개발환경 보안 자체 점검목록

신청제품 명칭

V1.0

YYYY. MM. DD.

신청기관 명칭

「보안기능 시험제도 운영 지침」에 의하여 개발환경 보안 자체 점검 목록을 제출하며 기재사항에 허위가 없음을 확인하였습니다.

년 월 일

작성자

작성자

작성자

작성자

작성자

1장

개발환경 보안 자체 점검목록 개요

「개발환경 보안 자체 점검목록」은 아래와 같이 4개 분야 84개 항목으로 구성되며, 각 항목들은 점검 내용에 따라 '1단계' 또는 '2단계'로 분류됩니다.

<개발환경 보안 자체 점검목록 분야 및 항목수>

분야	항목 수	주요 내용	단계별 항목 수
1. 일반사항	6	신청기관 정보, 제품 개발·생산 방식 등	1단계 6 2단계 0
2. 신청기관 보안관리 체계	17	신청기관이 자체 정보보안 수준을 강화하기 위해 필요한 △내부 지침 △기술적 수단 등의 보안대책에 대한 점검항목	1단계 11 2단계 6
3. 신청제품 개발환경 보안	51	신청기관이 신청제품 개발·생산을 위한 개발환경을 안전하게 구축하고, 사이버 위협요인으로 인한 침해사고 대응하며, 수급자에 배포하는 제품의 무결성, 안전성을 유지하기 위해 점검해야 할 항목	1단계 27 2단계 24
4. 신청제품 공급망 관리	10	신청기관이 신청제품 개발·생산과정에서 공급망으로부터의 사이버 위협을 예방하기 위해 구성요소에 대한 △조달·소싱 △구성요소 투명성 등 점검해야 할 항목	1단계 4 2단계 6
합계	**84**		1단계 48 2단계 36

'1단계'에 해당하는 항목은 기본 항목이며 보안기능 시험 신청기관은 제출문서 중 하나인 「개발환경 보안점검 자체 점검목록」 작성 시 '1단계'에 해당하는 항목을 모두 작성해야 합니다.

'2단계'에 해당하는 항목은 추후 신청기관 개발환경 보안을 강화하기 위해 항목으로 별도의 안내가 있을 때까지 신청기관에서 작성하지 않아도 무방합니다. 다만, 신청기관에서 이미 '2단계'에 해당하는 항목과 관련된 절차 등을 보유하고 있는 경우 자유롭게 작성할 수 있습니다.

'1. 일반사항'의 점검항목은 해당되는 내용을 기입합니다.

‘2. 신청기관 보안관리 체계’, ‘3. 신청제품 개발환경 보안’, ‘4. 신청제품 공급망 관리’의 점검항목은 다음을 참고하여 선택항목을 선택하고 세부 내용을 기입합니다.

신청기관의 자체 점검 수준은 ‘문서’, ‘관행’, ‘없음’ 중 선택하고 주요 내용을 기입합니다.

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

['문서'를 선택한 경우] 신청기관의 관련 문서를 식별하고 주요 내용을 간략히 기입합니다.

['관행'을 선택한 경우] 사내에서 적용 중인 지식·절차가 있으나 문서화되지 않은 경우 주요 내용을 기입합니다.

'문서'와 '문서화되지 않은 절차'가 모두 존재하는 경우 두 가지 항목을 모두 선택할 수 있습니다.

['없음'을 선택한 경우] 해당되는 내용이 없는 경우 '없음'을 선택합니다.

1. 일반사항

■ 신청기관 일반사항

1.1 1단계

신청기관이 속한 국가 및 소재지 주소

점검 가이드

신청기관이 속한 국가와 주소를 기입하시기 바랍니다.

외국계 기업의 한국 법인(또는 지사)인 경우 모기업이 속한 국가와 주소를 함께 기입하시기 바랍니다.

자체 점검결과

신청기관	국가	
	주소	
모기업 (해당시)	국가	
	주소	

1.2 1단계

신청제품의 개발기관 및 개발국가

점검 가이드

항목 선택 시 다음을 참고하여 선택하고 세부 내용을 기입하시기 바랍니다.

[1번 선택 시] 신청제품 개발과 관련된 본사, 지소 등 소재지가 여러 장소에 분포하는 경우 구분하여 기입하시기 바랍니다.

[2번 선택 시] 외부 개발자의 국적을 기입하시기 바랍니다.

[3번 또는 4번 선택 시] 개발에 참여한 개발기관 및 개발국가를 모두 기입하시기 바랍니다.

[5번 선택 시] 개발 방식을 직접 서술하시고 개발기관 및 개발국가를 모두 기입하시기 바랍니다.

자체 점검결과

o 신청제품 개발방식은 아래 다섯 가지 중 하나를 선택하시기 바랍니다.

☐ 1. 신청기관에 속한 개발자가 신청제품 전체 직접 개발

☐ 2. 신청기관에 속한 개발자와 프리랜서 등과 같은 소속기관이 없는 외부 개발자가 함께 신청제품 개발

☐ 3. 신청기관에서 신청제품 일부는 직접 개발, 일부는 외부 개발업체 활용하여 개발

☐ 4. 신청제품 전체 외부 개발업체 활용하여 개발

☐ 5. 기타

o 위 선택항목에 따른 자체 점검 내용을 서술하시기 바랍니다.

1.3 1단계

신청제품의 생산기관 및 생산국가

점검 가이드

항목 선택 시 다음을 참고하여 선택하고 세부 내용을 기입하시기 바랍니다.

[1번 선택 시] 신청제품 생산과 관련된 본사, 지소, 공장 등 소재지가 여러 장소에 분포하는 경우 구분하여 기입하시기 바랍니다.

[2번 선택 시] 생산에 참여한 생산기관 및 생산국가를 모두 기입하시기 바랍니다.

[3번 선택 시] 생산 방식을 직접 서술하시고 생산기관 및 생산국가를 모두 기입하시기 바랍니다.

자체 점검결과

o 신청제품 생산방식은 아래 세 가지 중 하나를 선택하시기 바랍니다.

☐ 1. 신청제품 직접 생산

☐ 2. 신청제품 위탁 생산

☐ 3. 기타

o 위 선택항목에 따른 자체 점검 내용을 서술하시기 바랍니다.

1.4 1단계

신청기관의 전체 직원 수 및 개발자 수

점검 가이드

신청기관에 속한 전체 직원 수, 전체 개발자 수, 신청제품 개발자 수를 기입하시기 바랍니다.

외국계 기업의 한국 법인(또는 지사)인 경우 대한민국에서 상시 근무하는 인원을 기입하시기 바랍니다.

자체 점검결과

전체 직원	
전체 개발자	
신청제품 개발자	

1.5 1단계

신청제품의 물리적인 형태

점검 가이드

신청제품 구성요소별로 소프트웨어(S/W), 펌웨어(F/W), 하드웨어(H/W. S/W 또는 F/W가 탑재되는 하드웨어 일체형 제품의 하드웨어 부분 포함)로 구분하여 기입하시기 바랍니다.

신청제품의 형태에 따라 복수 선택 가능합니다.

예시로, 신청제품이 침입차단시스템이고 하드웨어 일체형 제품인 서버와 소프트웨어 제품인 관리콘솔로 구성된 경우, 신청제품 구성요소 중 하나인 서버의 물리적인 형태는 펌웨어 및 하드웨어이며 관리콘솔의 물리적인 형태는 소프트웨어입니다.

자체 점검결과

물리적인 형태	신청제품 구성요소
☐ 소프트웨어(S/W)	
☐ 펌웨어(F/W)	
☐ 하드웨어(H/W)	

1.6 1단계

신청기관에서 준수하고 있거나 획득한 기업체 정보보안 관련 국내/국제 표준 또는 인증

점검 가이드

기업체 정보보안 관련 인증을 획득한 경우 해당 인증을 기입해 주시기 바랍니다.

(예시) ISO/IEC 27001, ISO/IEC 28000, ISO/IEC 28001, ISO/IEC 5230, ISO/IEC DIS 18974, ISMS-P 또는 ISMS 등

획득한 인증이 없는 경우 '해당 없음'을 기입하시기 바랍니다.

자체 점검결과

2. 신청기관 보안관리 체계

■ 보안 규정

2.1 1단계

신청기관에 △물리·정보보안 △직원 채용 시 인적보안 규정이 있다.

점검 가이드

(예시) 물리적 보안 전담 부서, IT/전산 보안 전담 부서, 부서별 책임자/실무자/경비 등 물리적 보안 및 IT/전산 보안과 관련하여 책임이 있는 부서 및 직원들의 역할 및 책임 범위 등이 해당됩니다. 소속된 직원뿐 아니라 신청제품과 관련된 외부 직원에게 부과되는 보안규정(또는 관행)도 포함됩니다. 신청기관의 인사 규정(또는 관행)에 의해 소속 직원이나 프리랜서와 같은 계약직원 채용 시 인적 보안을 확인하는 경우 이와 관련된 내용이 해당됩니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 보안 규정의 준수

2.2 1단계

신청기관에 소속 직원 또는 업무와 관련한 외부 직원이 물리·정보보안에 대한 규정의 준수를 약속하는 절차가 있다.

점검 가이드

(예시) 서약서, 계약서 등이 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.3 **2단계**

신청기관의 내부 자료에 대해 △내용과 중요도에 따른 등급 부여 △등급에 따른 접근권한 차등화 등을 정한 관리 규정이 있다.

점검 가이드

(예시) 소스코드, 설계자료, QA자료, 도입기관 목록, 영업자료 등 다양한 자료를 내용과 중요도에 따라 등급을 구분하고 자료별로 접근권한이 있는 직원을 차등화하는 경우 이와 관련된 내용이 해당됩니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.4 **1단계**

신청기관이 신청제품에 대한 보안수칙을 정하고 직원 및 관련된 외부 직원에게 준수 의무를 부과하는 절차가 있다.

점검 가이드

(예시) 신청제품 개발·생산과 관련된 내부 직원 및 관련된 외부 직원 대상으로 보안수칙을 통보하고 준수의무를 부과하는 것과 관련 내용을 기입해 주시기 바랍니다. 직원에는 신청제품 개발·생산에 관련된 모든 직원(신규 인력, 기존 인력, 외근 및 재택근무 인력, 개발 참여 외부 인력 등)이 포함됩니다. 신청제품 개발·생산과 관련된 외부 공급업체, 용역업체, 하청업체 등에서 직원들에게 신청제품 보안과 관련된 의무를 부과하도록 하는 방법을 포함해야 합니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.5 **2단계**

신청기관은 보유한 IT자산에 대한 사이버 공격 인지 시 대응체계를 운영하고 있다.

점검 가이드

(예시) 자체 탐지 또는 관계기관의 통보에 의해 악성코드 유포, 해킹 시도 등 사이버 위협 탐지 시 △공격 유형 △자료 유출 여부 △심각성 등 자체 기준에 따라 신청기관에서 대응하는 체계를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.6 **1단계**

신청기관의 내부 보안을 위해 마련된 보안 관련 내부 규정은 경영진 및 임원에게도 동일하게 적용하고 있다.

점검 가이드

(예시) 지위 고하에 무관하게 동일하게 보안 규정(또는 관행)이 적용되고 있는지 여부를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 접근 통제

2.7 1단계

신청기관이 신청제품과 관련된 중요자료를 취급하는 직원은 역할 및 책임 범위에 따라 취급 권한을 부여한다.

점검 가이드

(예시) 2.3 항목에서 기입한 규정(또는 관행)과 연계하여 신청제품과 관련된 중요자료에 취급 권한을 부여하고 실제로 접근을 통제해야 합니다. 신청기관 내에 신청제품과 관련된 중요자료를 취급하는 직원에 대한 별도 심사 절차 및 취급 권한 부여 절차가 있는 경우 그 내용을 기입해 주시기 바랍니다. 제품 보안 전담 부서, CEO/보안관리자/부서장/개발팀장/개발자 등 신청제품과 관련하여 보안 책임이 있는 부서 및 직원들의 역할 및 책임 범위 등이 해당됩니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.8 2단계

신청기관이 사용하는 업무공간에 대해 보안 등급을 부여하고 소속 직원에 별도의 출입 권한을 부여하고 있다.

점검 가이드

(예시) 신청기관 내에 업무공간(사무실, 개발실, 서버실 등) 별로 보안 등급(일반구역, 제한구역, 비밀구역 등)을 부여하고 직원에 별도의 출입 권한을 부여하는 절차가 있는 경우 이를 기입해 주시기 바랍니다.

물리적인 업무공간 분리가 없어 '없음'을 선택한 경우에는 신청기관의 경우 관리적으로 업무를 분리하는 방법(개발용・업무용 PC, 서버 구분하여 사용 등)을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.9 1단계

신청기관이 소재한 건물의 시설 내에서 신청기관이 사용하는 구역에 물리적 보안시스템을 운용하고 있다.

점검 가이드

(예시) 생체인식(지문/안면 등), 키패드, 스마트카드 등으로 출입자를 식별하는 장치가 설치된 출입문, 출입이 가능한 지점을 감시하는 감시카메라(CCTV 등), 허가받지 않은 출입자에 대한 경보장치, 회사 내부를 정기·수시 순찰하는 경비 등 해당하는 내용을 기입해 주시기 바랍니다. 외부 방문객에게 허용된 구역, 일반 직원에게 허용된 구역, 개발·생산 직원에게 허용된 구역 등 건물 내에 보안 등급이 다른 구역을 구분하고 있는 경우 구역별로 물리적 보안시스템을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.10 1단계

신청기관은 업무 목적으로 방문하는 외부인에 대해 적용하는 보안 절차가 있다.

점검 가이드

(예시) 협력·납품·하청업체 직원, 신청기관에서 고용한 외부 프리랜서 등 업무 목적으로 방문하는 외부인이 신청기관의 제한구역(서버실, 개발실 등)에 접근하는 경우 출입을 통제하는 절차를 포함하여 보안 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.11 2단계

신청기관은 업무 목적으로 방문하는 외부인에 대해 내부 전산망 접근권한을 별도로 부여하고 있다.

점검 가이드

(예시) 협력·납품·하청업체 직원, 신청기관에서 고용한 외부 프리랜서 등 업무 목적으로 방문·접속하는 외부인이 신청기관의 내부 전산망에 접근하는 경우 접근권한을 관리하는 방법을 기입해 주시기 바랍니다. 신청기관에서 신청제품 개발을 위해 도입한 ICT 제품·서비스를 직접 구축·운용·유지보수하지 않는 경우 외부 업체 직원의 지원을 받을 수 있으며, 외부 업체 직원의 계정이 신청기관의 내부망 해킹 등에 악용되지 않도록 관리하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.12 **2단계**

신청기관은 내부 전산망 접근권한을 부여받은 외부인이 더이상 접근권한이 필요하지 않을 경우 접근권한 회수 절차를 시행하고 있다.

점검 가이드

(예시) 협력·납품·하청업체 직원, 신청기관에서 고용한 외부 프리랜서 등 업무 목적으로 접근권한을 부여받은 외부인이 더이상 신청기관의 내부 전산망에 접근할 필요가 없는 경우 접근권한을 어떻게 회수하는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **교육·훈련**

2.13 **1단계**

신청기관은 소속 직원 및 외부 공급·용역·하청업체를 대상으로 수시 또는 정기적으로 보안 교육을 실시한다.

점검 가이드

(예시) 교육 시기, 교육 자료, 교육 참석자 확인 등 전반적인 교육 절차를 기입해 주시기 바랍니다. 개발인력(신청제품 개발과 관련된 외부 공급업체, 용역업체, 하청업체 등 포함)에 대해 공

급망 보안과 관련된 인식 교육을 포함할 것을 권고합니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 기술적 수단

2.14 **2단계**

신청기관은 보유한 IT 자산을 사이버 공격으로부터 보호하기 위해 해킹 공격을 탐지·대응하는 기술적 수단을 운용하고 있다.

점검 가이드

(예시) 신청기관에서 보유한 해킹 공격에 탐지·대응하는 기술, 제품 등을 기입해 주시기 바랍니다. 예를 들어, 방화벽·IPS·EDR 등 네트워크 주요 지점에서 공격을 탐지·차단하는 체계를 구축하고 운용할 수 있습니다. 또한, 운영체제 또는 브라우저가 제공하는 '원격 데스크톱 서비스'를 사용하지 못하도록 차단, 개발자 PC에 취약한 계정 사용하지 않도록 요구하는 등의 조치를 취할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.15 **1단계**

신청기관은 소속 직원이 반드시 로그인한 후 PC·서버를 사용하도록 한다.

점검 가이드

(예시) ID/패스워드, FIDO 디바이스, 생체인식(지문/홍채 등) 입력장치, 웨어러블 디바이스 등 신청기관에서 로그인 수단으로 사용 중인 방법을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음

주요 내용	

2.16 1단계

신청기관은 소속 직원이 사용하는 PC·서버에 설치된 주요 소프트웨어를 수시로 업데이트하고 있다.

점검 가이드

(예시) 운영체제, 안티바이러스 제품 등 주요 소프트웨어를 업데이트하도록 하는 신청기관의 방식을 기입하시기 바랍니다. 예를 들어, 패치관리시스템 등 자동화된 패치체계를 운용하거나, 사내 보안 전담 부서 주관 아래 각 직원이 자율적으로 업데이트하거나, PC·서버를 운용하는 직원이 판단하여 자율적으로 업데이트하는 등의 방식이 있을 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

2.17 1단계

신청기관은 보유한 PC·서버에 대한 악성코드 감염을 예방·대응할 수 있는 보안 조치를 적용하고 있다.

점검 가이드

(예시) 랜섬웨어를 포함하여 악성코드를 탐지하고 대응하는 보안제품(예: 안티바이러스 제품, 랜섬웨어 대응제품 등)을 설치, 중요자료 탈취에 대비하여 백업 시스템을 구축, 운영체제 또는 브라우저가 제공하는 '원격 데스크톱 서비스'를 사용하지 못하도록 차단, 개발자 PC에 취약한 계정 사용하지 않도록 요구하는 등의 조치를 취할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3. 신청제품 개발환경 보안

■ 개발 · 생산

3.1 1단계

신청기관은 개발 · 생산과정에 형상관리체계를 갖추고 있으며 신청제품에 적용하고 있다.

점검 가이드

(예시) 형상관리체계에서 도구(형상관리 도구, 버전관리 도구 등)를 형상관리시스템으로 사용하는 경우 도구 명칭과 도구 활용 방법을 기입해 주시기 바랍니다. 도구와 같은 형상관리시스템을 사용하고 있지 않은 경우 형상관리 방법을 기입해 주시기 바랍니다. 형상관리체계에 의해 신청제품의 형상이 변경된 경우 버전의 유일성을 추적할 수 있어야 하며, 보안기능 확인서 발급제품과 운용제품의 형상이 상이한 경우 어떤 부분이 변경되었는지 추적할 수 있어야 합니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.2 1단계

신청기관은 운영하는 형상관리체계에서 업무 목적으로 접속하는 외부인의 접근권한을 업무에 맞게 설정하여 부여한다.

점검 가이드

(예시) 형상관리체계에서 도구(형상관리 도구, 버전관리 도구 등)를 형상관리시스템으로 사용하는 경우 협력 · 납품 · 하청업체 직원, 신청기관에서 고용한 외부 프리랜서 등 업무 목적으로 형상관리시스템에 접속하는 외부인에게 업무에 적합하게 접근권한을 부여하는지 기입해 주시기 바랍니다. 도구와 같은 형상관리시스템을 사용하지 않는 경우 외부인이 관리대상 형상항목에 접근 시 어떻게 접근권한을 부여하고 관리하는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.3 1단계

신청기관은 신청제품의 소스코드 또는 하드웨어 설계도면에 대한 비인가자의 접근을 통제하는 수단을 운용하고 있다.

점검 가이드

(예시) 형상관리체계에서 도구(형상관리 도구, 버전관리 도구 등)를 형상관리시스템으로 사용하여 각 사용자의 업무에 따라 접근권한을 부여하거나, 접근권한이 부여되는 별도의 저장시스템(파일서버 또는 클라우드 스토리지 등)을 두어 보관하는 등의 방법을 사용할 수 있습니다. 신청기관에서는 소스코드 또는 하드웨어 설계도면 저장소에 대한 접근을 통제하고 빌드 시스템에 대한 공격에 대응하는 방법을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.4 1단계

신청기관은 신청제품의 소스코드 · 설계도 등 중요자료가 유출된 경우, △제품에 미치는 보안 영향 판단 △제품 수정 · 보완하는 등의 절차가 있다.

점검 가이드

(예시) 신청제품의 소스코드 · 설계도 등 중요자료가 유출되었으면 자체 개발한 부분 또는 오픈소스 활용 부분 등에 따른 보안 영향을 분석, 제품의 일부 또는 전부 보완 필요성을 검토하고 판단, 고객사 패치 필요성을 결정하는 등 신청제품에 적용하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.5 1단계

신청기관은 신청제품의 소스코드 · 설계도 등 중요자료가 유출된 경우, 기존 보안체계를 점검하여 보완하는 절차가 있다.

점검 가이드

(예시) 신청제품의 소스코드·설계도 등 중요자료가 유출된 경우 재발 방지를 위해 내부 보안 체계를 개선하는 등의 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.6 **2단계**

신청기관이 신청제품에 대한 SBOM 또는 HBOM을 활용하여 설계상에 없거나 취약점이 발견된 구성요소를 식별하는 절차가 있다.

점검 가이드

(예시) 신청기관에서 SBOM 또는 HBOM을 활용하여 신청제품의 개발·생산 시 취약점을 관리하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.7 **1단계**

신청기관이 신청제품 개발·생산과정에서 불가피하게 기존 설계에 없거나 승인되지 않은 구성요소(H/W·S/W 모듈)를 추가할 경우, 이를 점검하고 승인하는 절차가 있다.

점검 가이드

(예시) 추가되는 구성요소의 출처 확인, 취약점 점검 등 제품의 보안을 손상시키지 않음을 확인하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음

주요 내용	

3.8 2단계

신청기관은 신청제품 개발·생산 구역의 네트워크에 연결된 IT자산에서 생성·저장·소통되는 자료의 보호를 위해 별도의 통신경로를 구축, 운영하고 있다.

점검 가이드

(예시) 유선 및 무선 네트워크, 이동통신사 네트워크 등 포함하여 네트워크를 물리적·논리적으로 분리하여 운영하는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.9 1단계

신청기관은 신청제품의 일부 구성요소 중 외부에서 제공받는 구성요소의 위해성을 확인하는 절차가 있다.

점검 가이드

(예시) 위해성이란 구성요소에 내재된 악성코드, 취약점, 백도어 등을 의미합니다. 신청제품의 일부 구성요소를 외부 업체로부터 제공받는 경우 제공받는 구성요소의 위해성을 확인하는 절차나 수단을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.10 2단계

신청기관은 신청제품에 포함되는 오픈소스의 라이선스 규정을 준수하고 있다.

점검 가이드

(예시) 라이선스 준수란, 상용화에 따른 조건 준수, 수정된 소스코드의 공개, 공개적인 준수 선언 등을 의미합니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.11 **1단계**

신청기관은 신청제품에 활용되는 오픈소스에 대해 관련 웹페이지 및 기술커뮤니티 등을 통해 취약점 정보를 상시 모니터링하고 있다.

점검 가이드

(예시) 신청제품의 보안을 강화하기 위해 제품에서 활용하는 오픈소스 관련 공개된 최신 취약점 정보를 확인하고 주의하는 방법을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.12 **1단계**

(외부 전문업체에 H/W 설계 또는 Artwork를 위탁하는 경우) 신청기관은 수탁업체에서 준수해야 할 보안 항목을 통보하고 준수 절차를 마련, 운영한다.

점검 가이드

(예시) 수탁업체가 준수해야 할 보안 항목을 정하고 이를 준수하여 줄 것을 요청, 수탁업체가 준수해야 할 보안 항목을 정하지는 않지만 수탁업체로부터 자체 보안정책 및 현황 등을 통보받음, 수탁업체와 협의하여 준수해야 할 보안 항목을 정하고 문서(계약 또는 공문 등)로 보증 등 적용 중인 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.13 **1단계**

신청기관은 신청제품을 타 업체가 개발·생산하는 제품의 일부 구성요소로 제공할 경우 출하 전, 위해성을 확인하는 절차가 있다.

점검 가이드

(예시) 위해성이란 구성요소에 내재된 악성코드, 취약점, 백도어 등을 의미합니다. 신청기관에서 신청제품을 개발·생산하여 외부 업체에게 제공하는 경우 제공하는 구성요소의 위해성을 확인하는 절차나 수단을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.14 **1단계**

신청기관은 신청제품의 공격 경로를 최소화하기 위해 검토하는 절차가 있다.

점검 가이드

(예시) 신청기관은 신청제품에 개발자 모드 제거, 취약점 점검 도구를 활용한 기능·포트·프로토콜·서비스 점검, 시큐어 코딩 적용 등을 수행하는 등 신청제품의 공격 경로를 최소화하기 위한 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.15 1단계

신청기관은 ①부서간 ②본사-지사, 지사-지사간 ③외부 공급·하청업체간 신청제품의 개발·생산 관련 중요자료를 전달하는 절차가 있다.

점검 가이드

(예시) 보안 저장매체 사용, 자료 암호화 전송 등 안전하기 전달하기 위한 절차 등이 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **배포·유통**

3.16 1단계

신청기관은 신청제품을 수급자에게 안전하게 전달하기 위한 배포(출하) 절차가 있다.

점검 가이드

신청제품의 배포(출하) 절차는 아래 두 가지 중 해당하는 항목을 선택하시기 바랍니다.

1. 신청기관이 신청제품을 직접 수급자에게 배포(출하)
2. 신청기관이 신청제품을 배송 전문업체에게 위탁하여 수급자에게 배포(출하)

(예시) 신청기관과 수급자 간에 또는 신청기관과 배송 전문업체 간에 신청제품의 배포(출하)에 대해 ①서면(이메일 포함)으로 통보하거나 ②계약사항에 기재하거나 ③양자간 서면약속·공문 교환 등의 방법으로 공유할 수 있습니다. 신청기관은 신청제품의 배포(출하) 과정에서 발생할 수 있는 사고(분실·무단 대체 등)에 대해 책임소재 규정 및 책임추적 절차를 ①서면(이메일 포함)으로 통보하거나 ②계약사항에 기재하거나 ③양자간 서면약속·공문 교환 등의 방법으로 공유할 수 있습니다. 신청기관이 신청제품을 배포하고, 제품의 분실·무단 대체 등 사고에 대응하기 위한 세부 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.17 2단계

신청기관은 신청제품의 온라인 배포 또는 업데이트를 위해 운용 중인 모든 서버(Cloud Instance 포함)에 대해 △사용자별 권한 관리 △인증 수단 적용 △취약점 점검 등의 절차가 있다.

점검 가이드

(예시) 신청기관에서 소프트웨어 또는 펌웨어를 온라인으로 배포하거나, 운용 중인 제품을 온라인으로 업데이트하는 경우 안전하게 온라인으로 배포·업데이트하기 위한 방법을 기입해 주시기 바랍니다. 온라인 배포·업데이트 시 신청기관에서 개발·생산한 정당한 제품만이 서버를 통해 수급자에게 전달되도록 서버에 접근하는 사용자를 관리해야 합니다. 신청기관은 온라인 배포·업데이트를 위해 운용 중인 모든 서버의 취약점을 점검하여 서버를 통한 악성코드 유포 시도 등의 해킹으로부터 서버를 보호해야 합니다. 이와 관련된 절차 등을 기입해 주시기 바랍니다.

'없음'을 선택한 경우, 온라인 배포·업데이트를 수행함에도 관련 절차가 부재한 경우와, 오프라인으로만 신청제품을 배포·업데이트하므로 온라인 배포·업데이트를 위한 서버가 불필요하여 운용하지 않는 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.18 1단계

신청기관은 신청제품의 배포 또는 업데이트 절차에 착수하기 전, 제품에 대해 △계획되지 않은 구성요소의 변경(무결성) 및 △악성코드·취약점·백도어 등(위해성)의 잔존 여부를 확인한다.

점검 가이드

(예시) 신청기관에서 신청제품을 새롭게 릴리즈하거나 제품을 업데이트하여 릴리즈 하기 전에 무단으로 손상되지 않은 정확한 제품이 릴리즈될 수 있도록 확인하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 결함 대응

3.19 1단계

신청기관은 배포한 제품이 운용 중 취약점이 발견되거나, 취약점으로 인한 해킹사고가 발생한 경우 해당 취약점을 제거하고 제품을 보완하며, 취약점에 대응하는 조직을 운영한다.

점검 가이드

(예시) 신청기관에서 릴리즈한 제품에 취약점 발생 시 대응하기 위한 조직을 의미하며, 기존의 개발팀, 별도의 대응팀 등 신청기관의 운영 중인 조직을 기입해 주시기 바랍니다. 대응 조직이 없는 경우 취약점에 누가 어떻게 대응하는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 안전한 개발환경 구축

3.20 2단계

신청기관은 신청제품 개발·생산을 위해 도입해야 하는 ICT 제품·서비스를 식별하고 이에 대한 도입기준과 절차가 있다.

점검 가이드

(예시) 신청기관에서 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)를 도입하기 위해 준수하는 내부 규정(또는 관행)이 있는 경우 이를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.21 2단계

신청기관은 신청제품 개발·생산을 위해 도입 예정인 ICT 제품·서비스를 성능 확인 등의 목적으로 계약 이전에 시범 설치·운용할 경우, △운용 기간 △운용 전산 환경 △설치·철거 절차가 있다.

점검 가이드

(예시) 신청기관은 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)를 도입하기 위해 성능 확인 등을 목적으로 시범적으로 설치 및 운용할 수 있습니다. 이때 적용하는 내부 규정(또는 관행)이 있는 경우 이를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.22 **1단계**

신청기관은 신청제품 개발·생산을 위해 필요한 △ICT 제품·서비스 도입 △시범 설치·운용 시, 공급자와 △지식 재산권 △소유권 △사용 권한의 범위 등을 합의하고 이를 서면으로 기록한다.

점검 가이드

(예시) 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 개발 서버, 클라우드 서비스 등)를 도입하기 위한 계약서에 관련 내용을 포함할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.23 **2단계**

신청기관은 신청제품 개발·생산을 위해 필요한 △ICT 제품·서비스 도입 △시범 설치·운용 시, 공급자와 △취약점 등 결함 대응책임 △해킹사고 발생 시 상호 간의 책임소재 등을 합의하고 이를 서면으로 기록한다.

점검 가이드

(예시) 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)를 도입하기 위한

계약서에 관련 내용을 포함할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.24 **2단계**

신청기관과 신청제품 개발·생산을 위해 필요한 ICT 제품·서비스 공급자가 맺은 계약에 △개발자(업체) △공급·유통 관계자(업체) △도입 ICT 제품·서비스 연계 정보시스템 제공자(업체) △시스템 설치 관계자(업체) 등의 정보시스템 보안 수준에 대한 요구사항이 수록되어 있다.

점검 가이드

(예시) 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)를 도입하기 위한 계약서에 관련 내용을 포함할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.25 **2단계**

신청기관은 신청제품 개발·생산을 위해 도입하는 ICT 제품·서비스에 대한 △인수기준 △검증 절차 등을 마련하여 적용한다.

점검 가이드

(예시) 신청기관에서 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등) 도입 시 검수하고 검증하기 위해 준수하는 내부 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음

주요 내용	

3.26 2단계

신청기관은 신청제품 개발·생산을 위해 필요한 ICT 제품·서비스 공급자가 제출하는 SBOM에 대해 △열람 권한 △활용 권한 △제3자 유출금지 등 보안 유지를 서면으로 합의한다.

점검 가이드

(예시) 신청기관은 신청제품 개발·생산에 필요하여 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)의 취약점을 지속적으로 관리하기 위해 공급자에게 SBOM 제출을 요청할 수 있으며 SBOM 활용을 위한 제반 사항을 계약서 등에 포함할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.27 2단계

신청기관은 신청제품 개발·생산을 위해 필요한 ICT 제품·서비스에 대해 △공급자 △공급자가 제공하는 ICT 제품·서비스의 배제기준을 수립, 적용한다.

점검 가이드

(예시) 신청기관은 공급자 주재국 정부 정책에 의한 영향, 준법성, 공급자 경영 지배구조 등을 고려하여 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 개발 서버, 클라우드 서비스 등)를 공급하는 공급자 선정 시 적용할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.28 2단계

신청기관은 자사의 공급망 안정성을 유지하기 위하여 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스와 동종·동일 기능을 제공하는 대체 공급업체 선정 등의 대책을 마련하였다.

점검 가이드

(예시) 신청기관에서 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)가 신청제품 개발 및 유지보수에 중요한 역할을 하는 경우 해당 ICT 제품·서비스의 공급이 중단된 경우 신청제품의 개발 및 유지보수에 중대한 차질이 발생할 수 있습니다. 이처럼 공급망 안정성 유지를 위해 대체 공급업체 선정 등의 대책을 마련하고 있는지 기입하시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.29 2단계

신청기관은 신청제품 개발·생산을 위해 필요한 ICT 제품·서비스 도입 시 △보안기능 확인서 △CC인증 등의 사전인증제도를 통해 보안기능과 안전성이 확인된 ICT 제품·서비스를 도입한다.

점검 가이드

(예시) 신청기관은 다양한 제도 또는 검증 절차를 통해 신청제품 개발·생산을 위해 검증된 ICT 제품·서비스를 도입할 수 있으며, 신청기관에서 적용 중인 기준을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.30 2단계

신청기관은 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스가 목적에 맞게 운용되고 오·남용되지 않도록 △운용기준 △운용 절차 등이 있다.

점검 가이드

(예시) 신청기관에서 신청제품 개발·생산에 필요한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)를 운용하기 위해 준수하는 내부 규정(또는 관행)이 있는 경우 이를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.31 **2단계**

신청기관은 신청제품 개발·생산을 위해 보유한 IT자산에 신청기관이 인가하지 않은 S/W가 설치되지 않도록 관리한다.

점검 가이드

(예시) 신청기관은 IT 자산을 관리하는 솔루션 등을 활용하거나 내부 규정(또는 관행)을 통해서 인가받지 않은 S/W가 설치되지 않도록 관리할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.32 **1단계**

신청기관의 신청제품 개발·생산을 위해 보유한 IT자산에 설치된 S/W에 대해 공급자가 인정·발급하는 사용 권한을 가지고 있다.

점검 가이드

(예시) 사용 권한의 예로는 합법적인 절차를 통해 구입한 라이선스 등이 있습니다. 신청기관에서 사용하는 S/W의 사용 권한을 어떤 수준으로 확보하고 있는지 기입해 주시기 바랍니다. 예를 들어, 모든 S/W, 업무상 중요한 S/W, 없음 등 사용 권한을 확보한 S/W의 범주를 기입할 수 있습니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.33 **1단계**

신청기관은 소속 직원이 신청제품 개발·생산을 위해 사용 권한이 없는 S/W를 사용 가능토록 임의 조작하는 것을 금지한다.

점검 가이드

(예시) 신청기관에서 S/W 라이선스를 구입한 사실이 없거나 만료된 경우 크랙 등과 같은 임의 조작을 통해 소속 직원이 사용하지 못하도록 하는 방법을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.34 **2단계**

신청기관은 중요 구역에서 지정된 정보통신기기 외 다른 정보통신기기의 반입·사용을 금지하거나 특정 정보통신기기의 반입·사용을 금지하는 정책을 수립하고 실효적으로 운영하고 있다.

점검 가이드

(예시) 신청기관은 예를 들어 개발실과 같은 중요 구역에 반입·사용되는 정보통신기기를 제한할 수 있습니다. 관련 절차가 있는 경우 내용을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 운용 안전성 유지

3.35 2단계

신청기관은 신청제품 개발·생산을 위해 도입하는 ICT 제품·서비스의 공급과정 및 운용 중에 발생할 수 있는 보안 위협을 상정한 대책이 있다.

점검 가이드

(예시) 신청기관에서 신청제품 개발·생산을 위해 도입하는 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)의 공급과정에서 발생할 수 있는 △사전 통보되지 않은 제품변경 △합의되지 않은 배포 절차 변경 △악성코드 오염 등과 같은 보안 위협에 대비하기 위한 대책을 기입해 주시기 바랍니다. 신청기관은 도입한 ICT 제품의 운용 중에 취약점이 발견되거나, 취약점으로 인한 해킹사고가 발생한 경우 해당 취약점을 제거하고 제품을 보완하는 방법을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.36 1단계

신청기관은 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스에 대한 자동화된 업데이트 및 패치 절차가 있다.

점검 가이드

(예시) 신청기관에 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)의 공급자 정책에 따라 자동화된 업데이트 및 패치 제공 여부가 달라질 수 있으며, 자동화된 업데이트 및 패치가 가능한 ICT 제품·서비스의 경우 이를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요			

내용	

3.37 2단계

신청기관은 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스의 취약점을 수시 점검하고 발견된 취약점은 △공급자 책임 유무 △위험성 △발현 가능성 △시급성 등을 종합판단, 조속한 시일 내에 제거한다.

점검 가이드

(예시) 신청기관에서 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)의 취약점을 점검하는 절차와 취약점 발견 시 조치 방안을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.38 1단계

신청기관은 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스의 유지보수 등을 원격지에서 수행해야 하는 경우, 안전한 원격 접근 방식을 적용하고 있다.

점검 가이드

(예시) 신청기관에서 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)의 유지보수를 원격지에서 수행해야 하는 경우 안전하게 원격 접근할 수 있도록 하는 방법을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.39 1단계

신청기관은 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스 등을 운용하면서 발생한 로그 기록을 유지하고 검토한다.

점검 가이드

(예시) 신청기관에서 신청제품 개발을 위해 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)에서 발생한 로그 기록을 유지하고 검토하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.40 1단계

신청기관은 신청제품 개발·생산을 위해 도입한 ICT 제품·서비스의 중단 등 예기치 못한 상황 발생 시 공급자의 지원을 받아서 복구하는 절차가 있다.

점검 가이드

(예시) 신청기관에서 신청제품 개발을 위해 도입한 ICT 제품·서비스(컴파일 도구, 빌드 도구, 형상관리 도구, 버전관리 도구, 시험 도구, 취약점 점검 도구, 개발 서버, 클라우드 서비스 등)에 고장, 장애 등과 같은 사고 발생 시 복구하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **백업**

3.41 1단계

신청기관은 신청제품과 관련된 자료를 백업하는 절차가 있다.

점검 가이드

(예시) 신청기관에서 신청제품 개발·생산에 필요한 자료를 백업하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **폐기**

3.42 **1단계**

신청기관은 신청제품 개발·생산을 위해 운용 중인 IT 자산과 자료의 폐기를 위한 절차가 있다.

점검 가이드

(예시) 신청기관은 개발 서버, 개발자 PC, 보안장비 등 IT 자산의 수명이 다한 경우 △폐기 대상 선정 △재활용 여부 판단 △잔존 데이터 확인·완전 삭제 등과 같은 방법으로 안전하게 폐기할 수 있습니다. 이와 관련된 신청기관의 규정·지침 또는 관행 등을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **침해사고 대응 정책**

3.43 **2단계**

신청기관은 침해사고 대응을 위한 내부 지침 또는 매뉴얼에 따라 사고 유형·규모별로 공급자가 포함된 대응 및 복구훈련을 실시한다.

점검 가이드

(예시) 신청기관에서 공급자와 함께 공급망 침해사고 대응 및 복구훈련을 실시하기 위한 내부 지침 또는 매뉴얼이 있는 경우 문서를 식별하고 내용을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.44 1단계

신청기관은 내부자에 의한 침해사고 발생 시 행위자를 추적하여 식별하고 내부 지침 또는 매뉴얼에 따라 조치(예:직무수행 조정 등)한다.

점검 가이드

(예시) 신청기관에서 내부자에 의한 침해사고 발생 시 조치하기 위한 내부 지침 또는 매뉴얼이 있는 경우 문서를 식별하고 내용을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.45 2단계

신청기관은 공급망으로부터 전이된 위협요인에 의한 침해사고 발생시 도입 계약에 의거, 공급자에게 책임추적을 요구한다.

점검 가이드

(예시) 신청기관에서 공급망 침해사고와 관련하여 공급자에게 책임을 추적(예: 1차 공급자 → 2차 공급자 → ...)하도록 요구할 수 있는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.46 2단계

신청기관은 공급망으로부터 전이된 위협요인에 의한 침해사고 발생에 대한 대응계획과 이행에 필요한 요구사항을 공급자에게 서면으로 통보한다.

점검 가이드

(예시) 신청기관에서 공급망 침해사고 발생 시 대응계획과 이행에 필요한 요구사항을 공급자에게 어떻게 통보하는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **침해사고 대응**

3.47 **1단계**

신청기관은 공급망으로부터 전이된 위협요인에 의한 침해사고 발생시 내부 지침 또는 매뉴얼의 규정에 따라 책임자(책임부서)에 보고한다.

점검 가이드

(예시) 신청기관에서 공급망 침해하고 발생 시 내부 책임자에게 보고하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.48 **2단계**

신청기관은 공급망으로부터 전이된 위협요인에 의한 침해사고 발생시 책임추적 결과에 따라 △위협요인 식별 및 분리 △공급망·공급자 조정 등의 조치를 취한다.

점검 가이드

(예시) 신청기관에서 공급망 침해하고 발생 시 책임을 추적(예: 1차 공급자 → 2차 공급자 → ...)한 결과를 바탕으로 위협의 요인이 되는 공급자 배제 등 취할 수 있는 조치를 기입해 주시기

바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.49 **2단계**

신청기관은 공급망으로부터 전이된 위협요인에 의한 침해사고 발생시 계약에 따라 공급자에게 △결함 대응 △취약요인 제거 △정보 복구 등의 조치를 요청하고 이행한다.

점검 가이드

(예시) 신청기관에서 공급망 침해하고 발생 시 공급자에게 서면으로 통보했던 요구사항을 이행하는 내용을 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.50 **1단계**

신청기관은 개발환경에 공급망 침해사고 발생 시 신청제품에 미치는 영향을 파악하고 대응하는 절차가 있다.

점검 가이드

(예시) 신청기관에서 개발환경에서 공급망 침해하고 발생 시 신청제품에 미치는 영향을 파악하고 신청제품의 보안 영향 분석 및 수정 등 대응하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

3.51 2단계

신청기관은 운용 중인 ICT 제품·서비스의 취약점으로 인한 해킹 등 보안 사고 발생 시, 국가정보원 등 관계기관에 정보를 공유하고 신고한다.

점검 가이드

(예시) 신청기관에서 공급망 침해사고 발생 시 유관기관에 신고하는 절차를 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

4. 신청제품 공급망 관리

■ 구성요소 예측

4.1 2단계

신청기관은 신청제품의 공공분야 납품 소요를 예측하여 이에 필요한 S/W·H/W 구성요소에 대해 △사용 권한 △개발주체에 의한 취약점 개선 빈도 △(H/W가 포함될 경우) 소요를 충족하는 공급 안정성 여부 등을 점검한다.

점검 가이드

(예시) 신청제품에 포함되는 S/W, H/W 구성요소를 신청기관에서 개발·생산하여 안정적으로 공급할 수 있는 경우 이를 기입해 주시기 바랍니다. 신청제품에 포함되는 S/W, H/W 구성요소 중 외부 공급자를 통해 공급받아야 하는 구성요소가 있는 경우 신청기관에서 해당 구성요소에 대한 사용 권한을 지속적으로 확보하고, 해당 구성요소에 취약점 발생 시 개발주체를 통해서 적시에 개선되며, 안정적으로 해당 구성요소를 공급받을 수 있는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 구성요소 조달·소싱

4.2 2단계

신청기관은 신청제품을 개발·생산과정에서 외부 업체로부터 S/W·H/W 구성요소를 공급받는 경우, 공급망 안정성 유지를 위해 대체 공급업체 선정 등의 대책이 있다.

점검 가이드

(예시) 외부 업체로부터 공급받는 S/W·H/W 구성요소별로 공급 중단 등을 대비하여 대체 공급업체 선정 등 대책을 마련하고 있는지 기입해 주시기 바랍니다. 예를 들어, 신청제품의 S/W·H/W 구성요소 중 원천기술보유국의 수출·기술통제 등 제재로 인해 배포·유지보수 등 생명주기 관리가 지장을 받지 않도록 대체 공급업체 확보 등의 조치를 시행해야 합니다.

'없음'을 선택한 경우, 외부 업체로부터 구성요소를 공급받음에도 관련 절차가 부재한 경우와, 외부 업체로부터 구성요소를 공급받지 않아서 당장은 절차가 불필요하여 부재한 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

4.3 1단계

신청기관은 개발·생산하는 제품의 일부 구성요소를 외부 업체로부터 제공받는 경우 공급업체와 구성요소의 무결성·진위성 보호를 위한 상호조치를 약속하거나 이행하고 있다.

점검 가이드

(예시) 무결성 및 진위성 확인은 외부 공급자로부터 제공된 제품 구성요소가 위변조 없이 신청기관에게 제공되었음을 확인하는 것입니다. 예를 들어, 신청기관이 공급업체와 구성요소의 무결성/진위성 보호를 위한 계약/공문/서면합의 등의 상호조치를 약속하거나 이행하는 등이 있습니다.

'없음'을 선택한 경우, 외부 업체로부터 구성요소를 공급받음에도 관련 절차가 부재한 경우와, 외부 업체로부터 구성요소를 공급받지 않아서 당장은 절차가 불필요하여 부재한 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

4.4 2단계

신청기관은 외부 공급자로부터 제공받는 제품 구성요소에 대해 무결성 및 진위성을 확인·검증하는 절차가 있다.

점검 가이드

(예시) 무결성 및 진위성 확인은 외부 공급자로부터 제공된 제품 구성요소가 위변조 없이 신청기관에게 제공되었음을 확인하는 것입니다. 예를 들어, S/W 구성요소의 해시값을 검증하거나 전자서명 검증 등을 통해 확인할 수 있습니다.

'없음'을 선택한 경우, 외부 업체로부터 구성요소를 공급받음에도 관련 절차가 부재한 경우와, 외부 업체로부터 구성요소를 공급받지 않아서 당장은 절차가 불필요하여 부재한 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

4.5 1단계

신청기관은 신청제품을 타 업체가 개발·생산하는 제품의 일부 구성요소로 공급할 경우 수급자와 구성요소의 무결성·진위성 보호를 위한 상호조치를 약속하거나 이행하고 있다.

점검 가이드

(예시) 무결성 및 진위성 확인은 외부 공급자로부터 제공된 제품 구성요소가 위변조 없이 신청기관에게 제공되었음을 확인하는 것입니다. 예를 들어, 신청기관이 타 업체와 구성요소의 무결성/진위성 보호를 위한 계약/공문/서면합의 등의 상호조치를 약속하거나 이행하는 등이 있습니다.

'없음'을 선택한 경우, 신청제품을 타 업체 제품 구성요소로 공급함에도 관련 절차가 부재한 경우와, 신청제품을 타 업체 제품 구성요소로 공급하지 않아서 당장은 절차가 불필요하여 부재한 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요			

내용	

4.6 2단계

신청기관은 신청제품의 구성요소 공급자 목록을 상시 관리하고 필요시 갱신하고 있다.

점검 가이드

(예시) 외부 업체로부터 공급받는 신청제품의 구성요소별로 공급자 목록을 관리하고 있는지 기입해 주시기 바랍니다.

'없음'을 선택한 경우, 외부 업체로부터 구성요소를 공급받음에도 관련 절차가 부재한 경우와, 외부 업체로부터 구성요소를 공급받지 않아서 당장은 절차가 불필요하여 부재한 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ **구성요소 투명성 확보**

4.7 2단계

신청기관은 신청제품의 S/W · H/W 구성요소 중 제3자가 개발한 부분에 대한 SBOM 또는 HBOM을 공급자로부터 제출받는다.

점검 가이드

(예시) 신청제품에 신청기관에서 직접 개발하지 않은 구성요소가 포함된 경우 SBOM 또는 HBOM을 공급자로부터 제출받는지 기입해 주시기 바랍니다.

'없음'을 선택한 경우, 외부 업체로부터 구성요소를 공급받음에도 관련 절차가 부재한 경우와, 외부 업체로부터 구성요소를 공급받지 않아서 당장은 절차가 불필요하여 부재한 경우를 구분하여 명시해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

4.8 2단계

신청기관은 신청제품의 S/W · H/W 구성요소 중 직접 개발한 부분에 대한 SBOM 또는 HBOM을 작성한다.

점검 가이드

(예시) 신청제품 및 제품의 구성요소에 대한 SBOM, HBOM을 작성 및 관리하는 내용을 기입해 주시기 바랍니다. SBOM, HBOM의 표준 형식, 생성 및 업데이트 시점 등도 기입해 주시기 바랍니다. 신청제품에 오픈소스 등과 같은 제3자 구성요소가 포함된 경우 SBOM을 생성하여 관리할 것을 강력히 권고드립니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

■ 공급 안정성

4.9 1단계

신청기관은 신청제품의 S/W 구성요소 사용 권한(라이선스)이 자체 예측한 공공분야 납품 · 운용 기간보다 일찍 도래하지 않도록 사용계약을 관리한다.

점검 가이드

(예시) 신청기관에서 공공분야에 도입되어 운용 중인 신청제품 또는 구성요소(제3자 제공 암호모듈 등)의 사용 권한(라이선스)이 적절하게 보장될 수 있도록 어떻게 관리하는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			

4.10 1단계

신청기관은 신청제품의 S/W · H/W 구성요소를 공급하는 기업 · 공급자가 국제사회의 무역 · 기술수출통제 제재를 받고 있는지 여부를 확인한다.

점검 가이드

(예시) 「공공분야 도입·운용 IT보안제품 新 보안적합성 검증체계」(2022.10.5.)의 '공급망 보안 강화를 위한 예방 조치'에 따라 신청제품의 구성요소가 제재 대상이 아님을 확인하였는지 기입해 주시기 바랍니다.

자체 점검결과

선택	☐ 문서	☐ 관행	☐ 없음
주요 내용			