기록한다.

- 반출입 일시 및 장소
- 사용자 정보
- 기종(모델), 기기식별정보(시리얼번호 등)
- 반출입 사유
- 보안점검 결과
- 관리자 확인 서명 등

② 예외사항이 있을 경우 명확한 사유 및 관련자 협의, 책임자 승인 등 관련 근거를 기록하여야 한다.

## 제6장 업무 수행

### 제17조(출력문서 관리)

보안담당자는 핵심기술을 포함하는 문서의 출력과 복사를 통제하는 출력물 보안시스템을 구축해야 한다. 출력물 보안시스템은 기능은 다음과 같다.

1. 임직원의 인쇄작업의 권한을 부여하고 관리 서버를 이용하여 통제한다.
2. 임직원이 인쇄하는 모든 인쇄물의 기록을 서버에 저장한다. 서버에 전송되는 인쇄 정보는 사용자 정보와 문서 정보이며 인쇄 내용 전부를 이미지화 시켜 저장하는 방식을 권장한다.
3. 인쇄물(종이)에 사용자의 인쇄 정보(사용자 이름, 사원번호, 부서, IP 주소, 출력 일자 시간 등)을 함께 출력한다.
4. 인쇄물(종이)에 사용자 정보와 인쇄 정보를 포함하여 유출된 문서의 경로 추적 및 원본 비교 한다.
5. 인쇄물에 보안등급 및 회사정보, 주의문구를 추가한다.
6. 외부 인원의 출력과 복사를 제한한다.

## 제18조(업무 회의, 출장)

- ① 보안담당자는 회의 시 다음의 보안 준수 사항을 시행한다.
  1. 보안담당자는 회의 운영 기간 동안 배포될 발표 자료 등 공개자료에 산업기술 비밀에 관련된 사항이 없는지 확인한다.
  2. 보안업무담당자를 지정하여 회의 시 보안업무를 담당하도록 한다.
  3. 보안업무담당자는 기밀을 필요로 하는 회의 자료는 별도의 시건 장치가 되어 있는 장소에 보관하고 철수 시 직접 회수한다.
- ② 보안담당자는 출장 등에서의 다음의 보안 준수 사항을 시행한다.
  1. 보안담당자는 출장 시 이동 자료 등 공개자료에 대한 보안성을 검토한다.
  2. 보안담당자는 중요한 제품 전시회의 경우에는 보안업무담당자를 직접 파견한다.
  3. 인터뷰나 홍보를 통한 산업기술보호 유출을 막기 위해 관련 인력에 대한 사전교육을 실시하거나, 사전교육을 받은 인원이 인터뷰나 홍보를 전담하도록 한다.
  4. 기밀을 요하는 자료는 별도의 시건 장치가 되어 있는 장소에 보관하고 철수 시 직접 회수한다.
  5. 전시회에 게시되었던 자료와 제품에 대한 국내 이송 과정을 지침 준하여 검토하며 전시되었던 제품이나 게시물을 현지에서 폐기할 경우에는 보안책임자가 지정한 담당자 입회하에 폐기한다.
  6. 핵심 인력이 해외 출장 시 보안담당자는 사전에 보안 교육을 실시한다. (필수적으로 이루어져야 하는 보호조치는 보호등급에 따른 연구개발 참여연구원의 별도 관리, 해외 출장 시 사전교육, 참여연구원의 퇴직(예정) 시 보호조치 등이 있다. 참여연구원이 해외 출장 시에 사전에 연구개발의 내용 유출 및 보안에 관한 보호 교육을 실시한다.

## 제19조(외부인원 관리)

- ① 산업기술을 보유한 기관에서 보안담당자는 핵심기술을 보관하고 있는 구역에 대하여는 외부인의 출입을 통제해야 한다.
  1. 외부인의 출입 시 보안요원의 보안에 관한 보호 교육을 받는다.
  2. 보호구역 내에서는 내부직원과 동행해야 하며 단독행동은 금지한다. 이때 허용 가능한 보호구역을 정한다.
- ② 보안담당자는 연구개발 내용 및 연구개발 성과물의 유출 등을 방지하기 위하여 외부인 및 외국인 채용직원에 대한 보호조치를 다음 각호에 따라 수행한다.
  1. 외국인 연구원의 연구개발 참여는 원칙적으로 제한한다. 다만, 불가피한 사유가 있다고 판단되는 경우에는 대상기관의 장에게 사전승인을 받는다.
  2. 외국인을 채용하여 산업기술 분야 등에 근무하게 하는 경우 외국인력에 대한 신원확인 및 함께 근무에 따른 철저한 보안관리를 하여야 한다.
  3. 국내에서 근무하는 외국인력에 대한 보안관리는 별도의 보안규정 마련한다. 채용 대상 외국인력의 인적사항 확인, 검증하고 외국인력 대상 별도의 보안관리 대책 수립 및 운영 방안을 고용계약과 병행하여 확정 후 고용과 동시에 보안 교육을 실시한다. 단, 외국인 직원에 대한 보안관련 조치 시 부당하게 처우하지 않는다.



- 가. 외국인력이 국가핵심기술 분야에 근무하도록 하는 것은 꼭 필요한 최소한의 범위에서 참여하도록 한다.
- 나. 외국인력 채용 검토를 위한 신원과 경력을 공식적으로 검증할 자료의 제출을 요청하고 필요한 경우에는 공증을 실시한다.
- 다. 근무에 따른 기술 보호 등 보안 의무(국내 관련 법령 준수 의무 부과 등)에 대해 보안 교육을 실시하고 숙지하도록 한다.
- 라. 사전 승인 절차에 의하여 해당 근무지역 이외 출입을 제한하도록 조치하고 이에 따른 출입증(사원증)을 발급한다.
- 마. 고용계약서상에 기관의 보안규정 준수 의무 및 기술 보호 의무(국내 기술 보호 법령 준수 등) 부과 등을 명시하고 보안규정을 준수한다는 내용이 포함된 비밀유지서약서(국문·영문)를 징구한다. 국가핵심기술 분야에 참여하는 경우에는 산업기술보호법(제10조) 및 관련 규정에 따라 국가핵심기술 보호를 위한 의무조치 부과하는 별도의 비밀유지서약서를 징구한다.

※ 외국인력 채용 시 비밀유지서약서 포함사항(예시)

- 근무 중 직무상 연구개발 등 취급한 기술·정보는 기관에 귀속
- 계약기간 및 종료 후에도 일정 기간 비밀유지의무 명기
- 문서·자료 반출 시 사전 승인과 노트북, 정보통신망 등 이용 시 자료 유출 위험에 대한 사용 제한 또는 검색 및 통제 가능 명기
- 업무상 접근한계와 구역의 출입제한 및 비밀보호 의무 부여 명기
- 계약만료 시 업무상 개발한 자료, 반환 의무와 기술자료 유출 여부 검색 가능 조건 명기 등

5. 외부 인원의 직무 수행 중 보안관리는 다음과 같다.

- 가. 정기적으로 보안 교육을 실시하고 임직원 참여 보안예방활동에 적극 참여하도록 조치한다
- 나. 근무 중 담당 직무와 관련이 없는 보호구역 등의 지정된 근무 장소 외 출입 통제 대책 수립 및 조치
- 다. 정보통신망 접근 권한 통제 및 감독 방안 수립 및 관리
- 라. 부서장/담당 임원의 통제(승인·경유)하에 E-mail, FAX 등 이용
- 마. 노트북 및 저장장치 반출·입시 기술보호총괄책임자 및 기술보호부서책임자 승인
- 바. 해당 근무부서에 대해 주기적·불시적인 보안점검 실시 등
- 사. 외국인력이 근무 중 직무상 해외로 출·입국에 따른 전후 보안 교육 실시 및 서약서 징구
- 아. 직무상 관련이 없는 기술자료 등을 무단으로 복사하거나 외장하드등 정보저장장치 등에 저장하는 것을 사전에 차단한다.
- 자. 사전에 승인되지 않은 야근을 많이 하거나 또는 잦은 휴일 근무가 발생되지 하지 않도록 사전 검토하고 관리한다.
- 차. 외국인력이 고용계약 등의 종료에 따라 퇴직할 경우 해당 직무분야의 기술정보 또는 성과물이 국외로 유출될 가능성을 배제할 수 없다. 따라서 외국인의 퇴직에 따른 기술유출 등의 위험을 최소화할 수 있는 보안 대책이 필요하다.

- 카. 외국인력이 계약기간 만료에 따라 직무 수행 중에 취득한 기술 등 기밀 내용이 누설되지 않도록 PC 등 하드웨어 및 보유 기술자료, 성과물 및 연구 노트 등을 모두 회수한다.
- 타. 대상 기관은 퇴직 등에 따른 근무기간 동안 외국인력이 직무 수행 중에 취득하거나 인지한 기술정보 등에 대한 보안의무를 고지한다.
- 파. 퇴직 이후에 근무기간 취득하거나 지득한 기술정보 등의 비밀유지 의무를 부과하기 위하여 이를 위반 시 제재사항 등이 명시된 비밀유지서약서(영문·국문)를 징구 한다.

## 제20조(보안 교육)

- ① 국가핵심기술을 보유·관리하고 있는 대상기관의 장은 정기적으로 국가핵심기술 취급 전문인력을 대상으로 보안 교육을 시행하여야 한다.
- ② 국가핵심기술을 보유·관리하고 있는 대상기관의 장은 국가핵심기술 취급 전문인력의 신규채용이나 보안 사고 발생 등 보안상 필요하다고 판단되는 경우 추가로 보안 교육을 시행하여야 한다.
- ③ 국가핵심기술을 보유·관리하고 있는 대상기관의 장은 보안 교육 과정에 산업기술 보호 관련 법률, 법률 위반 시 법적 책임 등의 내용을 포함하여야 한다.
- ④ 교육책임자 또는 담당자를 지정하고 교육·훈련의 내용 및 평가가 포함된 교육·훈련규정을 작성하여야 하되, 필요한 경우에는 외부 전문기관에 교육을 의뢰할 수 있다.
- ⑤ 작업원에 대한 교육·훈련은 연간계획을 수립하여 실시하며, 작업원이 맡은 업무를 효과적으로 수행할 수 있도록 제조·품질관리와 그 밖에 필요한 사항에 대하여 실시하여야 한다.
- ⑥ 국가핵심기술 제조업자의 교육·훈련 규정에는 생물학적제제 등의 제조관리 및 품질관리를 실시하는 데에 필요한 교육내용이 포함되어야 한다.

## 제21조(부서 보안)

1. 적용범위
  - (1) 조직 및 부서 내 기술문서 정보를 이용하는 사무 관리에 관하여 기술문서 정보 관리에 적용하도록 한다.
  - (2) 관리 대상 범위는 문서 뿐만 아니라 이메일, 메신저와 같은 부서 조직 내 생성, 관리되는 다양한 콘텐츠까지 포함한다.
2. 정의
  - (1) 결재 : 부서 내 결정할 권한이 있는 관리자가 부서 조직원이 제출한 안건을 검토하고 허가하거나 승인하는 행위를 말한다.
  - (2) 결재문서 : 관리대상 기술문서에 포함되어 있으며 전자적 또는 대면 결재행위에 소속되어 있는 문서를 말한다.
  - (3) 관리대상 기술문서정보 : 조직 및 부서 내에서 관리되어야 할 문서정보로, 업무에 대한 설명책임이나 증거력 확보의 필요성이 높은 문서정보를 말한다.
  - (4) 문서 : 특정 매체에 기재된 내용, 맥락, 구조를 갖춘 정보나 데이터를 말한다.

- (5) 문서관리책임자 : 조직 및 부서 내에서 기술문서정보의 운영 및 관리업무를 총괄하는 자를 말한다.
  - (6) 문서 정보 : 개인 또는 직원이 업무상 작성 또는 취득한 문서, 도면 및 전자적 기록으로 기존의 종이서류 및 도면은 물론 PC 등으로 만든 전자문서, 스프레드시트, 이미지 정보, 영상, 음성과 이메일, 실험데이터 등 전자적으로 작성하거나 취득한 모든 정보를 말한다.
  - (7) 보관 : 소관 부서에서 문서의 처리 완결 후, 보존되기 전까지 문서를 관리하는 것을 말한다.
  - (8) 보존 : 장기간에 걸쳐 전자문서나 기록물을 기술적/관리적으로 존속하게 하는 과정과 운영을 말한다.
  - (9) 소관 부서 : 업무를 진행하는 과정에서 문서를 작성, 처리하는 부서를 말한다.
  - (10) 이관 : 전자문서나 기록물을 한 장소에서 다른 장소로 옮기는 것과 관리/소유권/책임이 변경되는 것을 말한다.
  - (11) 이송 : 전자문서나 기록물의 진본성, 신뢰성, 무결성, 이용 가능성을 유지하면서 전자문서나 기록물을 한 시스템에서 다른 시스템으로 옮기는 활동을 말한다.
  - (12) 전환 : 문서를 한가지 매체/포맷에서 다른 매체/포맷으로 변경하는 행위를 말한다.
  - (13) 접근 : 정보나 전자문서를 찾거나 검색하는 권리나 기회를 말한다.
  - (14) 처분 : 전자문서 또는 기록물의 보존이나 폐기 또는 이관 결정과 관련된 광범위한 행위를 말한다.
  - (15) 추적 : 전자문서나 기록물의 이동과 사용에 관한 정보를 기록하고 유지하는 행위를 말한다.
  - (16) 폐기 : 문서를 재구성하지 않고 완전히 제거하거나 삭제하는 과정을 말한다.
3. 기술문서 정보관리의 대상
- (1) 공식적으로 결재 또는 접수한 기록물을 포함하여 결재 과정에서 발생한 수정내용 및 이력 정보, 업무수행과정의 보고사항, 검토사항 등을 관리해야 한다.
  - (2) 결재문서 이외에 업무 설명책임이나 업무수행에 필요한 문서정보들도 관리해야 한다.
4. 문서관리책임자 지정
- (1) 조직의 장은 조직 내 기술문서 정보관리를 위해서 문서관리책임자를 지정해야 한다.
  - (2) 문서관리책임자는 조직 내 문서정보의 운영, 관리에 관한 사항을 총괄한다.
5. 관리대상 기술문서의 성립 및 효력 발생
- (1) 결재문서는 다른 규정에 특별하게 정한 경우를 제외하고는 당해 결재문서에 대한 최종 결재권자의 결재로 성립하고 효력이 발생한다. 효력발생 시기를 따로 정한 때에는 그에 따르며 수신자가 있는 문서의 효력발생 시기는 수신자에게 도달한 때로 한다.
  - (2) 문서정보는 업무활동을 완전하게 표현하여야 한다. 업무나 활동에 대한 맥락과 문서내용을 파악할 수 있는 정보가 명확하게 문서정보에 표현되어야 한다.
6. 문서정보의 유형
- (1) 관리대상문서정보 : 조직에 의해 관리되어야 할 문서로 업무에 대한 설명책임이나 증거력 확보의 필요성이 높은 문서를 말한다.
  - (2) 비관리대상문서정보 : 조직에 의해 관리될 필요가 없는 문서 정보를 말한다.

- (3) 결재문서는 관리대상문 서로서 아래와 같이 나누어진다.
  - 1) 내부결재문서 : 조직 내부적으로 국가핵심기술과 관련하여 계획을 수립하거나 처리방침을 받거나 보고 또는 검토하기 위하여 결재를 받는 문서를 말한다.
  - 2) 대내문서 : 조직 내부 및 각 부서 간에 지시, 명령 또는 협조 하거나 보고 또는 통지를 위하여 수발하는 문서를 말한다.
  - 3) 대외문서 : 외부 조직과 수발하는 문서를 말한다.
- (4) 업무참조 문서정보는 조직 내 결재행위와 관련은 없지만, 업무의 효율적인 진행이나 지식공유, 이관 등의 경우에 업무를 이해하는데 보조할 수 있는 문서 정보로서 업무 추진과정에서 수집되거나 생성된 문서 정보 중에 결재 과정에 포함되지 않은 문서 정보를 말한다.

7. 관리대상 기술문서의 결정

- (1) 모든 결재 문서는 관리대상 문서정보로서 관리되어야 한다.
- (2) 업무문서정보를 관리대상 문서정보로 결정하기 위해서 다음의 사항을 고려한다.
  - 1) 업무나 활동과 관련한 법/규정의 문서관리 규정 또는 지침
  - 2) 업무나 활동의 증거나 설명책임이 요구되는 문서에 대한 내·외부 규정
  - 3) 업무 활동상의 필요성
  - 4) 타 업무활동이나 처리행위와의 연관 관계

8. 결재 문서의 구성

- (1) 기안문 및 시행문은 두문, 본문 및 결문으로 구성한다. 두문은 기관명 및 수신자로 한다. 본문은 제목, 내용 및 붙임으로 한다. 결문은 발신명의, 기안자, 협조자, 결재권자의 직위 또는 직급 및 서명, 등록번호와 시행일자 등으로 한다.
- (2) 결재 문서의 발신명의는 조직의 장으로 한다. 단 내부결재문서는 발신명의를 표시하지 아니한다.
- (3) 사내 부서 간의 업무협조를 위한 결재문서의 발수신은 소관부서장 명의로 하고, 소관 부서 내의 부서 상호 간에는 차하위부서장에 동일직위 명의로 한다.

9. 결재문서의 기안

- (1) 결재문서의 기안은 내부 규정에서 별도로 정하는 기안문서로 하여야 한다.
- (2) 기안자 또는 품의자는 품의를 기안함에 있어 그 안건의 목적, 실시방법, 시기 및 효과 등을 충분히 조사연구하고 관계자와 사전에 협의를 하여 품의의 원활한 진행에 노력하여야 한다.

10. 기술문서 정보의 이용

- (1) 결재가 끝난 문서정보는 각 소관부서장이 통제하고, 대외제공문서는 주관부서장이 통제한다. 각 소관부서장은 소관부서의 문서에 관한 감독책임이 있고 주관부서장은 문서관리에 관하여 지도할 책임이 있다.
- (2) 부서 상호간에 업무수행상의 필요에 따라 문서를 열람할 수 있으나, 승인 없이 타인에게 임의로 열람시키거나 그 사본을 대여할 수 없다.
- (3) 기술문서 정보의 접수

- 1) 문서정보는 소관부서에서 접수하며, 주관부서에서 직접 받은 문서정보는 문서접수대장에 기록한 후 지체없이 배부해야 한다.
  - 2) 주관부서의 담당자는 접수된 문서정보를 처리 담당자에게 인계하고, 처리 담당자는 문서정보를 공람하게 할 수 있다.
- (4) 기술문서 정보의 발송
- 1) 발신한 문서는 결재를 받은 후 시행문을 작성하여 발신한다.
  - 2) 문서정보의 발신 명의를 조직의 장으로 한다.
  - 3) 대외문서는 결재 후 기안문을 시행문과 함께 주관부서의 문제통제와 직인을 받고 보완관리자의 확인 이후 대외문서 발송대장에 기록 후 소관 부서에서 발신한다.
  - 4) 문서정보는 정보통신망을 이용하여 발신함을 원칙으로 한다. 다만 정보통신망을 이용하여 발송할 수 없는 문서는 이를 출력하여 발신할 수 있다.
- (5) 기술문서 정보의 이관
- 1) 주관부서는 소관부서의 이관 대상 문서정보를 인수, 관리해야 한다.
  - 2) 전자적 형태로 생산되지 아니한 문서정보를 인수하는 경우에는 원본 및 목록의 일치 여부, 물리적 상태 확인 등의 검수 절차를 거쳐야 한다.
  - 3) 주관부서장은 인수절차 종료시, 그 결과를 해당 소관부서에 통보하여야 한다.
  - 4) 인수 완료 결과를 통보받은 소관부서장은 해당 전자적 문서정보를 물리적으로 복구가 불가능하도록 삭제 또는 파기하여야 한다.
- (6) 기술문서 정보의 보존
- 1) 주관부서장은 문서정보 중 보존기간이 10년 이상인 경우에는 장기보존 문서로 관리해야 한다. 주관부서장은 전자적 문서정보의 손실을 방지하기 위하여 백업 및 복원 기능을 구비하여야 한다.
  - 2) 주관부서장은 문서정보를 안전하게 보존 관리하기 위하여 보존환경의 유지, 보안대책 및 재난 대비 계획 수립, 시행 등 필요한 조치를 취한다.
  - 3) 보존 중인 기술문서 정보에 대하여 보존 기준에 따라 상태 점검을 매년 1회 이상 실시해야 한다.
- (7) 기술문서의 폐기
- 1) 보존기간이 경과된 문서정보에 대해서는 소관 부서의 의견조회, 주관부서의 심사 등을 거쳐 보존기간 재책정, 폐기 또는 보류로 구분하여 처리한다.
  - 2) 조직의 문서정보의 평가 및 폐기를 위하여 별도의 평가심의회를 구성하여 운영하는 것이 바람직하다.
  - 3) 폐기해야 할 문서정보의 이용 이력을 검토하여 폐기 상태를 확정 또는 수정해야 한다.
  - 4) 기술문서 정보의 물리적 파괴는 비밀 수준에 맞는 방법으로 이루어져야 한다. 전자 형식의 문서 정보는 재포맷하거나 덮어쓰기를 통해 물리적으로 파괴해야 한다.

## 제7장 사고대응 및 상벌

### 제22조(보안사고 대응)

1. 국가핵심기술과 관련된 중요한 정보나 자료가 외부로 유출되거나 누설 또는 분실 등 보안사고 발생한 경우 피해를 최소화하고 빠른 복구를 통해 업무의 연속성을 보장하기 위해서 신속하고 체계적으로 대응할 수 있도록 하고 발생 초기에 적절한 대응이 이루어지도록 한다.
2. 보안사고 단계별 대응 절차를 마련한다.

#### (1) 사고탐지

보안관리자가 직접 보안사고 발생 사실을 감지하거나 내부직원 또는 외부인에 의한 신고 접수로 사고 발생을 탐지할 수 있다.

#### (2) 초기대응

- 1) 보안관리자는 초기에 대응할 수 있는 수행하고 침해 사고 관련 부서에 통지한다.
- 2) 보안사고 대응팀이 구성되면 초기 조치 사항들을 인계하고 이후는 보안사고 대응팀과 함께 공조한다.
- 3) 원활한 인수인계 및 조치사항들을 검토하기 위해 각 단계에서 수행되는 모든 세부 사항들은 문서화를 통해 그 기록을 유지하고 관리해야 한다.

#### (3) 대응전략 체계화

- 1) 실제 사고의 발생 여부, 보안사고의 유형 및 보안사고로 인한 잠재적인 업무 영향에 대해서 파악한다.
- 2) 적절한 정보가 모아지면 이를 판단 근거로 현재 사고 처리 방향을 결정한다.
- 3) 다음과 같은 사항에 대해서 파악하여 최적의 대응전략을 결정한 후 의사결정자의 최종 승인을 받고 최대한 빠른 시간 내에 대응 조치를 진행한다.
  - ① 외부에 유출된 정보 또는 기술이 얼마나 중요하고 민감한지 여부
  - ② 사건이 외부에 알려졌는지, 유출자는 누구인지, 경제적 피해 규모는 얼마인지 확인
  - ③ 외부기관에 협조를 요청 여부
- 4) 사고 대응 과정에서 수사기관에 신고하여 법적인 대응이 필요한 지를 결정한다.
- 5) 사고의 내용이 법적인 제제가 필요한 사항이 아닌 내부에서 처리해야 할 사항이라면 보안사고 대응 조치가 마무리된 이후에 처리한다.

#### (4) 사고 조사

- 1) 조사의 핵심은 보안 사고를 유발한 행위자와 보안사고의 대상이 무엇인지 알아내는 것이 중요하다.
- 2) 사고 조사 과정은 증거자료 수집과 분석 단계로 나눌 수 있다.
  - ① 증거자료 수집 : 보안사고 분석을 위해 살펴보아야 할 범행들과 단서들을 수집한다. 특히 법적 소송을 염두에 둔다면 수집하는 증거자료는 무결성과 적법성을 유지해야 한다.
  - ② 분석 단계 : 사고와 관련하여 육하원칙에 기초하여 수집된 증거자료를 분석한다.

(5) 보고서 작성

- 1) 보고서는 보안사고를 분석한 내용을 육하원칙에 의거하여 작성 및 원인분석에 따른 대응 방안도 작성한다.
- 2) 작성된 보고서를 받은 상급자 또는 의사결정권자가 알기 쉬운 형태로 작성한다.

3. 향후 동일한 보안 사고가 발생하지 않도록 사후 조치를 마련한다.

사고 원인 분석에 따른 보안 대책을 근거로 관련 규정이나 지침의 변경 및 개정, 보안교육 자료 준비, 보안 실태 점검 계획 및 모의 훈련 시행 등에 반영하도록 한다.

**제23조(보안우수자 및 위반자의 조치 및 징계)**

1. 보안우수자의 선정 및 포상

(1) 보안우수자 선정 및 포상 기준 마련

- 1) 자체 규정에 보안우수자 선정 및 포상 기준을 수립한다.
- 2) 상위기관 및 규제기관의 보안감사, 보안 평가 및 자체적으로 실시하는 보안관리 점검 등을 통하여 이행 성적이 우수한 임직원을 선정한다.
- 3) 인사고과, 승진, 포상, 교육훈련 등 모든 임직원이 관심을 가질 수 있는 포상기준을 마련한다.

(2) 보안우수자 선정 절차

- 1) 자체 보안심의회 또는 인사위원회 등의 심의를 거쳐 선정한다.
- 2) 보안관리자는 최종 확정된 보안우수자 후보를 상급자 또는 의사결정권자에게 보고하여 최종 승인을 받는다.

2. 보안 위반자의 조치 및 징계

(1) 보안 관리 위반자의 처벌 규정 마련

- 1) 보안 위반자의 처벌 절차 및 수위를 결정할 수 있는 규정을 마련한다.
- 2) 보안 규정 및 관련 가이드를 준수하지 않거나 본인의 부주의 및 과실로 인하여 보안사고가 발생한 경우 그 귀책 사유를 감안하여 국가핵심기술의 연구, 개발, 제조 및 생산의 참여를 제한해야 한다.

(2) 보안관리 위반자 징계 절차 이행

- 1) 보안 관리 부서에서 위반자를 적발하거나 신고가 접수된 경우 자체 조사를 통하여 징계 안건을 보안심의회 또는 인사위원회에 통보한다.
- 2) 징계 안건을 토대로 그에 합당한 징계 조치를 부여하고 보안심의회 또는 인사위원회에 안건을 상정한다.
- 3) 인사위원회는 보안 위반자의 징계 조치를 검토한 후 징계 조치 결과를 인사관리 부서에 통보한다.
- 4) 인사관리 부서는 징계 조치 결과를 위반자에게 통보하고 전 임직원들에게 이러한 사실을 공지해야 한다.
- 5) 보안사고의 심각성으로 외부 기관으로부터 처벌을 받은 자는 징계 시 그 결과를 반영한다.

- 6) 보안관리자는 보안위반자가 보안을 필요로 하는 국가핵심기술 관련 업무 참여를 제한하고 위반자에 대한 현황을 지속적으로 관리하고 유지한다. 다만 인권침해가 되지 않는 조건에서 사후관리를 철저하게 한다.

## 제8장 퇴사

### 제24조(퇴사 시 의무)

#### 1. 퇴직자 관리

퇴직자가 업무 수행 중에 습득한 국가핵심기술 관련 중요한 정보를 외부에 누설하는 것을 방지하기 위해서 퇴직 시에 반드시 보안 관리 규정의 절차를 준수해야 한다.

##### 1) 퇴직 전 단계

- ① 퇴직예정자의 기술정보유출을 의심해 볼 만한 특별한 행동의 사례를 확인한다.
  - 높은 기술 보안 등급에 해당하는 인력의 갑작스러운 사직 요구
  - 조직에 대해 갑작스럽게 부정적 태도로 돌변
  - 해당 업무와 관련 없는 기술 정보의 보유
  - 기술 정보의 외부 유출 흔적
  - 눈에 띄게 외부 메일을 사용한 흔적
- ② 퇴직예정자는 업무 인수인계 및 관련 서류, 조직의 모든 자산을 일체 반환토록 하며 기술 정보 및 시설 접근권한 또한 제한해야 한다.
- ③ 퇴직예정자에 대한 전반적인 보안점검이 이루어진 후에는 퇴직자가 연구정보를 누설하거나 오용하지 않을 의무와 위반 시 처벌에 대해 명시된 보안서약서를 징구한다.

##### 2) 퇴직 승인

퇴직자의 최종 승인이 이루어지기 전에 모든 보안 절차의 준수 여부를 확인하고, 업무 인수인계가 명확하고 완전하게 완료되었는지, 다른 누락된 사항이 없다고 판단되면 퇴직을 최종 승인한다.

#### 2. 퇴직 후 보안 조치 사항

- 1) 퇴직자가 모든 퇴직 준비를 마치고 개인물품을 외부로 보낼 때 중요한 정보가 포함되어 있는지 검토해야 한다.
- 2) 퇴직 이후에도 관련 사항에 대해서 상호 협의할 수 있는 체계를 구축한다.



**[별첨 1] 관련 기관별 역할**

기관명	주요 역할	연락처/홈페이지
산업통상자원부	산업기술유출방지 및 보호에 관한 법률 및 정책	1577-0900 www.motie.go.kr
한국바이오협회	바이오, 제약 업계 소통 채널	031-628-0037 www.koreabio.org
한국산업기술보호협회	산업기술유출방지 및 보호에 관한 정책지원 및 중소기업 지원	02-3489-7000 www.kaits.or.kr
NIS 산업기밀보호센터	국내 첨단기술을 보호하고 산업보안활동을 수행	111 www.nis.go.kr
경찰청 (산업기술보호수사팀)	산업기술 유출범죄 전문 수사 및 예방, 기업지원활동	182 www.police.go.kr
공정거래위원회	독점 및 불공정거래 방지정책 수립 운영	1670-0007 www.ftc.go.kr
특허청	부정경쟁방지 및 영업비밀 보호에 관한 법률 및 정책	1544-8080 www.kipo.go.kr



[별첨 3] 비밀유지 서약서

**비밀유지 서약서(예시)**

소 속 :  
성 명 :  
생년월일 : \_\_\_\_년 \_\_\_\_월 \_\_\_\_일

위 본인은 20\_\_년 \_\_월 \_\_일자로 회사명(이하 '회사'라 함)에 입사하여, 회사로부터 영업비밀 및 영업자산의 중요성과 영업비밀 등의 보호와 관련한 법령 및 회사의 취업규칙, 영업비밀 관리 규정 기타 사규, 방침, 정책 등에 관하여 충분한 설명을 듣고 그 내용을 이해하였기에, 다음 사항을 준수할 것을 서약합니다.

1. 본인은, 아래와 같은 정보가 회사의 영업비밀에 해당함을 확인하며, 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등을 준수할 것을 서약합니다.
  - ① 영업비밀 관리규정 기타 회사의 내부 규정에 기재된 영업비밀 보호 대상
  - ② 영업비밀임이 표시된 기술자료, 공장 배치도, 제품 설계도면, 금형, 시제품, 제조 및 판매 매뉴얼, 제조원가, 판매 및 가격결정, 거래선 자료, 인력정보 등에 관한 정보 등
  - ③ 통제구역, 시건장치, 패스워드 등으로 접근이 제한된 컴퓨터시스템, 보관함, 통제구역에 보관된 기록매체, 문서, 물건, 정보 등
  - ④ [추가 사항 기재]
  - ⑤ 그 밖에 회사가 영업비밀로 지정하고 표시하였거나, 회사가 영업비밀로 관리하고 있는 비밀정보
2. 본인은, 회사에 재직 중 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산을 재직 시는 물론 퇴사 후에도 이를 비밀로 유지하고, 회사의 사전 서면 동의 없이는 경쟁업체나 제3자에게 제공하거나 누설하지 않으며, 부정한 목적으로 공개하거나 사용하지 않을 것을 서약합니다.
3. 본인은, 회사에 재직 중 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산에 대한 모든 권리가 회사의 소유임을 인정하고, 이를 회사에 귀속시킬 것을 서약합니다.
4. 본인은, 회사에 재직 중 회사의 승인을 받지 아니하고는 통제구역, 허가받지 않은 정보, 시설 등에 접근하지 아니하며, 회사의 영업비밀을 복제하거나 사본 등의 형태로 보관하지 아니할 것을 서약합니다.
5. 본인은, 입사 전 또는 재직 중에 취득한 타인의 영업비밀 등에 해당하는 정보를 회사에 제공하거나 개시하지 않을 것이며, 업무상 그 정보의 개시가 불가피하다고 판단되는 경우에는 사전에 회사와 상의하여 타인의 영업비밀 등을 침해하지 않도록 할 것을 서약합니다.
6. 본인은, 회사에 재직 중에 회사의 사전 승인을 받지 아니하고는 회사와 동종, 유사 업체의 임직원으로 겸직하거나 자문을 제공하지 아니할 것을 서약합니다.
7. 본인은, 회사의 컴퓨터 등 정보처리장치와 정보통신망을 업무용으로만 사용할 것이며, 회사가 불법 행위 방지 및 영업비밀 등의 보호를 위하여 필요한 경우 본인의 컴퓨터 등 정보처리장치나 전자 우편 또는 인터넷 등 정보통신망의 사용 내역, 기타 필요한 정보를 모니터링 할 수 있으며, 불법행위 또는 영업비밀 등의 누설이나 침해의 우려가 있을 경우 관련 내용을 열람할 수 있음을 (이해하고, 이에 동의합니다.)

8. 본인은, 퇴사 시 재직 중에 보유하고 있던 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산과 관련된 자료 모두를 회사에 반납하고, 이에 관한 어떠한 형태의 사본도 개인적으로 보유하지 않으며, 반납할 수 없는 것은 폐기할 것을 서약합니다.

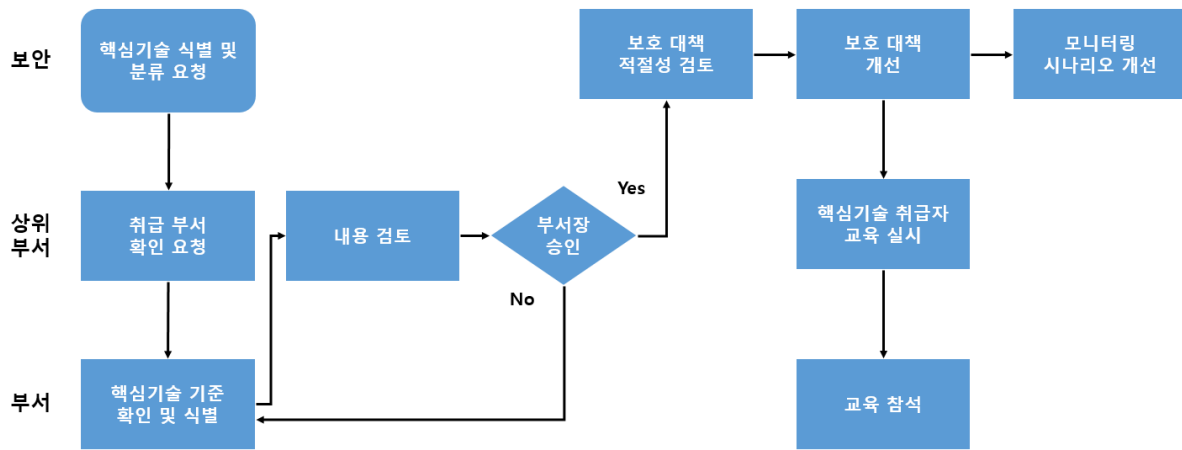
위 서약한 사항을 위반할 경우 관련 법규에 의한 민·형사상 책임을 감수할 것임을 서약합니다.

*(위 내용을 확인하고 이해하였으며, 이에 서명함)*

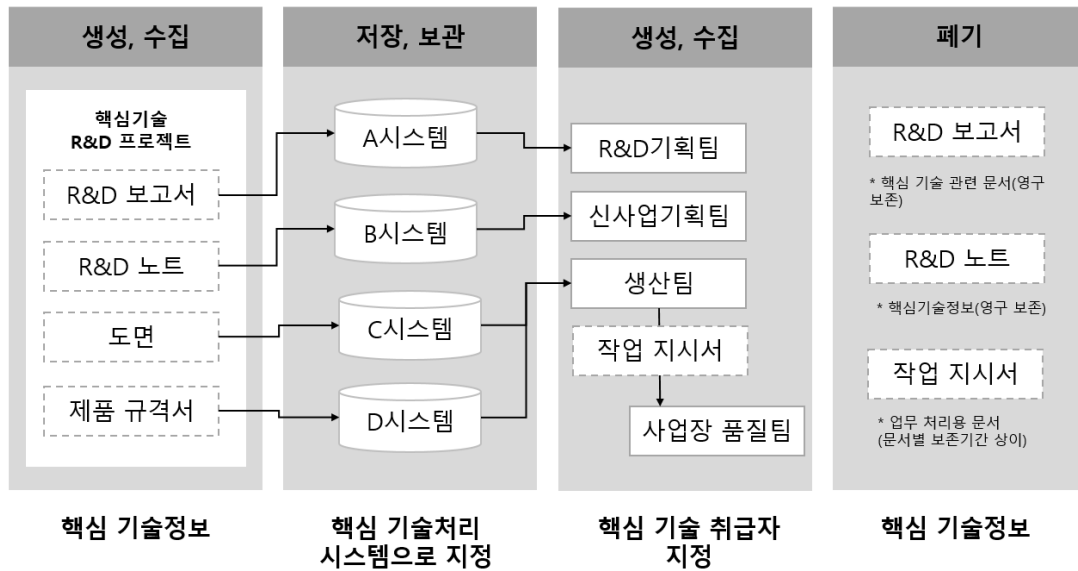
20\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.  
서약자: \_\_\_\_\_ (서명)

회사명 귀하

[별첨 4] 핵심기술 식별 및 관리 프로세스(예시)



[별첨 5] 핵심기술정보 Life-Cycle(예시)



## [별첨 6] 핵심기술 유출 실태와 원인분석

### □ 불법적인 기술탈취

(유형 ①) 내부자(전·현직 임직원)에 의한 기술 탈취

(사례) 의료기기 제조업체 A사의 연구소장이 퇴사후 경쟁업체 B사의 기술 자문으로 활동하면서 B사에서 유사 제품 출시

(원인분석/정책 방향) 기술인력에 대한 적절한 관리 및 보상 부재

→ 보안관리 노력 강화 및 경업금지 약정 체결 활성화, 보상체계 보완

(유형 ②) 외부자(협력업체 및 경쟁업체 등)에 의한 기술 탈취

(사례) 디스플레이 검사장비업체 O사의 직원이 국내 S사와 L사의 AM-OLED기술을 USB에 담아 유출하여 해외 경쟁업체로 유출

(원인분석/정책 방향) 협력업체의 취약한 보안 의식 및 수준

→ 협력업체의 보안관리 강화 및 보안 수준 제고 지원

### □ 거래 과정에서의 기술 유출

(유형 ③) 하도급 거래 과정에서의 기술 유출

(사례) 대기업 L사가 배터리라벨 제조 중소기업 S사에 대한 품질관리 명목으로 기술자료 제공 요구, 취득한 기술로 중국 자체 생산에 유용

(원인분석/정책 방향) 갑을관계 관행으로 하도급업자의 법적 권리행사 곤란

→ 기술자료 제공 요구 및 유용행위에 대한 적발·감시 강화

(유형 ④) 공동연구 과정에서의 기술 유출

(사례) 교수 K씨가 지하철 광고 시스템 개발 중소기업 A사와 센서 기술 공동연구를 통해 취득한 신기술을 동의 없이 개인 명의로 특허 등록

(원인분석/정책 방향) 비밀유지 약정 미체결 및 공유기술 범위 명시 미흡

→ 비밀유지약정 보편화, 권리자의 신속한 권리회복제도 도입

(유형 ⑤) 기술 자문 과정에서의 기술 유출

(사례) 기술닥터 P가 개발업체 B사의 기술자문 과정에서 취득한 부품 세척기 신기술을 B사 몰래 특허 출원한 뒤 미국 환경회사에 유출

(원인분석/정책 방향) 인식 부족 및 비밀유지 약정 미체결

➔ 표준계약서(비밀유지약정 포함) 보급, 기술관리 가이드라인 보급

(유형 ⑥) 사업 제안 과정에서의 기술 유출

(사례) 모바일게임 개발업체 C사가 업무제휴를 위해 M사에 기획서 및 핵심자료를 제공하였으나, 협의없이 C사의 유사게임을 해외에서 출시

(원인분석/정책방향) 계약체결 이전 단계에서의 기술보호 인식부족

➔ 비밀유지약정 체결 및 제공된 기술자료 보호를 위한 근거 마련

(유형 ⑦) M&A 과정에서의 기술유출

(사례) 상하이 자동차가 쌍용차 인수 후 고용유지와 신차개발 투자를 약속. 그러나 구조 조정 실시 및 투자 약속 불이행, 완성차 생산기술과 하이브리드 관련 기술 등을 유출하고 09년 법정관리 신청 후 철수

(원인분석/정책방향) 외국 투자 위축 우려로 소극적 규제

➔ M&A시 신고대상 확대 검토 (현재, 국가연구개발비를 지원받은 국가핵심기술의 해외 M&A의 경우로 한정)

(유형 ⑧) 기술수출 과정에서의 기술유출

(사례) 국가핵심기술의 해외수출 및 M&A추진시 고의로 행정절차를 회피 또는 관련 제도를 인지하지 못해 사전 미신고·승인상태에서 수출

(원인분석/정책 방향) 기업의 제도 인지 부족

➔ 국가핵심기술에 대한 모니터링 강화 및 제도 안내 강화

## [별첨 기] 핵심기술 유출 대응 절차(예시)

