정보보호제품
평가·인증 수행규정

2017. 06. 26.

미래창조과학부

IT보안인증사무국

목 차

정보보호제품 평가·인증 수행규정

제1장 총 칙

제1조(목적) 이 규정은「국가정보화기본법」 제38조 및 동법 시행령 제35조,「국가표준기본법」 제21조,「정보보호시스템 평가·인증지침」에 의하여 정보보호제품 또는 보호프로파일(이하 '정보보호제품 등'이라 한다) 평가 및 인증업무와 평가기관 승인에 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 규정은 정책기관, 인증기관, 평가기관, 신청기관, 인증서 보유기관에 적용한다.

제3조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "정보보호제품"이라 함은 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 총칭한다.
2. "평가기준"이라 함은 국제상호인정협정 관리위원회의「정보보호시스템 공통평가기준」을 미래창조과학부장관이 수용, 고시한 것을 말하며, 이 평가기준에 대한 관리위원회의 최종 해석 내용을 포함한다.
3. "평가방법론"이라 함은 미래창조과학부장관이 수용, 고시한 평가기준에 대한 국제상호인정협정 관리위원회의「정보보호시스템 공통평가방법론」을 말하며, 이 평가방법론에 대한 관리위원회의 최종 해석 내용을 포함한다.
4. "보호프로파일"이라 함은 특정 유형의 정보보호제품에 대해 필요한 보안요구사항을 구현 독립적으로 서술한 문서를 말한다.
5. "평가"라 함은 정보보호제품 등이 평가기준 및 평가방법론에 부합하는지 여부를 평가기관이 조사하는 것을 말한다.
6. "재평가"라 함은 인증제품의 보증에 주요한 영향을 주는 변경이 발생한 경우에 평가기관이 수행하는 평가를 말한다.
7. "변경승인(인증효력유지)"이라 함은 인증제품의 보증에 경미한 영향을 주는 변경이 발생한 경우 인증기관이 인증효력이 유지됨을 승인하

는 것을 말한다.

8. “인증”이라 함은 인증서를 발급하기 위해 평가기관이 수행한 정보보호제품 등의 평가결과를 인증기관이 승인하는 것을 말한다.
9. “신청기관”이라 함은 평가제출물(이하 ‘제출물’이라 한다)을 구비하여 평가기관에 정보보호제품 등의 평가를 의뢰한 기관이나 업체를 말한다.
10. “인정기관”이라 함은「국가표준기본법」에 의하여 한국인정기구(KOLAS)를 운영하는 국가기술표준원을 말한다.
11. “공인시험기관”이라 함은 인정기관으로부터 공인시험기관 인정서를 획득한 기관이나 업체를 말한다.
12. “평가기관”이라 함은 「국가정보화기본법」에 의해 지정받은 기관 또는 인증기관으로부터 평가기관으로 승인받은 공인시험기관을 말한다.
13. “시험평가”라 함은 공인시험기관이 정보보호제품 등의 평가수행능력 보유를 증명하기 위해「정보보호제품 평가·인증 수행규정」에서 정한 절차에 따라 수행하는 예비 평가활동을 말한다.
14. “정책기관”이라 함은 정보보호제품 평가·인증에 관한 정책과 관련 규정을 수립·시행하는 기관을 말한다.
15. “인증기관”이라 함은 인증업무를 수행하며 평가·인증 체계를 지속적으로 감독하고 운영할 책임이 있는 기관을 말한다.
16. “인증보고서”라 함은 인증기관이 인증결과를 종합하여 작성한 문서를 말한다.
17. “공통평가기준 인증서”(이하 ‘인증서’라 한다)라 함은 인증기관이 평가기관에서 수행한 정보보호제품 등의 평가결과를 확정하여 발급하는 증서를 말한다.
18. “인증서보유기관”이라 함은 인증서를 취득하거나 인증서의 사용 권리를 양수하여 보유하고 있는 기관이나 업체를 말한다.
19. “인증제품”이라 함은 인증기관으로부터 인증서를 교부받은 제품을 말한다.
20. “인증마크”라 함은 정보보호제품이 인증기관에 의해 인증된 제품임을 증명하는 표지(標識)를 말한다.
21. “제출물”이라 함은 신청기관이 정보보호제품 등을 평가받기 위하여 평가기관에 제출하는 제품 및 관련 문서 등을 말한다.

22. “평가단위보고서”라 함은 평가과정에서 제출물이 평가방법론의 항목별 요구수준을 만족하는지 여부를 평가한 후 그 결과를 작성한 문서를 말하며, 개발환경 보안점검 관련 보고서, 독립시험서, 침투시험서 등을 포함한다.
23. “관찰보고서”라 함은 평가과정에서 제출물이 평가기준 및 평가방법론의 항목별 요구수준을 만족하지 못하는 내용을 종합하여 작성한 문서를 말한다.
24. “평가결과보고서”라 함은 평가기관이 정보보호제품 등의 상세한 평가결과에 관하여 인증기관에 제출하는 문서를 말한다.
25. “평가신청제품”이라 함은 평가계약 후 평가착수 전까지의 정보보호제품 등을 말한다.
26. “평가대상제품(TOE : Target of Evaluation)”이라 함은 평가에 착수한 후 인증서를 교부받기 전까지의 정보보호제품 등을 말한다.

제2장 평가·인증체계

제1절 공 통

제4조(기본목표) 정보보호제품 평가·인증제도는 다음 각 호를 위하여 안전성과 신뢰성이 검증된 정보보호제품 보급을 그 목적으로 한다.

1. 정보보호제품에 대한 국제적인 신뢰성 확보
2. 국가통신망의 정보보호수준 제고
3. 정보보호제품 보안기능 개선으로 제품의 경쟁력 제고

제5조(평가원칙) 평가기관은 평가 결과의 객관성, 공정성, 반복성, 재생산성 및 적절성을 보장하기 위하여 다음 각 호의 사항을 준수하여야 한다.

1. 객관성 : 주관적인 견해를 배제하고 정확한 해석을 기반으로 객관적인 평가를 수행하여야 한다.
2. 공정성 : 정보보호제품, 보호프로파일 그리고 신청기관에 대한 편견과 선입견을 배제하고 공정한 평가를 수행하여야 한다.
3. 반복성 : 평가된 정보보호제품 등을 동일한 평가자가 다시 평가하여도 동일한 결과가 산출되어야 한다.

4. 재생산성 : 평가된 정보보호제품 등을 다른 평가자가 다시 평가하여도 동일한 결과가 산출되어야 한다.
5. 적절성 : 정보보호제품 등의 평가결과가 평가보증등급의 요구사항을 만족함을 보증하여야 한다.

제6조(평가·인증 절차) 정보보호제품 평가·인증 절차는 별표 1과 같다.

제7조(인증서 상호인정) 이 규정에 따라 국내에서 발급한 인증서는 국제상호인정협정에 의하여 가입국에서 인정되며, 우리나라 이외의 인증서발행국이 발급한 인증서는 국제상호인정협정에 의하여 국내에서도 인정한다. 다만, 국제상호인정협정이 국내법 또는 평가·인증 관련규정과 상충되는 경우에는 국내법 또는 관련규정이 우선한다.

제8조(평가·인증 관련기관) ①정보보호제품 평가·인증 관련기관은 별표 2와 같이 정책기관, 인증기관, 인정기관, 평가기관, 신청기관, 인증서보유기관으로 구분한다.

②미래창조과학부는 정책기관으로서 다음 각 호의 업무를 수행한다.

1. 정보보호제품 등의 평가·인증 수행에 관한 국가정책 결정
2. 정보보호시스템 평가·인증 지침, 평가기준·방법론, 보호프로파일 등의 수립 및 시행
3. 인증기관 지정 및 철회
4. 인증기관의 인증업무 감독

③한국전자통신연구원 부설 국가보안기술연구소는 인증기관으로서 다음 각 호의 업무를 수행한다.

1. 정보보호제품 평가·인증 수행규정, 평가·인증업무 수행에 관한 가이드·절차서 등의 수립 및 시행
2. 인증 수행에 따른 인증보고서 작성 및 인증서 발급
3. 인증제품 목록 공개 등 인증제품 관리
4. 인증기관 운영에 관한 자체 규정 수립 및 시행, 인증자 자격관리
5. 평가기관 승인·정지·취소 및 평가자 자격 승급·강등·정지·취소
6. 평가기관의 평가업무 감독 및 평가기관 보안관리 실태점검
7. 공인시험기관 인정 시 기술역량심사 참여
8. 신청기관과 평가기관간의 분쟁조정

9. 국제상호인정협정 관련 활동

10. 인증된 보호프로파일 등록 및 관리

제9조(비밀엄수) ①평가기관 및 인증기관에 소속된 자는 재직 중은 물론 퇴직 후에도 직무상 지득한 기밀을 누설하거나 신청기관 또는 인증서보유기관의 지적재산권을 침해하여서는 아니 된다.

②평가기관 및 인증기관은 소속된 자에게 보안 서약서를 받고 평가·인증 관련 보안교육을 실시한다. 다만, 보안서약서 작성 시 평가기관은 별지 제1호 서식을 사용하며, 인증기관은 이에 준하는 내부의 별도 서식을 사용한다.

제10조(제출물의 관리) ①신청기관과 평가기관간 제출물을 인계인수할 경우에는 제출물 인계인수증(별지 제2호 서식)을 작성하여야 한다.

②평가기관은 인수받은 제출물을 제출물 관리대장(별지 제3호 서식)에 기록 유지하여야 하며, 인증기관 요구시 인증기관에 제출물 관리대장의 사본을 제출하여야 한다.

③인증기관과 평가기관은 민감한 제출물을 외부에 공개하여서는 아니 된다. 다만, 민감하지 않은 제출물은 신청기관 또는 인증서보유기관의 사전 동의 및 입회하에 공개할 수 있다.

제11조(제출물의 분류) ①제출물은 유출될 경우 신청기관에 손해를 미치는 정도에 따라 다음과 같이 분류한다.

1. 기밀 : 신청기관의 핵심기술이 포함된 문서 또는 제품으로서 유출될 경우 신청기관에 막대한 손실을 초래할 우려가 있는 제출물

2. 일반 : 기밀을 제외한 모든 제출물

②평가기관은 신청기관의 기밀이 적절히 보호될 수 있는 제1항의 기준을 참고하여 신청기관과 협의하여 제출물을 분류하여야 한다.

제12조(제출물의 표시) ①기밀은 다음과 같은 표시를 제출물 중앙상단에 적색으로 표시한다.

②관리번호는 다음 규격에 의하여 문서인 때에는 표지의 좌측상단에 기입하고 제품인 경우에는 이에 준하여 식별이 용이하도록 적절한 부위에 기

입한다.

제13조(제출물의 보관) 제출물중 기밀은 이중 잠금장치가 있는 캐비닛 등에 보관하고 일반은 잠금장치가 있는 캐비닛 등에 보관한다. 다만, 캐비닛에 보관할 수 없는 제출물은 그에 상응한 보호조치를 마련하여야 한다.

제14조(보호프로파일 개발) 보호프로파일을 개발하여 평가·인증 받고자 하는 기관이나 업체는 사전에 정책기관 및 인증기관과 협의하여야 한다.

제2절 신청기관

제15조(평가신청) ①신청기관이 평가를 신청할 때에는 평가신청서(별지 제4호 서식)와 제출물 2부를 평가기관에 제출하여야 하며, 평가보증등급별 제출물은 평가기준을 준용한다. 다만, 제출물은 한글 또는 영어로 작성할 수 있다.

②신청기관은 제출물에 대한 정당한 법적 권한을 가지고 있어야 하며, 신청기관이 제공한 제출물이 타인의 지적재산권을 침해하여 분쟁이 발생한 경우 이에 대한 모든 책임을 진다.

③신청기관은 평가범위 및 평가보증등급에 부합하도록 제출물을 작성하여야 한다.

④신청기관은 평가기관으로부터 추가 자료 제출을 요청받은 경우에는 협의된 기한 내에 해당 자료를 제출하여야 한다.

⑤신청기관은 평가기관으로부터 제출물의 수정·보완을 요구받은 사항에 대해서는 협의된 기한 내에 수정·보완하여 제출하여야 한다.

제16조(보호프로파일 적용) ①신청기관은 평가신청제품과 관련하여 인증된 보호프로파일이 존재하는 경우 해당 보호프로파일을 준수하여 평가신청할 수 있다.

②신청기관은 제1항의 보호프로파일 준수시 해당 보호프로파일에서 명시한 방식을 준수해야 한다.

제17조(제품명 오용 금지) 신청기관은 정보보호제품 등의 보안기능에 적합한

제품명으로 평가를 신청하여야 한다.

제18조(평가공동신청) ①2개 이상의 기관이 공동으로 평가를 신청할 경우에는 그 중 1개 기관을 대표기관으로 정하고, 여타 기관은 공동신청기관 명부(별지 제5호 서식)에 연서하여 신청하여야 한다.

②대표기관은 인증서보유기관으로서 이 규정에서 정한 인증제품 관리 책임을 진다.

제19조(비용 납부) ①신청기관은 평가기관과 체결한 계약에 따라 평가 컨설팅, 평가 준비 및 수행, 인증효력유지 등 평가기관에서 제공하는 평가 업무에 필요한 비용을 납부하여야 한다.

②신청기관은 인증서 및 인증마크 발급 등에 필요한 비용을 요청받은 경우에는 이를 납부하여야 한다.

제20조(평가환경 제공) 신청기관은 평가기관으로부터 평가환경의 제공을 요청받은 경우에는 특별한 사유가 없는 한 이에 응하여야 한다.

제21조(회의 참석) 신청기관은 평가수행계획서 검토회의 등 평가기관이 주관하는 회의에 참석하여야 한다. 다만, 부득이한 사정이 있는 경우에는 평가기관과 협의하여 참석하지 아니할 수 있다.

제22조(이의 제기) ①신청기관은 평가·인증업무에 대하여 이의·불만·분쟁사항이 있는 경우에는 이의·불만·분쟁처리 신청서(별지 제6호 서식)에 의거 그 사유를 명시하여 평가기관 또는 인증기관에 이에 대한 처리를 요청할 수 있다.

②제1항의 요청을 받은 기관은 신청서를 접수한 날로부터 30일 이내에 처리결과를 신청기관에 통보한다. 다만, 부득이한 사유가 있는 경우에는 신청기관에 통보한 후 일정한 기간을 정하여 연장할 수 있다.

제3절 평가기관

제23조(평가기관 지정요건) ①평가기관으로 승인받고자 하는 공인시험기관(이하 '승인신청기관'이라 한다)은 다음 각 호의 요건을 구비하여야 한다.

1. 법인으로서 대한민국 내에 위치
2. 평가기관 품질매뉴얼상 기술책임자 1명을 포함한 선임평가자 3명 이

상, 주임평가자 2명 이상 보유

3. 독립된 의사결정 체계 유지 및 평가업무 수행에 필요한 사무공간과 장비 등 확보
4. 국제표준규격(ISO/IEC 17025)에 따라 수립한 자체 품질매뉴얼 및 절차서 구비
5. 기타 인증기관이 평가업무 수행에 필요하다고 인정한 사항

②승인신청기관은 국제상호인정협정(CCRA)의 부록B 제3항(평가기관 인정 및 승인)에 기술된 평가기관 승인관련 요구사항을 충족시켜야 한다.

제24조(평가기관 승인신청) ①승인신청기관은 평가기관 승인신청서(별지 제7호 서식)에 다음 각 호의 서류를 첨부하여 인증기관에 승인을 신청하여야 한다.

1. 평가기관 준수사항 서약서 1부(별지 제8호 서식)
2. 국제표준규격(ISO/IEC 17025)에 따라 수립한 자체 품질매뉴얼 이행실적 1부
3. 평가관련 조직 및 인력 등이 포함된 일반현황 1부
4. 인정기관이 발행한 공인시험기관 인정서 사본 1부
5. 법인등기부등본 사본, 사업자등록증 사본, 법인 및 대표자 인감증명서 사본, 대표자 개인신용보고서 각 1부

②인증기관은 제1항에 의하여 제출받은 평가기관 승인신청서 및 첨부서류가 미비하거나 기재사항이 누락된 경우에는 일정한 기간을 정하여 이를 보완하게 할 수 있다.

제25조(시험평가 등) ①승인신청기관은 인증기관과 사전협의를 거쳐 평가업무 수행범위 및 시험평가용 제품을 선정하고 관련문서를 인증기관에 제출하여야 한다.

②승인신청기관은 시험평가용 제품에 대한 평가를 수행하고 다음 각 호의 결과물을 제24조 제1항에 따라 인증기관에 평가기관 승인신청서를 제출한 날로부터 180일 이내에 인증기관에 제출하여야 한다.

1. 평가수행계획서(별지 제14호 서식)
2. 평가단위보고서(별지 제15호 서식)
3. 관찰보고서(별지 제16호 서식)
4. 평가결과보고서(별지 제9호 서식)

5. 회의록

제26조(승인신청기관 심사 등) ①인증기관은 제25조 제2항의 결과물을 접수받은 날부터 120일 이내에 승인신청기관에 대해 평가업무 수행역량과 자체 품질매뉴얼 준수 실태 등을 종합 검토하여 승인 여부를 결정한다. 다만, 부득이한 사유가 있는 경우에는 일정한 기간을 정하여 연장할 수 있다.

②인증기관은 제1항에 의한 심사결과 승인신청기관이 평가기관으로서 적합하지 아니하다고 판단될 때에는 30일 이내의 기간을 정하여 해당사항을 보완하게 할 수 있다.

③인증기관이 승인신청기관에 대하여 평가기관으로 지정한 때에는 평가기관 승인서(별지 제10호 서식)를 승인신청기관에 교부하고 다음 각 호의 사항을 공지한다.

1. 평가기관의 명칭 및 소재지
2. 평가기관의 평가업무 수행 범위
3. 평가기관의 승인일자 및 유효기간

제27조(평가기관 관리 등) ①인증기관은 평가기관에 대하여 다음 각 호의 사항을 연 1회 이상 정기 및 수시 점검할 수 있다.

1. 평가·인증 관련규정의 준수 여부 및 평가업무 수행의 적절성
2. 평가자 보수교육 이수 등 평가자 자격유지 실태
3. 평가시험실 및 각종 평가업무용 시설에 대한 보안관리 실태
4. 기타 평가기관 유지에 필요한 사항

②평가기관은 제1항의 점검결과 나타난 문제점에 대하여 보완 조치하고 그 결과를 인증기관에 통보하여야 한다.

③평가기관이 평가관련 규정 및 제도를 수립하거나 외부에 평가관련 문서를 공개할 경우에는 인증기관과 사전 협의하여야 한다.

④평가기관은 평가자 전보, 입사·퇴사, 조직 변경, 평가기관 인수·합병·명칭변경, 평가시험실 이전·축소·확장 등 평가기관 운영과 관련하여 변동사항이 발생할 경우에는 15일 이내에 인증기관에 그 사실을 통보하여야 한다.

⑤평가기관은 외부에 평가·인증제도 관련 허위 사실 또는 공개되지 않은 정보를 유포하여서는 아니 된다.

⑥평가기관은 선임평가자 중 1명 이상을 기술책임자로 지정하여야 하며, 기술책임자는 평가기관 내에서 평가기준 및 평가방법론을 정확하고 효율적으로 적용할 책임이 있다.

제28조(평가기관 재심사) ①인증기관은 평가기관이「정보보호제품 평가·인증 수행규정」등 관련규정을 준수하고 있는지 여부를 확인하기 위하여 매 4년마다 재심사를 실시하고, 평가기관의 평가업무 수행범위 변경, 평가기관 인수·합병·명칭변경, 평가시험실 이전·축소·확장 등 중요사항의 변경이 발생한 경우 별도의 재심사를 실시한다.

②인증기관은 매 4년마다 재심사를 실시하는 경우 제24조, 제25조 및 제26조의 규정을 준용하여 평가기관 재심사를 실시한다. 다만, 재심사를 실시하기 전 1년 이내에 평가기관 승인서의 평가업무 수행범위에 명시될 평가보증등급에 대한 평가실적이 있는 평가기관에 대해서는 제25조에서 정한 시험평가를 면제할 수 있다.

③평가업무 수행범위 변경에 따른 재심사는 제29조의 규정을 준용하고, 평가기관 인수·합병·명칭변경, 평가시험실 이전·축소·확장 등 중요사항의 변경에 따른 별도의 재심사는 인증기관과 사전협의를 거쳐 실시한다.

④평가기관은 평가기관 자격 만료 3개월 전에 인증기관에 재심사를 신청하여야 한다.

⑤평가기관은 재심사 과정에서 나타난 지적사항에 대하여 보완조치하고 그 결과를 인증기관에 통보하여야 한다.

제29조(평가업무 수행범위 변경) ①평가기관은 평가업무 수행범위를 확장하고자 할 경우 인정기관이 발행한 해당 공인시험기관 인정서 사본과 함께 공문으로 인증기관에 수행범위 변경을 요청하여야 한다.

②인증기관은 제25조 및 제26조의 규정을 준용하여 평가업무 수행범위 변경에 대한 재심사를 실시하고 승인여부를 결정한다.

제30조(평가기관 자격정지) ①인증기관은 평가기관이 다음 각 호의 하나에 해당하는 사유가 발생한 때에는 3년 이내의 기간을 정하여 평가기관 자격을 정지하거나 평가업무를 정지시킬 수 있다.

1. 평가기관이 제23조의 지정요건을 충족하지 못하는 경우
2. 평가기관이 특별한 사유 없이 제27조 제2항 또는 제4항을 이행하지 않거나 제27조 제3항 또는 제5항을 위반한 경우

3. 평가기관이 특별한 사유 없이 제28조 제4항 또는 제5항을 이행하지 않은 경우

4. 평가기관이 특별한 사유 없이 제4항을 이행하지 않은 경우

5. 기타 평가기관의 귀책사유로 평가업무 수행에 차질이 초래된 경우

②제1항의 규정에도 불구하고 부득이한 사정이 있는 경우에는 평가기관은 신청기관과 협의하고 인증기관의 승인을 받아 제한된 범위에서 평가업무를 수행할 수 있다.

③평가기관은 제1항에 의해 평가업무가 중단된 경우 인증서보유기관 및 신청기관과 협의 하에 평가제출물을 반환하고 평가제출물을 활용하여 작성한 평가단위보고서 등 평가관련 산출물을 처리하여야 한다.

④평가기관은 자격 정지 종료일 이전에 자격정지 사유에 대하여 보완조치하고 제28조의 규정을 준용하여 인증기관의 재심사를 완료하여 자격을 회복하여야 한다.

제31조(평가기관 자격취소) ①인증기관은 평가기관이 다음 각 호의 하나에 해당하는 사유가 발생한 때에는 평가기관 자격을 취소할 수 있다.

1. 허위 또는 부정한 방법으로 평가기관 자격을 취득한 경우

2. 허위 또는 부정한 방법으로 평가를 수행하여 평가관련 산출물을 제출한 경우

3. 최근 1년간 정보보호제품 등 대한 평가실적이 없는 경우

4. 평가기관 자격정지 처분을 받고도 인증기관 승인 없이 그 기간내에 평가업무를 수행한 경우

5. 평가기관 자격정지 처분을 3회 이상 받은 경우

6. 신청기관의 지적재산권 관련정보를 신청기관의 동의 없이 모회사, 자회사, 계열회사, 투자자, 채권자 등 제3자에게 유출한 경우

7. 평가기관이 파산하거나 자격취소를 요청한 경우

8. 기타 평가기관으로서 자격유지가 불합리하다고 판단되는 경우

②평가기관은 자격이 취소된 경우에는 30일 이내에 제출물을 인증서보유기관 및 신청기관에 반납하고 평가제출물을 활용하여 작성한 평가단위보고서 등 평가관련 산출물을 인증서보유기관 및 신청기관과 협의하여 처리하여야 한다.

제32조(평가기관 승인서 반납) 평가기관은 평가기관의 자격이 정지되거나 취

소된 경우 평가기관 승인서를 인증기관에 지체 없이 반납하여야 한다.

제33조(평가자 구분 및 자격요건) ①인증기관은 평가기관에 속한 평가자의 평가수행 능력에 따라 다음 각 호와 같이 자격을 구분하여 심사하고 해당 위촉장(별지 제11호 서식)을 수여한다.

1. 선임평가자 : EAL4 이내의 등급에 대해 평가수행이 가능한 자. 다만, 인증기관은 EAL5 이상의 등급에 대해 평가수행이 가능한 선임평가자를 별도로 지정 가능함
2. 주임평가자 : EAL2 이내의 등급에 대해 평가수행이 가능한 자
3. 수습평가자 : 상위 평가자의 평가업무를 보조하는 자

②제1항의 평가자에 대한 최소 자격요건은 다음 각 호와 같다.

1. 선임평가자 : 주임평가자 자격 취득 후 평가업무에 3년 이상 종사한 자로서 10회 이상 평가수행에 참여하고 EAL4 등급의 평가역량을 보유한 자
2. 주임평가자 : 정보통신분야 학사 이상의 학위를 보유하거나 개발·시험·품질보증 등 평가 유관업무를 3년 이상 수행한 자로서 수습평가자 자격 취득 후 2회 이상 평가수행에 참여하고 EAL2 등급의 평가역량을 보유한 자
3. 수습평가자 : 인증기관이 인정하는 평가·인증관련 일반교육과정을 이수하고 '수습평가자 자격시험'을 통과한 후 평가기관에 속한 자

③평가기관은 소속 평가자가 제2항의 최소 자격요건 만족시 인증기관에 평가자 자격 위촉 또는 승급을 요청할 수 있으며, 이 경우 다음 각 호의 문서를 인증기관에 제출하여야 한다. 다만, 수습평가자 위촉 요청시에는 제2호를 면제할 수 있다.

1. 평가자 이력카드(별지 제12호 서식)
2. 평가수행계획서 등 평가업무 수행중 작성한 문서 사본 1부
3. 인증자가 요청하는 기타 문서

④인증기관은 제3항에 의하여 심사 요청을 받았을 때에는 평가자 자격요건 충족 여부를 심사한 후 승급 여부를 결정한다. 다만, 승급 여부 결정이 어렵다고 판단될 경우에는 추가적인 증빙자료를 요청하거나 필요시 승급을 요청한 평가자에게 설명을 요청할 수 있다.

⑤승급을 요청한 평가자가 인증기관으로부터 승급불가 또는 보류 판정을 받을 경우에는 판정일로부터 6개월간 재심사를 요청할 수 없다.

제34조(평가의 독립성 보장) 평가대상제품의 개발 또는 제출물 작성에 참여한 평가자는 해당 제품의 평가에 참여하여서는 아니 된다.

제35조(평가자문) ①평가기관은 다음 각 호의 사항에 대하여 신청기관의 자문 또는 컨설팅 요청이 있는 경우에는 이에 응할 수 있다.

1. 평가기준 및 평가·인증 절차
2. 보호프로파일 적용 방법 또는 평가보증등급별 제출물 작성 방법
3. 평가·인증 정책 등

②제1항 제3호에 대하여 자문할 경우에는 그 내용에 대하여 사전에 인증기관과 협의하여야 한다.

제36조(평가신청접수증 발급) ①평가기관은 신청기관으로부터 평가신청을 접수한 경우에는 제출물을 검토한 후 평가신청접수증(별지 제13호 서식)을 발급하여야 한다. 다만, 다음의 각호와 같은 경우에는 평가신청접수증을 발급하지 아니할 수 있다.

1. 평가신청 접수와 동시에 계약서를 작성하는 경우
2. 제출물의 내용에 미비점이 발견되어 신청기관에 보완을 요청하였으나 신청기관이 이를 이행하지 않은 경우
3. 평가신청제품에 대해 평가기관의 인력, 기술력 또는 관련 시험장비의 미비 등으로 평가를 수행할 수 없다고 판단되는 경우

②제1항 제3호에 대하여 검토할 경우에는 가용 평가인력, 평가신청제품의 유형 및 시험에 소요되는 난이도, 평가신청 보증등급에 적합한 평가수행 역량 등을 종합적으로 검토하여야 한다.

③제1항 제2호 또는 제3호에 의하여 평가신청을 거부할 경우에는 그 내용에 대하여 사전에 인증기관과 협의하여야 한다.

제37조(평가계약) ①신청기관은 평가신청접수증을 발급받은 후 평가기관에 평가계약을 요청할 수 있으며 평가기관은 신청기관과 협의하여 평가계약일을 정하고 평가계약서를 작성한다.

②평가기관은 평가계약을 체결한 후 30일 이내에 제출물 1부를 인증기관에 공문으로 제출하여야 하고, 인증기관 요청시 평가계약서 사본을 제출하여야 한다.

③신청기관은 평가계약 체결시 보안목표명세서, 인증보고서 등 인증기관

홈페이지 및 국제상호인정협정 홈페이지에 공개될 정보에 대한 공개 동의서(별지 제25호 서식)를 평가기관에 제출하여야 한다. 다만, 보안목표명세서에 민감한 정보가 포함되어 있을 경우, 별도로 공개용 보안목표명세서를 작성하여 제출할 수 있다.

제38조(전문성 확보) ①평가기관은 평가신청제품 및 평가대상제품의 평가에 필요한 인력, 기술력 등의 전문성을 확보하고 인증기관에게 이를 입증해야 한다. 다만, 평가기관은 전문성 확보에 신청기관의 지원이 필요한 경우 제5조의 각 호의 원칙에 위배되지 않는 범위에서 지원을 요청할 수 있다.
②인증기관은 제1항에 의하여 평가기관의 전문성을 검토하는 경우 추가적인 증빙자료를 요청하거나 평가기관에게 설명을 요청할 수 있다.

제39조(제출물 설명회) 평가기관은 평가신청제품에 대한 이해도 제고를 위하여 평가착수 전에 신청기관에 인증기관이 참석하는 제출물 설명회를 요청할 수 있다.

제40조(평가수행계획서 작성) ①평가기관은 평가착수를 위하여 평가신청제품의 특성, 평가보증등급, 평가범위, 평가반 구성 및 평가일정 등이 포함된 평가수행계획서(별지 제14호 서식)를 작성하고 인증기관 및 신청기관과 협의하여야 한다. 다만, EAL3 이상의 등급 제품에 대해서는 인증기관과 사전에 별도 협의하여야 한다.
②평가반 구성 및 평가일정은 평가신청제품의 특성, 평가보증등급 및 평가범위 등을 고려하여 정한다.
③평가기관은 평가진행 도중에 평가자 교체, 평가일정 변경, 평가대상제품 명칭 변경 등 평가수행계획서를 수정할 필요가 있을 경우에는 인증기관과 사전 협의하여야 한다.

제41조(평가업무 수행) ①평가기관은 인증기관이 승인한 평가수행계획서에 따라 평가대상제품이 평가기준 및 평가방법론의 요구수준을 만족하는지 여부를 평가한다.

②평가기관은 평가업무 수행과 관련하여 생산한 다음 각 호의 문서를 평가기관 기술책임자의 검토를 완료하여 인증기관에 제출하여야 하며, 평가과정 중에 최소 1회 이상 평가진행 현황을 인증기관에 보고하는 평가진도 점검회의를 개최하여야 한다.

1. 평가수행계획서(별지 제14호 서식)
2. 개발환경보안점검 관련 보고서, 독립시험서, 침투시험서 등을 포함하

는 평가단위보고서(별지 제15호 서식)

3. 관찰보고서(별지 제16호 서식)

4. 평가결과보고서(별지 제9호 서식)

5. 평가결과보고서 영문 요약본

6. 평가·인증 관련 회의록

7. 기타 평가관련 자료 또는 인증기관이 요청한 자료

③평가기관은 제2항의 문서 내용 중에서 인증기관으로부터 수정·보완을 요청받은 사항에 대해서는 특별한 사유가 없는 한 이행하여야 한다.

④평가기관은 인증기관 및 신청기관에 평가수행계획서와 관찰보고서의 내용을 설명하고 동의를 득하여야 한다.

⑤평가기관은 필요하다고 판단될 경우 신청기관에 독립 및 침투시험을 위한 평가환경 지원을 요청할 수 있다.

⑥평가기관은 평가를 완료한 경우에는 인증기관 요청시 평가결과를 발표하고, 제37조 제3항에 의하여 한글 및 영어로 작성된 보안목표명세서를 검토한 후 인증기관에 제출하여야 한다.

제42조(평가관련업무 위탁) ①평가기관은 제품 평가과정에서 외부 전문가의 참여가 필요하다고 판단될 경우에는 신청기관 및 인증기관과 사전 협의하여 참여시킬 수 있다.

②평가기관은 일부 평가항목에 대한 시험을 외부기관에 의뢰할 경우에는 사전에 시험의뢰 대상기관에 관한 다음 각 호의 서류를 첨부하여 인증기관에 승인을 요청하여야 한다.

1. 시험관련 조직 및 인력 등이 포함된 일반현황 1부

2. 시험실적 1부

3. 시험환경에 대한 보안관리대책 1부

4. 인증기관이 시험의뢰 대상기관의 적격성을 확인하는데 필요한 사항

③인증기관은 제2항에 의하여 제출받은 서류를 검토한 후 승인여부를 평가기관에 통보한다.

제43조(개발환경 보안점검) ①평가기관은 신청기관의 평가대상제품 개발환경에 대한 보안관리 실태를 점검할 수 있다. 이 때 필요한 제반비용은 신청기관이 부담한다.

②제1항의 보안점검은 별표 3의 절차에 따라 수행하여야 한다.

제44조(평가결과보고서 제공) 평가기관은 인증서보유기관이 평가결과보고서를 요청할 경우에는 제공할 수 있다. 다만, 평가기관의 평가관련 핵심기술 유출 소지가 있는 내용은 제공하지 아니할 수 있다.

제45조(평가중단) ①평가기관은 평가과정에서 평가계약서에 명시된 평가중단 사유가 발생하는 경우에는 평가기관 내부규정에 따라 평가를 중단할 수 있다.

②제52조 제7항에 따라 인증기관으로부터 평가중단을 요청받은 경우 서면으로 신청기관과 협의하여야 한다.

③평가기관이 평가를 중단하고자 하는 경우에는 그 사유를 명시하여 서면으로 인증기관과 협의하여야 한다.

④제2항 및 제3항의 협의결과 평가중단이 필요하다고 판단되는 경우에는 평가를 중단하고 그 사유를 평가중단통보서(별지 제17호 서식)에 의거 신청기관에 통보하여야 한다.

제46조(평가계약 해지) 평가기관은 다음 각 호의 하나의 사항이 발생한 경우에는 평가계약을 해지할 수 있다.

1. 신청기관의 파산, 부도, 폐업 등으로 인하여 평가기관이 평가를 계속 진행할 수 없는 경우
2. 신청기관이 자발적으로 평가를 철회한 경우
3. 제출물에 대한 소유권 침해소송 결과 지적재산권을 침해하였다고 확인될 경우

제47조(제출물의 반납) 평가기관은 인증완료 또는 평가계약이 해지된 경우에는 제출물을 신청기관에 반환하는 것을 원칙으로 하되, 필요시 인증기관과 협의를 거쳐 자체 폐기할 수 있으며 이 경우 현황을 기록 유지한다.

제48조(평가자 자격관리) ①수습이상 평가자는 특별한 사유가 없는 한 매 2년마다 인증기관 주관으로 실시하는 평가·인증관련 보수교육과정을 이수하여야 한다.

②인증기관은 필요시 주임이상 평가자에 대해 평가·인증 관련규정 준수여부, 보수교육 이수여부, 최근 2년간 제품평가 참여 실적 등을 심사하여 평가자 자격의 강등, 유지 또는 정지 여부를 결정한다.

③전보 또는 퇴사한 평가자는 해당일 기준으로 자격을 정지한다.

④평가자 자격이 강등된 자는 강등처분일로부터 6개월 이상 경과해야 인증기관에 자격 승급을 요청할 수 있다.

⑤평가자 자격이 정지된 자는 정지처분일로부터 6개월 이상 경과해야 인증기관에 자격정지 철회를 요청할 수 있다. 다만, 제3항에 따라 자격이 정지된 평가자가 평가기관으로 복귀하거나 승인신청기관에 소속되는 경우 인증기관은 제2항을 준용하여 심사 후 평가자 자격을 부여할 수 있다.

⑥인증기관은 평가자 자격이 정지된 자로부터 자격정지 철회 요청을 받을 경우 해당 평가자를 EAL2 등급 이하(선임평가자는 EAL4 등급 이하)의 제품평가에 보조 평가자로 참여시킬 수 있으며, 평가수행 실적을 검토하여 자격정지 철회 여부를 결정한다.

⑦인증기관은 다음 각 호의 하나에 해당하는 사유가 발생할 때 평가자 자격을 취소할 수 있다.

1. 허위 또는 부정한 방법으로 평가자 자격을 취득한 경우
2. 허위 또는 부정한 방법으로 평가를 수행하여 평가관련 산출물을 제출한 경우
3. 평가자 자격정지 상태에서 인증기관의 별도 허가 없이 평가업무를 수행한 경우
4. 평가자 자격정지 상태가 3년 이상 지속된 경우

⑧평가자 자격이 강등, 정지 또는 취소된 경우에는 평가자 위촉장을 인증기관에 지체 없이 반납하여야 한다.

제4절 인증기관

제49조(IT보안인증사무국) ①국가보안기술연구소의 장은 인증업무를 효율적으로 수행하기 위하여 IT보안인증사무국(이하 '인증사무국'이라 한다)을 설치·운영하며, 사무국의 편성은 별표 4와 같다.

②인증사무국은 본 수행규정상의 인증기관 역할을 수행하며 정부예산으로 운영된다.

③인증사무국의 장은 정보보호제품 인증기관을 대표하는 인증업무 책임자로서 인증위원회의 위원장 역할을 함께 수행한다.

제50조(인증자 구분 및 자격요건) ①인증기관의 인증자는 인증수행 능력에 따라 다음 각 호와 같이 구분한다.

1. 선임인증자 : EAL4 이내의 등급에 대해 인증수행이 가능한 자. 다만, 인증사무국의 장은 EAL5 이상의 등급에 대해 인증수행이 가능한 선임인증자를 별도로 지정 가능함
2. 주임인증자 : EAL3 이내의 등급에 대해 인증수행이 가능한 자
3. 수습인증자 : 상위 인증자의 인증업무를 보조하는 자

②제1항의 인증자에 대한 최소 자격요건은 다음 각 호와 같다.

1. 선임인증자 : 선임평가자 자격을 보유하고 인증 소양 교육을 받은 자 또는 주임인증자 자격 취득 후 인증과정에 10회 이상 참여한 자
2. 주임인증자 : 주임평가자 자격을 보유하고 인증 소양 교육을 받은 자, 또는 수습인증자 자격 취득 후 인증과정에 2회 이상 참여한 자
3. 수습인증자 : 정보통신분야 학사 이상의 학위를 보유하거나 개발·시험·품질보증 등 평가 유관업무를 3년 이상 수행한 자로서 수습평가자 자격시험을 통과하고 인증기관에 소속된 자

③인증사무국의 장은 인증자가 제2항의 최소 자격요건 만족시 업무수행능력에 대한 자체심사를 실시한 후 인증자 자격을 부여한다.

제51조(교육과정 운영) ①인증기관은 다음 각 호의 교육과정을 자체적으로 편성·운영하거나 외부에 위임 또는 위탁할 수 있다. 다만, 일반교육과정은 교육 수요에 따라 교육 횟수를 증감하여 운영할 수 있다.

1. 일반교육과정 : 정보통신 및 정보보호분야 관계자를 대상으로 편성·운영
2. 보수교육과정 : 수습 이상의 평가자 및 인증자를 대상으로 연 1회 편성·운영
3. 평가·인증 관련 기타 교육과정

②인증기관으로부터 교육과정을 위임 또는 위탁받는 기관은 교육계획 등을 사전에 인증기관과 협의하여야 한다.

제52조(인증수행) ①인증기관은 제출물 설명회에 참석하고 필요시 추가 자료를 요청할 수 있다.

②인증기관은 제41조에 의해 평가기관이 제출한 문서 및 평가 활동이 평가기준, 평가방법론, 관련 규정을 준수하는지 감독한다.

③제2항의 감독 결과 미비점에 대해서는 인증기관 의견을 통보하고 평가기관으로 하여금 수정·보완하도록 한다.

④인증기관은 평가결과의 신뢰성 확보를 위하여 다음 각 호의 평가업무 수행과정에 참여하여 관리·감독할 수 있다.

1. 평가대상제품에 대한 독립시험 및 침투시험
2. 신청기관에 대한 개발환경 보안점검

⑤평가·인증과정에서 발생하는 문제점을 해결하기 위하여 인증기관의 기술책임자 주관 하에 회의를 개최하고 그 결과를 회의록에 기록 유지한다.

⑥제5항의 문제점에 대한 해결방안 수립시 객관성 및 공정성이 필요한 경우, 인증기관은 각 평가기관의 기술책임자가 포함된 기술검토위원회를 구성하여 관련 자문을 받을 수 있다.

⑦평가기관이 평가수행계획서의 평가일정에 준하여 평가관련 산출물을 제출하지 않거나 30일 동안 평가관련 산출물을 제출하지 않는 경우 인증기관은 평가기관에 사유를 요청할 수 있으며, 정당한 사유 없이 평가가 진행되지 않은 경우 제45조의 평가중단을 요청할 수 있다.

제53조(인증관련업무 위탁) ①인증기관은 제품 인증을 타기관 또는 조직내 타부서에 위탁하여 수행할 수 없다.

②제1항에도 불구하고 인증기관은 고도의 전문기술 또는 장비를 요하는 업무에 한해 자문형식으로 외부 지원을 받을 수 있다.

제54조(인증보고서 공개 등) ①인증기관은 정보보호제품 등에 대한 인증을 완료하고 인증보고서를 작성한다.

②인증기관은 정보보호제품을 사용하는 기관이 참고할 수 있도록 인증제품의 보안목표명세서, 인증보고서 등을 인증기관 홈페이지 및 국제상호인정협정 홈페이지에 공개한다. 다만, 신청기관의 지적재산권과 관련된 자료에 대해서는 평가기관 및 신청기관과 사전 협의하여 공개범위를 결정한다.

③인증기관은 인증된 보호프로파일, 인증보고서 등을 인증기관 홈페이지에 공개하고, 필요시 국제상호인정협정 홈페이지에 공개한다.

제55조(제출물 처리) ①인증기관은 평가계약이 해지되거나 인증을 완료한 경우 제출물을 신청기관에 반환하고, 반환이 불가능하거나 신청기관이 동의한 경우 등에는 자체 폐기하고 그 현황을 기록 유지한다.

②제1항의 경우에도 불구하고 업무상 계속 제출물(원시 프로그램 및 하드웨어 설계서는 제외)을 보관할 필요가 있을 경우에는 신청기관의 동의하에 계속 보관할 수 있다.

제56조(평가 및 인증산출물 처리) ①인증기관은 제출물을 제외한 평가·인증 업무 관련 자료 일체를 최소 5년간 보존하여야 한다.

②인증기관은 정책기관의 요구시 평가·인증 업무 관련 자료를 정책기관에 제출하여야 한다. 다만, 신청기관 또는 평가기관의 핵심기술이 포함된 문서의 경우에는 해당 기관과 협의하여 제출하지 아니할 수 있다.

③인증기관은 정책기관을 제외한 외부기관 또는 조직 내부의 타부서에 업무 관련 자료를 제공하여서는 아니 된다. 다만, 다음 각 호의 경우 정책기관 동의하에 제한적인 자료제공을 할 수 있다.

1. 법에 의한 정당한 자료제공 요청일 경우
2. 신청기관, 평가기관 등 이해당사자가 자료제공을 서면으로 동의할 경우
3. 평가·인증 현황 통계자료 등 특정 신청기관 또는 평가기관의 민감한 정보가 유출될 가능성이 없는 자료제공 요청일 경우

제57조(인증서 및 인증마크 교부) ①인증기관은 인증이 완료된 정보보호제품에 대해 신청기관에 인증서(별지 제18호 서식) 및 인증마크(별지 제19호 서식)를 교부한다. 다만, 인증마크는 신청기관이 인증마크 사용신청서(별지 제20호 서식)를 평가기관에 제출한 경우에 한해 교부한다.

②인증기관은 인증이 완료되기 전에 신청기관이 인증서를 발급받았다고 허위사실을 공표할 경우 인증서 발급을 거절하거나 6개월 범위 안에서 기간을 정해 인증서 발급을 연기할 수 있다.

제5절 인증위원회

제58조(인증위원회 운영) 인증기관은 다음 각 호의 업무를 수행하기 위하여 인증위원회(이하 '위원회'라 한다)를 운영할 수 있다.

1. 정보보호제품 평가·인증 수행규정 제·개정 심의
2. 평가결과의 타당성 및 공정성에 대한 심의
3. 평가기관 자격 승인·정지·취소 등에 대한 심의 및 신청기관, 평가기관, 인증기관, 인증서 보유기관간 분쟁 조정
4. 기타 정책기관 또는 위원회 위원장(이하 '위원장'이라 한다)이 필요하다고 인정하는 사항

제59조(위원회 구성) ①위원회는 다음 각 호와 같이 구성한다.

1. 위원장은 인증사무국의 장이 된다.
2. 위원은 위원장 1인을 포함하여 정책기관, 정부기관, 학계, 연구기관 등의 정보보호전문가 10인 이내로 한다.
3. 위원은 당연직 위원과 선임직 위원으로 구성한다.
4. 간사는 인증사무국의 기술책임자가 수행한다.

②당연직 위원은 정책기관 전문가로 한다.

③선임직 위원은 심의안건을 고려하여 정보보호관련 전문지식과 경험이 풍부한 자 중에서 정책기관과 협의하여 위촉 및 해촉한다.

제60조(위원장 및 간사의 직무) ①위원장의 직무는 다음 각 호와 같다.

1. 위원회 업무 총괄 및 회의 주재
2. 선임직 위원 위촉 및 해촉

②간사의 직무는 다음 각 호와 같다.

1. 심의안건 상정 및 위원회 회의 진행
2. 위원회 심의결과 및 회의결과 종합

제61조(위원회의 개최) ①위원장은 회의를 개최하고자 할 때에는 회의 개최 5일전까지 회의목적, 개최일시, 장소 및 안건 등을 위원에게 통보한다. 다만, 긴급하거나 불가피한 경우에는 회의 개최 전일까지 이를 통보할 수 있다.

②간사는 위원회 회의안건을 작성하여 위원회에 상정한다.

③위원회는 재적위원 과반수의 출석으로 개최하며 출석위원 전원의 찬성으로 의결한다.

제62조(심의·의결) ①위원회는 심의안건에 대한 이해도를 제고하기 위하여 심의를 요청한 기관에 설명을 요청할 수 있다.

②위원은 안건에 대한 심의결과를 의안 검토의견을 서면으로 위원장에게 제출하여야 한다.

③위원회가 정보보호제품 등의 평가결과에 대한 심의결과 '부(否)' 판정을 내린 경우 신청기관은 '부(否)' 판정 사유를 보완한 후 평가기관에 제출하고 평가기관은 인증기관에 재심의를 요청할 수 있다.

제63조(서면 심의) ①부득이한 사유 등으로 위원회를 개최할 수 없거나 심의 안건이 경미하다고 위원장이 판단할 경우에는 서면으로 심의·의결을 할 수 있다.

②서면으로 심의·의결할 경우에는 제61조 제3항을 준용한다.

제64조(보안조치) ①위원장은 평가·인증업무와 관련된 중요정보 유출을 방지하기 위하여 회의에 참여하는 위원에 대하여 서약서(별지 제21호 서식)를 제출받고 보안교육을 실시한다.

②위원은 회의 종료시 관련 자료를 모두 인증기관에 반납하여야 한다.

제65조(자문·심의비 지급) 인증기관은 회의에 참여한 위원에 대하여 소정의 자문·심의비를 지급한다. 다만, 공무원인 위원에 대하여는 자문·심의비를 지급하지 아니 한다.

제6절 인증서보유기관

제66조(인증내용 오·남용 금지) ①인증서보유기관은 인증제품에 대해 인증을 받은 내용 이외의 허위사실을 제품에 표기·광고하거나, 인증제품의 형상을 변경하는 등 인증받지 않은 제품에 대해 인증제품으로 표기·광고하여서는 아니 된다.

②인증서보유기관 등은 공통평가기준(CC) 인증마크, 국제상호인정협정 서비스마크 등을 인증기관과 협의 없이 무단사용해서는 아니 된다.

제67조(평가결과보고서 열람) 인증서보유기관은 평가기관에 대해 평가결과보고서의 열람 또는 제공을 요청할 수 있다. 다만, 평가기관은 평가기관의 지적재산권과 관련된 부분에 대해서는 열람 또는 제공 요청을 거절할 수 있다.

제3장 인증제품 관리

제68조(인증제품 목록 등 공개) ①인증기관의 장은 인증제품에 대한 정보를 인증기관 홈페이지 및 국제상호인정협정 홈페이지에 공개한다.

②제1항의 인증제품에 대한 정보는 다음 각 호의 사항을 포함하여야 한다. 다만, 국제상호인정협정 홈페이지에 공개되는 정보는 관련 규정에 따른다.

1. 제품 개요(평가대상제품명, 제품 유형, 개발사・신청기관 등)
2. 평가 개요(평가보증등급, 제품이 준수한 보호프로파일, 평가시 적용한 평가기준 버전, 평가기관 등)
3. 인증 개요(인증번호, 인증일 등)
4. 제품의 보안목표명세서
5. 제품에 대한 인증보고서
6. 인증서 사본(영문본에 한함)
7. 제69조의 인증효력유지와 관련된 보고서(해당사항이 있는 경우에만 한함)

③인증된 보호프로파일에 대한 정보는 다음 각 호의 사항을 포함하여야 한다. 다만, 국제상호인정협정 홈페이지에 공개되는 정보는 관련 규정을 따른다.

1. 보호프로파일 명칭
2. 보호프로파일의 제품 유형
3. 평가보증등급
4. 등재일
5. 보호프로파일 인증보고서
6. 보호프로파일 보조문서(해당사항이 있는 경우에만 한함)

제69조(인증효력유지) ①인증서보유기관이 인증제품의 보증에 주요한 영향을 주는 변경을 한 경우에는 재평가를 평가기관에 신청할 수 있고, 경미한 영향을 주는 변경을 한 경우에는 변경승인을 위하여 인증효력유지 신청서(별지 제22호 서식) 및 보안영향분석서(별지 제23호 서식)를 작성하여 평가기관에 신청할 수 있다.

②평가기관은 인증효력유지 여부 판단이 모호한 경우에는 인증기관에 자문을 구하여야 하며, 형상변경 범위 등에 대한 확인을 위하여 보안기능 분석시험을 수행할 수 있다.

③인증효력유지의 세부절차는 국제상호인정협정 관리위원회가 발표한 「보증 연속성 : CCRA 요구사항」(Assurance Continuity: CCRA Requirements) 최신문서를 준용한다.

제70조(인증서 재발급) ①인증서보유기관은 다음 각 호의 하나의 사안이 발생하여 인증서 재발급을 희망하는 경우 신청서(별지 제24호 서식)를 작성

하여 평가기관에 제출해야 한다.

1. 인증서를 훼손 또는 분실한 경우
2. 인증서의 사용 권리를 양수한 경우
3. 인증서보유기관이 기관명을 변경한 경우

②제1항 제2호에 의거 인증서 재발급을 요청할 경우에는 다음 각 호의 서류를 첨부하여야 한다.

1. 인증서 소유권 인수를 증명하는 서류
2. 인증제품 소스코드 관리 등 보안관리대책
3. 제66조에서 정한 인증제품 관리대책

③제1항 제3호에 의거 인증서 재발급을 요청할 경우에는 인증서보유기관 명칭 변경을 확인할 수 있는 서류를 첨부하여야 한다.

④인증기관은 제2항 및 제3항의 점검결과 미비점이 발견될 경우에는 인증서 재발급 요청기관에 보완을 요청할 수 있으며 특별한 사유 없이 이를 이행하지 않을 경우에는 인증서 재발급을 아니할 수 있다.

제71조(인증제품 조사) ①인증기관은 필요시 인증제품에 대한 새로운 취약성, 인증내용 오·남용 여부 등을 점검하기 위하여 평가기관 및 인증서보유기관의 협조를 요청할 수 있다.

②인증기관은 점검결과 문제점이 발견될 경우에는 이를 해당 기관에 통보하고 조사결과를 통보받은 기관은 특별한 사유가 없는 한 30일 이내에 보완조치하고 그 결과를 인증기관에 통보하여야 한다.

제72조(인증서효력 정지) ①인증기관은 제66조의 규정을 위반한 경우 6개월 범위 안에서 기간을 정해 인증서효력을 정지할 수 있다.

②인증기관은 인증서효력이 정지된 경우 인증제품 목록에 있는 해당제품에 인증서효력 정지기간을 표시하고 이를 인증기관 홈페이지에 공지한다.

③인증서효력이 정지된 인증서보유기관은 인증기관 요청 시 지체 없이 인증서를 인증기관에 반납하여 정지기간 동안 인증기관이 인증서를 보관할 수 있도록 하여야 한다.

제73조(인증 취소) ①인증기관은 다음 각 호의 경우에는 인증을 취소하고 그 사유를 인증서보유기관에 통보한다.

1. 허위 또는 부정한 방법으로 평가·인증을 받은 경우

2. 인증서 효력정지 처분을 받고도 그 기간내에 인증제품을 판매한 경우
3. 인증제품이 타사의 지적재산권을 침해한 경우
4. 인증서 효력정지 처분 기간내에 효력정지 사유에 대한 시정조치를 수행하지 않은 경우

②제1항에 의거 인증이 취소된 경우에는 해당 인증서보유기관에 대해 6개월 범위 내에서 평가신청을 제한할 수 있다.

③인증기관은 인증제품에 중대한 취약성을 확인한 경우 평가기관과 인증서보유기관에 통보·협의하여 다음 각 호와 같이 필요한 조치를 취할 수 있다.

1. 인증 취소
2. 후속 제품 인증이 완료된 경우 해당 인증제품 참조 정보 제공

④인증기관은 인증이 취소된 경우에는 해당 제품을 인증제품 목록에서 삭제하고 인증취소 목록으로 이동한 후 이를 인증기관 홈페이지에 공지한다.

⑤인증이 취소된 인증서보유기관은 지체 없이 인증서를 인증기관에 반납하여야 한다.

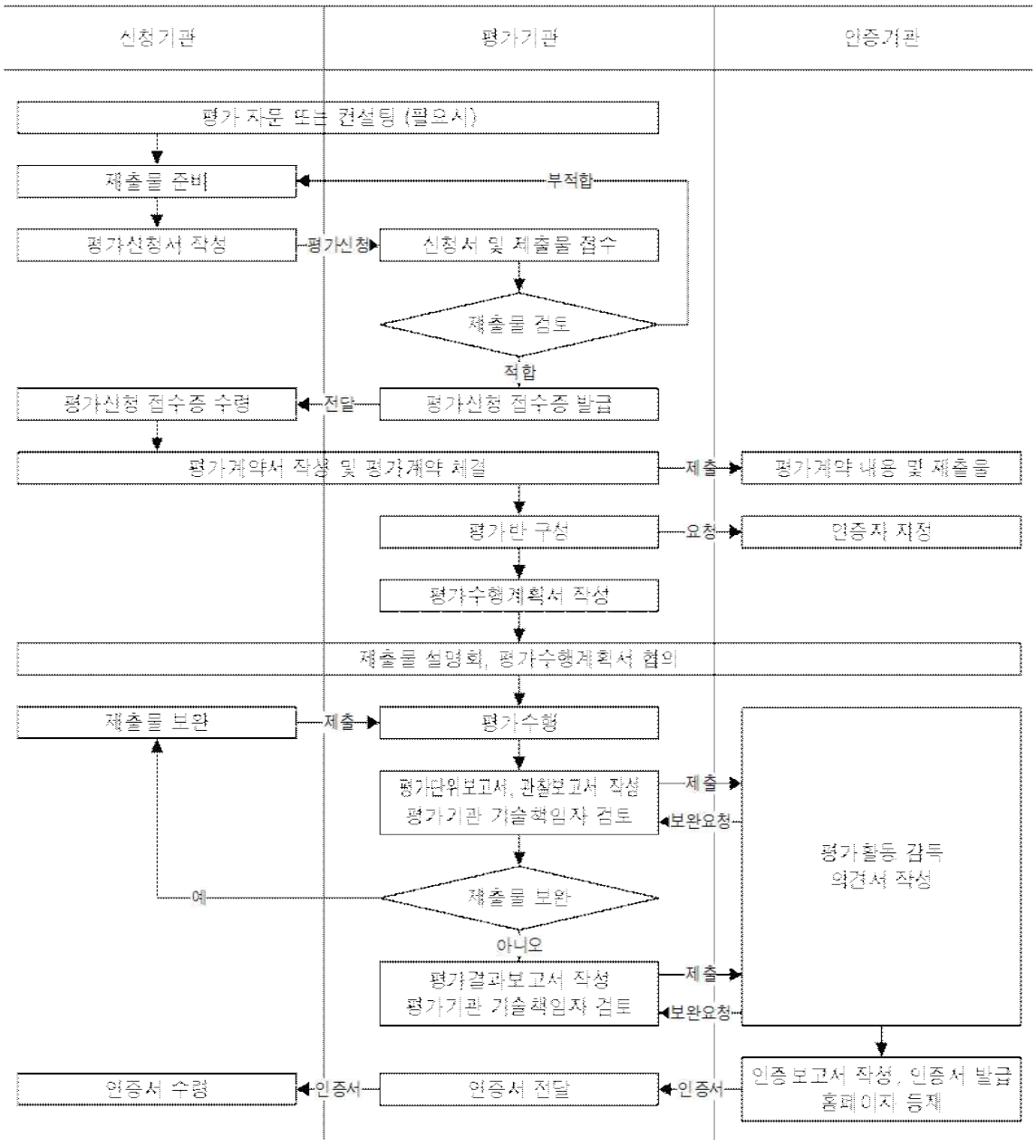
부 칙

제1조(시행일) 이 규정은 2017년 6월 26일부터 시행한다.

제2조(국내용 정보보호제품) 국내용 정보보호제품 평가·인증업무에 필요한 세부사항은 이 규정에서 붙임으로 정한 「정보보호제품 국내용 평가·인증 세부 수행절차」를 따른다.

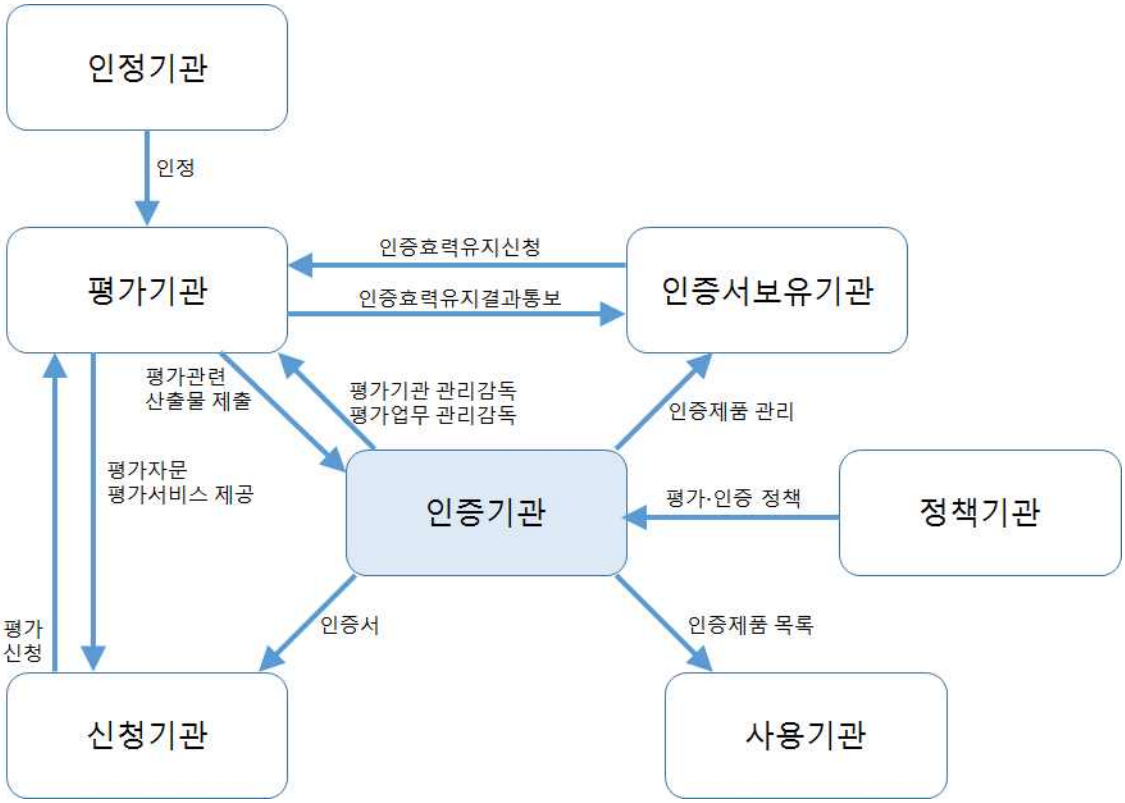
〔별표 1〕

정보보호제품 평가·인증 절차



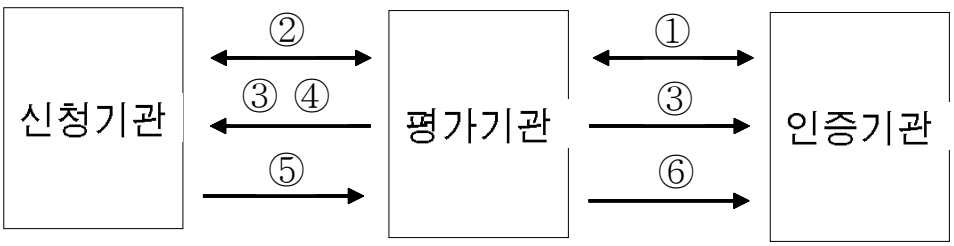
〔별표 2〕

정보보호제품 평가·인증체계



〔별표 3〕

개발환경 보안점검 절차



① 평가기관은 신청기관의 개발환경에 대한 보안점검을 할 경우에는 사전에 인증기관과 협의한다.

② 평가기관은 ①항의 협의내용을 신청기관에 통보하고 보안점검관련 일정 등을 협의한다.

③ 평가기관은 신청기관의 보안점검을 위한 세부계획을 수립하여 신청기관과 인증기관에 통보, 협조를 요청한다.

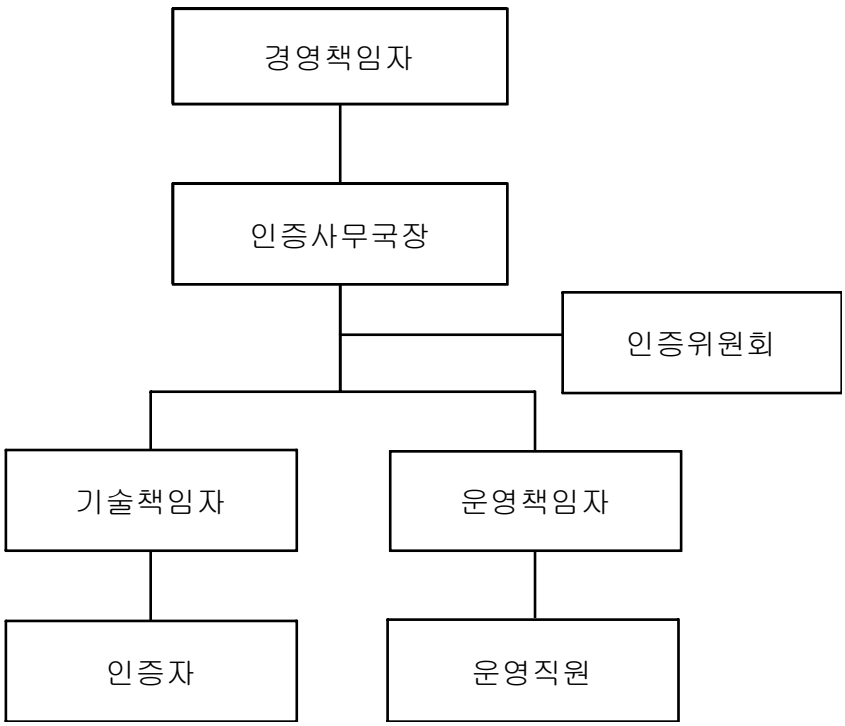
④ 평가기관은 보안점검 결과 나타난 문제점에 대한 조치계획을 수립하여 인증기관과 협의한 후 그 결과를 신청기관에 통보하여 시정토록 한다.

⑤ 신청기관은 ④항의 문제점에 대한 시정 결과를 평가기관에 제출한다.

⑥ 평가기관은 보안점검 결과를 평가결과보고서에 반영한다.

〔별표 4〕

IT보안인증사무국 조직도



〔별표 5〕

제 품 군 표 기

제품군	제품 유형 예
네트워크 정보보호 제품군 **NISS** (Network Information Security System)	· 침입차단시스템 · 침입방지시스템 · 가상사설망 · 인터넷전화 보안 · 네트워크 접근통제 · 무선랜 인증 · 무선침입방지
정보보호 기반 제품군 **ISIS** (Information Security Infrastructure System)	· 스마트카드 운영체제 · 전자여권 · 자바카드 플랫폼 · 자료유출방지 · 통합보안관리
컴퓨팅 정보보호 제품군 **CISS** (Computing Information Security System)	· 데이터베이스 접근통제 · 디지털복합기 · 서버 접근통제 · 보안 USB · 스마트폰 보안관리
보호프로파일 **PP** (Protection Profile)	-

* 상기 분류표기는 정보보호제품 전체를 의미하지 않음

〔별지 제1호 서식〕

서 약 서

소 속		직(급)위	
성 명			

본인은 정보보호제품 평가기관 직원으로서 공정하고 객관적인 업무 수행과 윤리 의무를 다하기 위하여 아래 사항을 준수할 것을 서약한다.

1. 정보보호제품 평가·인증 관련규정을 준수한다.

2. 부여된 책임과 권한에 따라 평가업무를 성실하고 공정하게 수행한다.

3. 재직 중은 물론 퇴직 후에도 직무상 지득한 기밀을 누설하지 않는다.

4. 평가기관 및 인증기관의 위상을 저해하는 어떠한 활동에도 참여하지 않는다.

만일 이를 위반할 경우에는 관련 법규에 의거 어떠한 처벌도 감수할 것을 서약합니다.

년 월 일

서약자 (서명 또는 인)

집행자 (서명 또는 인)

〔별지 제2호 서식〕

제출물 인계인수증

□ 제품명 :

제출물명	제출물형태	부수	비고

상기 제출물을 인계 및 인수하였습니다.

년 월 일

인계자 : (소속) (성명) (서명 또는 인)

인수자 : (소속) (성명) (서명 또는 인)

〔별지 제3호 서식〕

제출물 관리대장

제출물 접수 기록				반환·폐기 기록			
관리번호	수령일	수령자	TOE명	반환일/ 폐기일	반환자/ 폐기자	확인자	비고

〔별지 제4호 서식〕

(앞 면)

접 수 번 호 제 호	평가신청서			
신청기관	① 신청형태	□ 단독신청 □ 공동신청		
	② 상 호		③ 구 분	□제조자 □판매자 □수입자
	④ 주 소	□□□□□		
	⑤ 대 표 자 성 명		사업자등록번호	
	⑥ 담 당 자		부 서 명	
			전 화	
			팩 스	
평 가 신 청 제 품	⑦ 평가기준		⑧ 적용 보호프로파일	
	⑨ 제품명/보호프로파일		⑩ 제 품 분 류	
	⑪ 제품번호		⑫ 운 영 체 제	
	⑬ 개발국가		⑭ 개발자 명	
⑮ 신청구분	□최초평가 □재평가 □보호프로파일 평가		⑯ 신 청 등 급	
⑰ 인증번호				

정보보호제품 평가·인증 수행규정에 의하여 상기와 같이 평가를 신청하며, 기재사항에 허위사실이 없음을 확인합니다.

년 월 일

신 청 인 (서명 또는 인)

<평가기관장> 귀하

(뒷 면)

평가신청서 작성요령

1. 해당하는 빈칸에 ☑ 와 같이 표기한다.
2. 각 항목의 작성요령은 다음과 같다.
   ① 평가신청 형태에 따라 표기를 하고 2인 이상 공동으로 신청할 때는 별지 제5호 서식의 공동신청기관 명부를 추가로 작성한다.
   ② 신청기관의 상호 또는 명칭을 기재한다.(공동신청의 경우에는 대표신청기관 상호 또는 명칭 기재)
   ③ 신청기관이 정보보호제품 제조자, 판매자 및 수입자인지를 구분하여 모든 해당항목에 표기한다.(공동신청의 경우에는 대표신청기관)
   ④ 신청기관의 주된 사업장 주소를 기재한다.(공동신청의 경우에는 대표신청기관)
   ⑤ 신청기관의 이름 및 사업자등록번호를 기재한다.(공동신청의 경우에는 대표신청기관)
   ⑥ 평가신청 업무 담당자의 성명, 부서명, 전화번호 등을 기재한다.
   ⑦ 정보보호제품 또는 보호프로파일 평가에 적용되는 평가기준의 버전을 기재한다.
   ⑧ 정보보호제품이 적용한 보호프로파일 명칭을 기재한다.
   ⑨ 평가신청제품 또는 보호프로파일의 명칭(모델명)과 버전번호를 기재한다.
   ⑩ 평가신청 제품의 형태를 기재한다.(예 : 침입차단시스템)
   ⑪ 정보보호제품의 제품번호를 기재한다. 다만, 보호프로파일을 평가신청할 경우에는 기재하지 아니한다.
   ⑫ 정보보호제품의 운영체제 명칭과 버전번호를 기재한다. 다만, 보호프로파일을 평가신청할 경우에는 기재하지 아니한다.
   ⑬ 정보보호제품 또는 보호프로파일이 개발된 국가명을 기재한다.

⑭ 정보보호제품 또는 보호프로파일의 개발자 혹은 개발업체를 기재한다.

⑮ 다음의 평가신청 구분에 따라 표기한다.

- 최초평가 : 처음으로 정보보호제품을 평가신청하는 경우
- 재 평 가 : 인증제품의 보증에 주요한 영향을 주는 변경이 발생한 경우
- 보호프로파일 평가 : 보호프로파일 평가신청인 경우

⑯ 정보보호제품 또는 보호프로파일의 평가신청등급을 기재한다.

⑰ 재평가를 신청하는 경우 이전에 부여받은 인증서 번호를 기재한다.

〔별지 제5호 서식〕

공동신청기관 명부

신청기관	상호		구분	□ 제조자 □ 판매자 □ 수입자
	주소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담당자		부서명	
			전화	
			팩스	
신청기관	상호		구분	□ 제조자 □ 판매자 □ 수입자
	주소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담당자		부서명	
			전화	
			팩스	
신청기관	상호		구분	□ 제조자 □ 판매자 □ 수입자
	주소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담당자		부서명	
			전화	
			팩스	
신청기관	상호		구분	□ 제조자 □ 판매자 □ 수입자
	주소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담당자		부서명	
			전화	
			팩스	

〔별지 제6호 서식〕

이의·불만·분쟁처리 신청서

신 청 기 관	업 체 명	
	대 표 자	
	연 락 처	
제 품 명		
신 청 구 분	□ 이의 □ 불만 □ 분쟁	
사 유		

정보보호제품 평가·인증 수행규정에 의거하여 위와 같이 (이의, 불만, 분쟁) 해결을 신청합니다.

년 월 일

신청인 : (서명 또는 인)

〔별지 제7호 서식〕

<table>
<tr><td colspan="2">접 수 번 호
제 호</td><td colspan="4">평가기관 승인신청서</td></tr>
<tr><td rowspan="6">신청
기관</td><td>① 법 인 명</td><td colspan="4"></td></tr>
<tr><td>② 법인주소</td><td colspan="4">□□□□□</td></tr>
<tr><td>③ 평가기관주소</td><td colspan="4">□□□□□</td></tr>
<tr><td>④ 대표자
성 명</td><td></td><td>법인등록번호</td><td colspan="2"></td></tr>
<tr><td>⑤ 담당자</td><td></td><td>연락처</td><td colspan="2">전 화 :
E-Mail :</td></tr>
<tr><td>⑥ 평가업무
수행범위</td><td colspan="4"></td></tr>
</table>

정보보호제품 평가·인증 수행규정에 의거하여 평가기관 승인을 신청하오니 심사하여 주시기 바랍니다.

본 신청과 관련하여 신청서 및 첨부서류의 기재사항에 허위가 없으며, IT보안인증사무국의 승인심사에 모든 협력을 다하겠습니다. 또한, 승인심사 과정에서 알게 된 유·무형의 모든 정보를 임의로 유출하지 않으며, 심사 결과에 대해서도 어떠한 이의를 제기하지 않겠습니다.

년 월 일

신 청 인
법인대표: (법인인감)

IT보안인증사무국장 귀하

〔별지 제8호 서식〕

평가기관 준수사항 서약서

법인 _____(이하 '법인'이라 한다)은/는 평가기관 승인 신청기관으로서 다음 사항을 준수할 것을 서약합니다. 또한 평가기관으로 승인받은 이후에도 다음 사항을 준수할 것을 서약합니다.

1. 법인은 정보보호제품 평가·인증 관련규정을 준수하겠습니다.
2. 법인은 평가 수행에 있어 공통평가기준 및 방법론을 적용하고 인증기관의 관리·감독을 성실히 수용하겠습니다.
3. 법인은 평가신청기관의 저작권 사항 등 평가과정에서 지득한 정보를 모회사, 자회사, 계열회사, 투자자, 채권자 등 제3자에게 유출하지 않겠습니다.
4. 법인은 평가신청기관 등이 평가업무의 결함 또는 정보의 유출 등의 사유로 손해배상을 청구하는 경우, 이에 대한 손해배상 처리를 책임지겠습니다.

년 월 일

IT보안인증사무국장 귀하

법 인 명 : 법인등록번호 :
법인 주소 :
대표자성명 : (법인인감)

상기 법인의 대표자 _____은/는 법인의 손해배상 책임에 대해 연대보증책임을 질 것을 서약합니다.

대 표 자 명 : (대표자인감)
대표자 주소 :

〔별지 제9호 서식〕

<접수번호>

관리 번호	

평가결과보고서

<평가대상제품명>

년 월 일

<평가기관명>

제 1 장 개요

o 일반적으로 다음의 사항을 포함한다.

- 정보보호제품 평가·인증 관련규정(수행규정 등)
- 문서 식별정보, 보안목표명세서 및 평가대상제품 식별정보, 적용한 보호프로파일 식별정보
- 신청기관명, 평가기관명, 평가자 이름
- 기타 추가적으로 포함되어야 할 사항

제 2 장 평가대상제품 구조

o 서브시스템 수준의 구조도

* 보호프로파일 평가시 해당되지 않음

제 3 장 평가개요

o 일반적으로 다음의 사항을 포함한다.

- 평가방법(평가기준/평가방법론), 기법, 도구, 평가관련 규제사항 및 평가결과 배포 규제사항(법령, 조직의 내부규정 등) 등
- 기타 추가적으로 포함되어야 할 사항

제 4 장 평가결과

o 평가대상이 정보보호제품인 경우에는 일반적으로 다음의 사항을 포함한다.

- 보증클래스 명, 보증컴포넌트별 판정 및 평가자 판단 근거
- 개발자 시험서 개요, 독립 시험서 개요, 침투 시험서 개요, 악용 가능한 취약성 및 잔여 취약성 목록
- 기타 추가적으로 포함되어야 할 사항

o 평가대상이 보호프로파일인 경우에는 일반적으로 다음의 사항을 포함한다.

- 보호프로파일 평가기준(APE) 및 평가방법론에 의거한 보증컴포넌트별 판정 및 평가자 판단 근거 등
- 기타 추가적으로 포함되어야 할 사항

제 5 장 결론 및 권고사항

o 일반적으로 다음의 사항을 포함한다.

- 총론, 평가결과 요약표, 특이사항, 평가제출물 목록 등
- 기타 추가적으로 포함되어야 할 사항

부록 1 용어정의

부록 2 관찰보고서

o 일반적으로 다음의 사항을 포함한다.

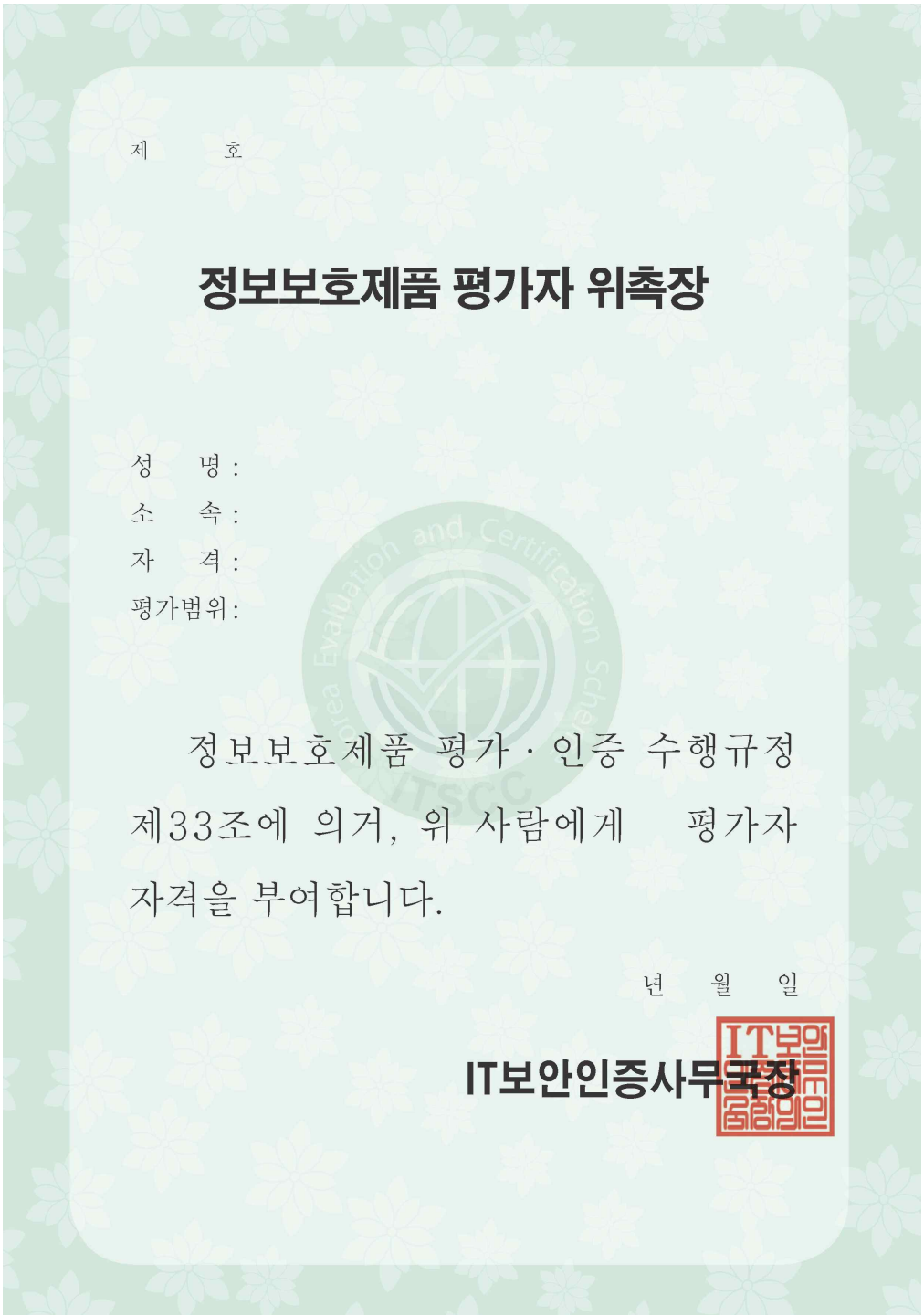
- 보완요청 목록(보완요청 항목, 처리상태, 제목수준의 요약) 등
- 기타 추가적으로 포함되어야 할 사항

［별지 제10호 서식］

평가기관 승인서

〔별지 제11호 서식〕

정보보호제품 평가자 위촉장



제 호

정보보호제품 평가자 위촉장

성 명 :
소 속 :
자 격 :
평가범위 :

정보보호제품 평가·인증 수행규정 제33조에 의거, 위 사람에게 평가자 자격을 부여합니다.

년 월 일

IT보안인증사무국장

〔별지 제12호 서식〕

평가자 이력카드

<table>
<tr><th colspan="6">교육 및 평가 이력카드</th></tr>
<tr><td rowspan="4">사진</td><td>소 속</td><td colspan="2"></td><td>직 위</td><td></td></tr>
<tr><td>생년월일</td><td colspan="2"></td><td>이 름</td><td></td></tr>
<tr><td rowspan="2">학 력</td><td colspan="2">최 종 학 력</td><td colspan="2">전 공</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>평가자 자격</td><td>취득일자(수습)</td><td>취득일자(주임)</td><td colspan="2">취득일자(선임)</td></tr>
<tr><td rowspan="4">근무경력</td><td>기 관 명</td><td colspan="2">근무부서/분야</td><td>기 간</td><td>비 고</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="4">국가기술
자격보유</td><td>기술종목 및 등급</td><td colspan="2">등록번호</td><td>등록일자
/유효기간</td><td>발급기관</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="7">교육훈련
(보수교육 등)</td><td>교 육 명</td><td colspan="2">기 간</td><td>교육기관</td><td>비 고</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

〔별지 제12호 서식(계속)〕

제품 평가 이력						
제 품 명	제품유형	평가 기간	평가자 역할	평가정보		비 고
				구분	보증등급	
주특기						

[작 성 요 령]

평가자 자격 : 수습, 주임, 선임 등 평가자 자격 취득일을 기재할 것

근무경력 : 근무기관 및 부서 뿐 아니라 근무분야도 구체적으로 기재할 것

국가기술 자격보유 : 정보보호 또는 IT와 관련된 국가공인 자격증 및 이에 준하는 국제 자격증을 기재할 것

교육훈련 : 정보보호 또는 IT와 관련된 교육과정 이수 실적을 기재할 것

평가구분 : 최초평가/재평가를 기재할 것

평가자 역할 : 평가수행시 역할(반장/반원) 및 담당하였던 분야를 기재할 것

비고 : 평가수행시 보유하였던 평가자 자격을 기재할 것

주특기 : 평가자로서의 경험, 지식 등을 많이 보유한 정보보호제품 유형 및 제품 시험·분석 관련 보유기술 등을 기재할 것

〔별지 제13호 서식〕

평가신청 접수증

접 수 번 호		
접수 담당자		
신 청 기 관	업체명	
	성 명	
	연락처	
제 품 명		
신 청 구 분	□ 최초평가 □ 재평가 □ 보호프로파일 평가	
평 가 기 준		
신 청 등 급		

위와 같이 접수하였음을 확인합니다. 년 월 일 <신청기관장> 귀하	접수인

〔별지 제14호 서식〕

<접수번호>

평가수행계획서

<평가대상제품명>

년 월 일

<평가기관명>

1. 개요

o 평가대상이 정보보호제품인 경우에는 일반적으로 다음의 사항을 포함한다.

- 평가대상제품명, 신청등급, 신청기관, 개발업체, 신청일, 계약일, 신청분류(최초평가/재평가), 적용된 암호기술, 운영체제 등
- 기타 추가적으로 포함되어야 할 사항

o 평가대상이 보호프로파일인 경우에는 일반적으로 다음의 사항을 포함한다.

- 보호프로파일명, 신청등급, 신청기관, 개발업체, 신청일, 계약일 등
- 기타 추가적으로 포함되어야 할 사항

2. 준수선언

o 일반적으로 다음의 사항을 포함한다.

- 평가기준 식별, 보호프로파일 식별(선택), 패키지 식별(선택) 등
- 기타 추가적으로 포함되어야 할 사항

3. 평가범위

o 일반적으로 다음의 사항을 포함한다.

* 평가대상이 보호프로파일인 경우에는 해당사항 없음

- 보안목표명세서에 명세된 물리적 범위와 논리적 범위를 서술
- 기타 추가적으로 포함되어야 할 사항

4. 평가일정

o 일반적으로 다음의 사항을 포함한다.

- 평가반 구성, 평가 소요기간, 평가 세부 수행계획 등
- 기타 추가적으로 포함되어야 할 사항

5. 신청기관 일반현황

o 일반적으로 다음의 사항을 포함한다.

- 주소, 조직 구성, 주요 사업 등
- 기타 추가적으로 포함되어야 할 사항

〔별지 제15호 서식〕

<접수번호>

평가단위보고서

<평가대상제품명>

년 월 일

<평가기관명>

1. 목적

o 평가단위보고서 작성 목적에 대해 서술

2. 참조문서

o 일반적으로 다음의 사항을 포함한다.

- 평가단위보고서에 사용된 평가 참조문서(예 : 공통평가기준, 공통평가방법론, 보호프로파일, 정보보호제품 평가·인증 수행규정) 등
- 평가단위보고서 작성에 사용된 제출물 등
- 기타 추가적으로 포함되어야 할 사항

3. 평가

o 일반적으로 다음의 사항을 포함한다.

- 평가항목별 평가자 조사활동 목적, 평가자 조사방법(평가과정), 평가자 판정 근거(결론) 등 세부 평가활동 내역 기록 등
- 기타 추가적으로 포함되어야 할 사항

4. 결론

o 일반적으로 다음의 사항을 포함한다.

- 공통평가방법론에서 요구하는‘평가자 요구사항별 평가자 판정’및‘컴포넌트별 평가자 판정’
- 기타 추가적으로 포함되어야 할 사항

※ 독립·취약성 시험, 개발환경보안점검과 관련한 계획서 및 결과보고서는 별도로 작성 가능

〔별지 제16호 서식〕

<접수번호>

관찰보고서

<평가대상제품명>

년 월 일

<평가기관명>

1. 개요

o 일반적으로 다음의 사항을 포함한다.

- 평가신청 개요 : 접수번호, 평가대상제품명, 평가보증등급, 신청기관명 등
- 관찰보고서 개요 : 관찰보고서 식별정보, 보완요청 목록, 회의 일시, 평가자 이름, 신청기관 담당자 이름 등

2. 보완요청

o 보완요청 항목에는 일반적으로 다음의 사항을 포함한다.

- 컴포넌트 식별, 보완내용, 평가에 미치는 영향정도, 보완요청 이행 기관, 보완요청 이행 기한, 보완요청을 이행하지 않은 경우 평가에 미치는 영향 등
- 기타 추가적으로 포함되어야 할 사항

3. 서명

o 일반적으로 다음의 사항을 포함한다.

- 보완요청 사항 요약정보(보완요청 항목 번호, 작업단위, 평가에 미치는 영향정도, 보완요청 이행 기간) 등
- 인증기관, 평가기관, 신청기관의 서명 등

〔별지 제17호 서식〕

평가중단통보서

1. 평가신청 내역

○ 접 수 번 호 :

○ 제 품 명 :

○ 평가신청등급 :

○ 신 청 분 류 :

○ 평 가 기 준 :

○ 평가신청접수일 : 년 월 일

2. 평가중단 사유

(부족시 별지 사용)

［별지 제18호 서식］

(국문)

정보보호제품 인증서

(영문)

정보보호제품 인증서

(국문)

보호프로파일 인증서

(영문)

보호프로파일 인증서

〔별지 제19호 서식〕

인 증 마 크

1. 인증마크 도안

2. 인증번호는 다음과 같다.

   KECS-제품군 표기-일련번호-발급년도

3. 제품군 표기는 별표 5와 같다.

4. 위의 인증마크는 사용자가 확인할 수 있도록 제품 또는 품질보증서 등에 부착하며, 인증기관과 사전협의를 통해 그 사용목적에 따라 동일한 비율로 확대하거나 축소하여 사용할 수 있다.

〔별지 제20호 서식〕

(앞 면)

<table>
<tr><td colspan="3">접수번호
제 호</td><td colspan="3">인증마크 사용신청서</td><td>처 리 기 간
15일</td></tr>
<tr><td rowspan="4">신청
기관</td><td>① 상 호</td><td></td><td>② 구 분</td><td colspan="3">□ 제조자 □ 판매자 □ 수입자</td></tr>
<tr><td>③ 주 소</td><td colspan="5">□□□□□</td></tr>
<tr><td>④ 대표자 성명</td><td></td><td>사업자등록번호</td><td colspan="3"></td></tr>
<tr><td>⑤ 담당자</td><td></td><td>부 서 명</td><td colspan="3">전 화 :
E-Mail :</td></tr>
<tr><td colspan="2">⑥ 제 품 분 류</td><td colspan="5"></td></tr>
<tr><td colspan="2">⑦ 제 품 명</td><td colspan="5"></td></tr>
<tr><td colspan="2">⑧ 운 영 체 제</td><td colspan="5"></td></tr>
<tr><td colspan="2">⑨ 인 증 번 호</td><td colspan="5"></td></tr>
<tr><td colspan="2">⑩ 평가보증등급</td><td colspan="5"></td></tr>
<tr><td colspan="2">⑪ 신 청 수 량</td><td colspan="5"></td></tr>
<tr><td colspan="7">정보보호제품 평가·인증 수행규정에 의거하여 상기와 같이 인증마크 사용을 신청하며, 기재사항에 허위사실이 없음을 확인합니다.

년 월 일

신 청 인 (서명 또는 인)

IT보안인증사무국장 귀하</td></tr>
</table>

(뒷 면)

인증마크 사용신청서 작성요령

1. 해당하는 빈칸에 ☑ 와 같이 표기한다.
2. 각 항목의 작성요령은 다음과 같다.
   ① 신청기관의 상호 또는 명칭을 기재한다.
   ② 신청기관이 정보보호제품 제조자, 판매자 및 수입자인지를 구분하여 모든 해당항목에 표기한다.
   ③ 신청기관의 주된 사업장 주소를 기재한다.
   ④ 신청기관의 이름 및 사업자등록번호를 기재한다.
   ⑤ 평가신청 업무담당자의 성명, 부서명, 전화번호 등을 기재한다.
   ⑥ 제품분류 또는 대상제품군(네트워크 정보보호제품, 정보보호 기반제품, 컴퓨팅 정보보호제품, 보호프로파일)을 기재한다.
   ⑦ 해당 정보보호제품의 제품명칭(모델명)과 버전번호를 기재한다.
   ⑧ 해당 정보보호제품의 운영체제 명칭과 버전번호를 기재한다.
   ⑨ 교부받은 인증번호를 기재한다.
   ⑩ 부여받은 해당 정보보호제품의 평가보증등급을 기재한다.
   ⑪ 교부받고자 하는 인증마크의 수량을 기재한다.

〔별지 제21호 서식〕

서 약 서

본인은 년 월 일부로 정보보호제품 평가·인증 수행규정에 의거하여 인증위원회의 위원으로 활동함에 있어 업무 수행중에 지득한 기밀사항을 무단으로 유출하거나 공개하지 아니할 것을 서약하며 이를 위반할 경우에는 관련 법규에 의거 어떠한 처벌도 감수할 것을 서약합니다.

년 월 일

서약자
소속 직급(위)
성명 (인)

집행자
소속 성명 (인)

〔별지 제22호 서식〕

인증효력유지 신청서

신청기관	상 호	
	대 표 자	
	담 당 자	전 화 : E-Mail :
인증제품	제 품 명	
	운 영 체 제	
	평가보증등급	
	인 증 번 호	

정보보호제품 평가·인증 수행규정에 의거하여 상기와 같이 인증효력유지를 신청합니다.

년 월 일

신청인 (서명 또는 인)

［별지 제23호 서식］

보안영향분석서

(Security Impact Analysis Report)

1. 인증제품 개요

가. 작성자 정보 (인증서보유기관명, 작성일, 작성자 등)

나. 인증제품 (제품명, 버전, 인증번호, 인증일, 평가보증등급 등)

다. 이전 『변경승인』에 관련된 내용 (제품명, 버전, 인증효력유지번호, 변경승인일, 변경승인 내용 등 전체 변경승인 이력)

2. 변경 내역

가. 변경 前≠ 시스템 구성 및 後 시스템 구성

나. 변경된 보안기능 및 인터페이스

다. 변경 사유 및 변경 내용 (변경 후 인증제품 세부 버전 포함)

라. 변경된 보안기능 항목 및 보안속성 (주체, 객체, 사용자 관련 정보)

마. 변경이 보안기능 항목 및 보안속성에 미치는 영향

바. 변경이 기본설계와 상세설계에 미치는 영향

사. 변경된 소스코드 및 설명 (인증제품 생성 시 포함된 전체 소스코드 대비 변경된 소스코드 위치 및 내용 설명)

아. 테스트 정보 (테스트범위 분석, Test Case, 시험절차, 테스트결과 등)

자. 변경된 제출물 범위 및 내용 서술

〔별지 제24호 서식〕

인증서 재발급 신청서

<table>
<tr><td rowspan="5">재발급
신청기관</td><td>상 호</td><td colspan="2"></td></tr>
<tr><td>주 소</td><td colspan="2"></td></tr>
<tr><td>대표자 성명</td><td colspan="2"></td></tr>
<tr><td>사업자등록번호</td><td colspan="2"></td></tr>
<tr><td>전화/E-Mail</td><td colspan="2"></td></tr>
<tr><td rowspan="5">재발급
사유</td><td>재발급신청사유</td><td>사유발생일자</td><td>사유별 세부내용</td></tr>
<tr><td>□ 인증서 분실 또는 훼손</td><td></td><td></td></tr>
<tr><td>□ 인증서보유기관명 변경</td><td></td><td></td></tr>
<tr><td>□ 인증제품 권리 양도 또는 양수</td><td></td><td></td></tr>
<tr><td>□ 기타</td><td></td><td></td></tr>
<tr><td rowspan="5">인증제품</td><td>인 증 번 호</td><td colspan="2"></td></tr>
<tr><td>제 품 분 류</td><td colspan="2"></td></tr>
<tr><td>제 품 명</td><td colspan="2"></td></tr>
<tr><td>보 증 등 급</td><td colspan="2"></td></tr>
<tr><td>인증서 교부일</td><td colspan="2"></td></tr>
</table>

정보보호제품 평가·인증 수행규정에 의거하여 상기와 같이 인증서 재발급을 신청합니다.

년 월 일

신청인 (서명 또는 인)

IT보안인증사무국장 귀하

〔별지 제25호 서식〕

정보 공개 동의서

제 품 명 :

본인은 정보보호제품 평가·인증 수행규정(제54조 2항)에 의거, 同 제품 보안목표명세서(또는 보호프로파일) 및 인증보고서 등에 영업비밀 등 중요자료가 포함되지 않아 인증기관 홈페이지 및 국제상호인정협정 홈페이지에 공개를 동의합니다.

년 월 일

업체명 : 대표자 성명 : (서명)

IT보안인증사무국장 귀하

정보보호제품 국내용 평가·인증
세부 수행절차

2017. 6. 26.

목 차

정보보호제품 국내용 평가·인증
세부 수행절차

제1조(목적) 이 지침은 정보호호제품 국내용 평가·인증업무에 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 규정은 정책기관, 인증기관, 평가기관, 신청기관, 인증서 보유기관에 적용한다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다. 단, 이 지침에 규정되지 않은 용어 정의는 「정보보호제품 평가·인증 수행규정」 제3조를 따른다.

1. “국내용 인증 정보보호제품”(이하 ‘국내용 제품’이라 한다)이라 함은 국가·공공기관에 납품할 목적으로 정보보호제품 국내용 평가·인증 세부 수행절차에 따라 인증받는 정보보호제품을 말한다.
2. “유사 정보보호제품”이라 함은 제품의 운영환경(운영체제, 하드웨어 사양 등)은 다르나 구현된 보안기능이 동일한 정보보호제품을 말한다.
3. “일괄평가”라 함은 유사 정보보호제품의 보안기능이 각각의 운영환경에서 정상적으로 안전하게 작동하는지 여부를 동시에 평가하는 방법을 말한다.
4. “정보보호제품 국내용 인증서”(이하 ‘국내용 인증서’라 한다)라 함은 인증기관이 평가기관에서 수행한 국내용 제품의 평가결과를 확정하여 발급하는 증서를 말한다.
5. “국가용 보안요구사항”이라 함은 관계기관이 해당 정보보호제품 유형별로 국가 공공기관에 필요한 필수 보안요구사항을 정의한 문서를 말한다.
6. “평가기준”이라 함은 「정보보호시스템 공통평가기준 버전 3.1 개정 2판」을 정보보호제품 국내용 평가·인증에 적합하게 해석한 것을 말한다.
7. “평가방법론”이라 함은 「정보보호시스템 공통평가방법론 버전 3.1 개정 2판」을 정보보호제품 국내용 평가·인증에 적합하게 해석한 것을 말한다.

제4조(평가・인증 절차) 정보보호제품 국내용 평가・인증 절차는 별표 1과 같다.

제5조(평가・인증 관련기관) 정보보호제품 국내용 평가・인증 관련기관은 「정보보호제품 평가・인증 수행규정」 제8조를 따른다.

제6조(제출물의 관리 등) 정보보호제품 국내용 평가・인증 시 제출물의 관리 등에 관한 규정은 「정보보호제품 평가・인증 수행규정」 제9조, 제10조, 제11조, 제12조, 제13조를 따른다.

제7조(국내용 제품 평가신청) ①신청기관은 정보보호제품을 국내용으로 평가・인증 받고자 할 경우에는 국내용 평가신청서(별지 제1호 서식)와 제출물 2부를 평가기관에 제출하여야 하며, 평가보증등급별 제출물은 별표 2와 같다. 다만, 제출물은 한글로 작성한다.

②신청기관은 국내용으로 평가・인증 받고자 하는 경우 국가용 보안요구사항을 준수하여 제품을 개발하여야 하며, 국내용 인증이 가능한 정보보호제품 유형은 별표 3과 같다.

③신청기관은 제출물 작성 시 「정보보호제품 평가・인증 수행규정」 제15조 제2항, 제3항, 제4항, 제5항을 따른다.

④신청기관은 제품명이 오용되지 않도록 국가용 보안요구사항 및 보안기능에 적합한 제품명으로 평가를 신청하여야 한다.

⑤2개 이상의 기관이 공동으로 평가를 신청할 경우에는 「정보보호제품 평가・인증 수행규정」 제18조를 따른다.

제8조(일괄평가신청) 신청기관은 유사 정보보호제품을 국내용으로 일괄 평가 받고자 할 경우에는 평가신청서(별지 제1호 서식)에 각 운영환경을 기재하여 평가기관에 평가를 신청할 수 있다. 다만, 운영환경의 변화가 평가신청 제품의 보안기능에 중대한 영향을 미칠 경우 그 제품은 일괄평가 신청대상에서 제외된다.

제9조(신청기관) 정보보호제품 국내용 평가・인증 시 신청기관의 책임 및 권한 등에 관한 규정은 「정보보호제품 평가・인증 수행규정」 제19조, 제20조, 제21조, 제22조를 따른다.

제10조(평가기관) ①국내용 제품 평가기관은 「정보보호제품 평가・인증 수행규정」에 따라서 인증기관이 승인한 평가기관으로 한다.

②평가기관 관리, 평가기관 재심사, 평가기관 자격정지 및 자격취소 등에 관한 규정은 「정보보호제품 평가·인증 수행규정」 제27조, 제28조, 제30조, 제31조, 제32조를 따른다.

제11조(평가자) 국내용 제품 평가자에 관한 규정은 「정보보호제품 평가·인증 수행규정」 제33조 및 제48조를 따른다. 다만, 「정보보호제품 평가·인증 수행규정」에 따라서 주임평가자로 위촉된 자는 EAL3 등급 이내에 대해 국내용 제품 평가수행이 가능하다.

제12조(평가기관 의무 등) ①평가대상제품의 개발 또는 제출물 작성에 참여한 평가자는 해당 제품의 평가에 참여하여서는 아니 된다.

②평가기관은 「정보보호제품 평가·인증 수행규정」 제35조에 따라 신청기관의 자문 또는 컨설팅에 응할 수 있다. 다만, 「정보보호제품 평가·인증 수행규정」 제35조 제1항 제2호의 보호프로파일 적용 방법에는 적용하지 아니한다.

③평가기관은 「정보보호제품 평가·인증 수행규정」 제36조에 따라 평가신청접수증을 발급하거나 발급하지 아니할 수 있다. 다만, 평가신청제품에 대한 국가용 보안요구사항이 존재하지 않는 경우 평가신청접수증을 발급하지 아니할 수 있다.

④평가기관은 「정보보호제품 평가·인증 수행규정」 제37조에 따라 평가계약을 체결하여야 한다. 다만, 정보보호제품 평가·인증 수행규정」 제37조 제3항에 따른 정보 공개는 국내용 인증 정보보호제품 정보 공개 동의서(별지 제9호 서식)에 따라 인증보고서를 인증기관 홈페이지에 공개하는 것에 한한다.

⑤평가기관은 「정보보호제품 평가·인증 수행규정」 제38조에 따라 전문성을 확보하여야 한다.

⑥평가기관은 「정보보호제품 평가·인증 수행규정」 제42조에 따라 국내용 제품 평가관련 업무를 위탁할 수 있다.

⑦평가기관은 「정보보호제품 평가·인증 수행규정」 제44조에 따라 국내용 제품 평가결과보고서를 제공할 수 있다.

⑧평가기관은 「정보보호제품 평가·인증 수행규정」 제45조 및 제46조에 따라 국내용 제품 평가를 중단하거나 평가계약을 해지할 수 있다.

⑨평가기관은 「정보보호제품 평가·인증 수행규정」 제47조에 따라 제출물을 반납하여야 한다.

제13조(사전점검) ①평가기관은 평가신청제품이 국가용 보안요구사항을 만족하는지 사전에 점검하고 기술책임자의 검토를 완료하여 인증기관에 그 결과를 제출하여야 한다.

②신청기관은 평가기관으로부터 사전점검 시 제품의 수정·보완을 요구받은 사항에 대해서는 수정·보완하여야 한다.

제14조(국내용 제품에 대한 평가) ①제출물 설명회 및 평가수행계획서 작성에 관한 규정은 「정보보호제품 평가·인증 수행규정」 제39조 및 제40조를 따른다. 다만, 국내용 제품에 대한 평가보증등급은 EAL2, EAL3 또는 EAL4로 한정한다.

②평가기관은 인증기관이 승인한 평가수행계획서에 따라 평가대상제품이 국가용 보안요구사항, 평가기준 및 평가방법론의 요구수준을 만족하는지 여부를 평가한다. 다만, 평가기관은 평가보증등급에서 요구하는 평가항목 중 인증기관과 사전 협의된 일부항목을 생략하여 평가할 수 있다.

③평가기관은 평가업무 수행과 관련하여 작성한 다음 각 호의 문서를 평가기관 기술책임자의 검토를 완료하여 인증기관에 제출하여야 하며, 평가과정 중에 최소 1회 이상 평가진행 현황을 인증기관에 보고하는 평가진도 점검회의를 개최하여야 한다.

1. 평가수행계획서(별지 제3호 서식)
2. 개발환경 보안점검 보고서, 독립시험서, 침투시험서
3. 관찰보고서(별지 제4호 서식)
4. 평가결과보고서(별지 제5호 서식)
5. 평가·인증 관련 회의록
6. 국가용 보안요구사항 준수 등 인증기관이 요청하는 기타 자료

④평가기관은 국내용 제품에 대한 평가 시 「정보보호제품 평가·인증 수행규정」 제41조 제3항, 제4항, 제5항, 제6항을 따른다. 다만, 정보보호제품 평가·인증 수행규정」 제41조 제6항에 따른 보안목표명세서는 한글로 제출하며 공개하지 아니한다.

⑤국내용 제품에 대한 평가범위는 제품 전 범위를 원칙으로 한다.

⑥평가기관은 국가용 보안요구사항을 평가에 적용하기 어려운 경우 인증기관과 협의 하에 관계기관에 보안요구사항의 해석에 대한 협조를 요청할 수 있다.

제15조(개발환경 보안점검) 평가기관은 「정보보호제품 평가·인증 수행규정」 제43조에 따라 신청기관의 평가대상제품 개발환경에 대한 보안관리 실태를 점검할 수 있다. 다만, 최근 2년 이내에 개발환경 보안점검을 수행한 경우 변경된 부분에 한하여 수행할 수 있다.

제16조(인증자) 국내용 제품 인증자에 관한 규정은 「정보보호제품 평가·인증 수행규정」 제50조를 따른다. 다만, 「정보보호제품 평가·인증 수행규정」에 따라서 주임인증자로 위촉된 자는 EAL4 등급 이내에 대해 국내용 제품 인증수행이 가능하다.

제17조(국내용 제품에 대한 인증) ①제출물 설명회 참석에 관한 규정은 「정보보호제품 평가·인증 수행규정」 제52조 제1항을 따른다.

②인증기관은 제14조 제3항에 의해 평가기관이 제출한 문서 및 평가활동이 국가용 보안요구사항, 평가기준, 평가방법론, 관련 규정을 준수하는지 감독한다.

③인증기관은 국내용 제품에 대한 인증 시 「정보보호제품 평가·인증 수행규정」 제52조 제3항, 제4항, 제5항, 제6항, 제7항을 따른다.

④인증기관은 인증관련 업무 위탁 시 「정보보호제품 평가·인증 수행규정」 제53조를 따른다.

⑤인증기관은 「정보보호제품 평가·인증 수행규정」 제55조 및 제56조에 따라 제출물, 평가산출물, 인증산출물을 처리한다.

제18조(국내용 인증서 발급 등) ①인증기관은 국내용 제품에 대한 인증을 완료하고 인증보고서를 작성한다.

②인증기관은 국내용 제품을 사용하는 기관이 참고할 수 있도록 인증보고서를 인증기관 홈페이지에 공개한다. 다만, 신청기관의 지적재산권과 관련된 자료에 대해서는 평가기관 및 신청기관과 사전 협의하여 공개범위를 결정한다.

③인증기관은 인증이 완료된 국내용 제품에 대해 신청기관에 국내용 인증서(별지 제6호 서식)및 국내용 인증마크(별지 제7호 서식)를 교부한다. 다만, 국내용 인증마크는 신청기관이 국내용 인증마크 사용신청서(별지 제8호 서식)를 평가기관에 제출한 경우에 한해 교부한다.

④인증기관은 인증이 완료되기 전에 신청기관이 인증서를 발급받았다고 허위사실을 공표할 경우 인증서 발급을 거절하거나 6개월 범위 안에서 기

간을 정해 인증서 발급을 연기할 수 있다.

제19조(인증위원회) 인증기관은 정보보호제품 국내용 평가·인증과 관련하여 필요시 인증위원회를 구성·운영할 수 있으며, 인증위원회 구성·운영에 관한 규정은 「정보보호제품 평가·인증 수행규정」 제2장 제5절을 따른다.

제20조(인증서보유기관) ①인증서보유기관은 「정보보호제품 평가·인증 수행규정」 제2장 제6절에 따라 인증내용 오·남용 금지 관련 규정을 준수하여야 하고, 평가기관에 평가결과보고서 열람을 요청할 수 있다.

②인증서보유기관은 인증서를 발급받은 이후 도입된 제품에 새로운 취약점이 발견될 경우에는 즉시 제거하는 등 평가보증등급을 유지하여야 한다.

제21조(인증제품 목록 공개) ①인증기관의 장은 국내용 인증제품에 대한 정보를 인증기관 홈페이지에 공개한다.

②제1항의 국내용 인증제품에 대한 정보는 다음 각 호의 사항을 포함하여야 한다.

1. 제품 개요(평가대상제품명, 제품 유형, 개발사·신청기관 등)
2. 평가 개요(평가보증등급, 적용한 국가용 보안요구사항, 평가시 적용한 평가기준 버전, 평가기관 등)
3. 인증 개요(인증번호, 인증일, 만료일 등)
4. 국내용 제품에 대한 인증보고서
5. 제23조의 인증효력유지 및 제24조의 인증서효력연장과 관련된 보고서(해당사항이 있는 경우에만 한함)

제22조(국내용 인증제품에 대한 관리) ①관계기관이 국가용 보안요구사항을 개정하는 경우 개정된 국가용 보안요구사항의 적용 대상 및 적용 시점은 정책기관과 관계기관이 협의하여 정할 수 있다.

②인증서보유기관이 인증제품에 개정된 국가용 보안요구사항을 적용하고자 하는 경우 재평가를 신청하여야 한다.

③인증기관은 인증서 효력기간 이내라도 다음 각 호의 사안이 발생하여 관계기관의 요청이 있는 경우 정책기관과 협의하여 평가기관 및 인증서보유기관에 필요한 조치를 요청할 수 있다.

1. 인증제품에 새로운 취약점이 발견된 경우
2. 인증제품의 보안기능에 대한 추가 또는 보완이 필요하다고 판단한 경

우

3. 신규 운영체제의 등장 등 인증제품의 안정적인 동작에 영향을 미칠 수 있는 중대한 운영환경 취약점이 발생한 경우

④인증제품 조사와 관련된 규정은 「정보보호제품 평가·인증 수행규정」 제71조를 따른다.

제23조(인증효력유지) 국내용 인증제품의 인증효력유지와 관련된 규정은 「정보보호제품 평가·인증 수행규정」 제69조를 따른다. 다만, 도입된 국내용 인증제품의 긴급한 보안패치 등을 위해 관계기관이 요청하는 경우 인증기관은 정책기관과 협의하여 변경승인 신청을 허용할 수 있다.

제24조(인증서효력연장) ①인증서의 효력은 발급일로부터 3년으로 하며 제2항, 제3항, 제4항에서 정한 절차를 통해 인증제품이 공개된 최신 공격기법에 취약하지 않음이 확인된 경우 인증서효력을 만료일로부터 3년간 연장할 수 있다. 다만, 제22조 제1항에 따라 관계기관이 정책기관과 협의하여 요청하는 경우 개정 이전 국가용 보안요구사항을 준수한 국내용 인증제품의 인증서효력연장을 제한할 수 있다.

②인증서보유기관은 인증서효력연장을 위하여 인증서 만료일 90일 이전에 인증서효력연장 신청서(별지 제10호 서식) 및 자체취약성분석서(별지 제11호 서식)를 작성하여 평가기관에 신청하여야 한다.

③평가기관은 인증서보유기관이 제출한 자체취약성분석서를 검토하여 인증제품이 공개된 최신 공격기법에 대해 취약하지 않음을 확인하고, 인증기관에 자문을 구하여 추가적인 시험을 실시할 수 있다.

④인증서보유기관은 인증서효력연장 신청시 인증제품의 형상을 변경한 경우에는 제23조에서 정한 절차에 따라 인증효력유지 신청을 동시에 해야 한다.

제25조(인증서효력 정지) ①인증기관은 다음 각 호의 경우에는 인증서효력을 정지시킬 수 있다.

1. 인증제품으로 판매된 제품 형상의 무단변경 수준이 「보증 연속성 : CCRA 요구사항」(Assurance Continuity: CCRA Requirements) 최신 문서에 의거, 변경승인 사유에 해당되는 경우 3개월 범위 안에서 기간을 정해 인증서효력을 정지할 수 있다.
2. 인증제품으로 판매된 제품 형상의 무단변경 수준이 「보증 연속성 : CCRA 요구사항」(Assurance Continuity: CCRA Requirements) 최신

문서에 의거, 재평가 사유에 해당되는 경우 3개월 이상 인증서효력을 정지할 수 있다.

3. 제20조 제1항의 인증내용 오·남용 금지 규정 및 제2항의 평가보증등급 유지의 규정을 위반한 경우 6개월 범위 안에서 기간을 정해 인증서효력을 정지할 수 있다.
4. 인증서보유기관이 제22조 제3항 제1호에 의한 조치를 요청받고 특별한 사유 없이 15일 이내에 조치를 취하지 않은 경우 6개월 범위 안에서 기간을 정해 인증서효력을 정지할 수 있다.
5. 인증서보유기관이 제22조 제3항 제2호 또는 제3호에 의한 조치를 요청받고 특별한 사유 없이 6개월 이내에 조치를 취하지 않은 경우 6개월 범위 안에서 기간을 정해 인증서효력을 정지할 수 있다.
6. 인증서효력 만료일까지 제24조 제3항에 대한 확인이 완료되지 않은 경우, 완료시까지 6개월 범위 안에서 인증서효력을 정지할 수 있다.

②인증기관은 인증서효력이 정지된 경우 인증제품 목록에 있는 해당제품에 인증서효력 정지기간을 표시하고 이를 인증기관 홈페이지에 공지한다. 다만, 인증기관 요청시 인증서보유기관은 인증서를 지체 없이 인증기관에 반납하여야 한다.

제26조(인증 취소) ①인증기관은 다음 각 호의 경우에는 인증을 취소하고 그 사유를 인증서보유기관에 통보한다.

1. 허위 또는 부정한 방법으로 평가·인증을 받은 경우
2. 인증서 효력정지 처분을 받고도 그 기간내에 인증제품을 판매한 경우
3. 인증제품이 타사의 지적재산권을 침해한 경우
4. 인증서 효력정지 처분 기간내에 효력정지 사유에 대한 시정조치를 수행하지 않은 경우

②제1항에 의거 인증이 취소된 경우에는 해당 인증서보유기관에 대해 6개월 범위 내에서 평가신청을 제한할 수 있다.

③인증기관은 인증제품에 중대한 취약성을 확인한 경우 평가기관과 인증서보유기관에 통보·협의하여 다음 각 호와 같이 필요한 조치를 취할 수 있다.

1. 인증 취소
2. 후속 제품 인증이 완료된 경우 해당 인증제품 참조 정보 제공

④인증기관은 인증이 취소된 경우에는 해당 제품을 인증제품 목록에서 삭제하고 인증취소 목록으로 이동한 후 이를 인증기관 홈페이지에 공지한다.

⑤인증이 취소된 인증서보유기관은 지체 없이 인증서를 인증기관에 반납하여야 한다.

부 칙

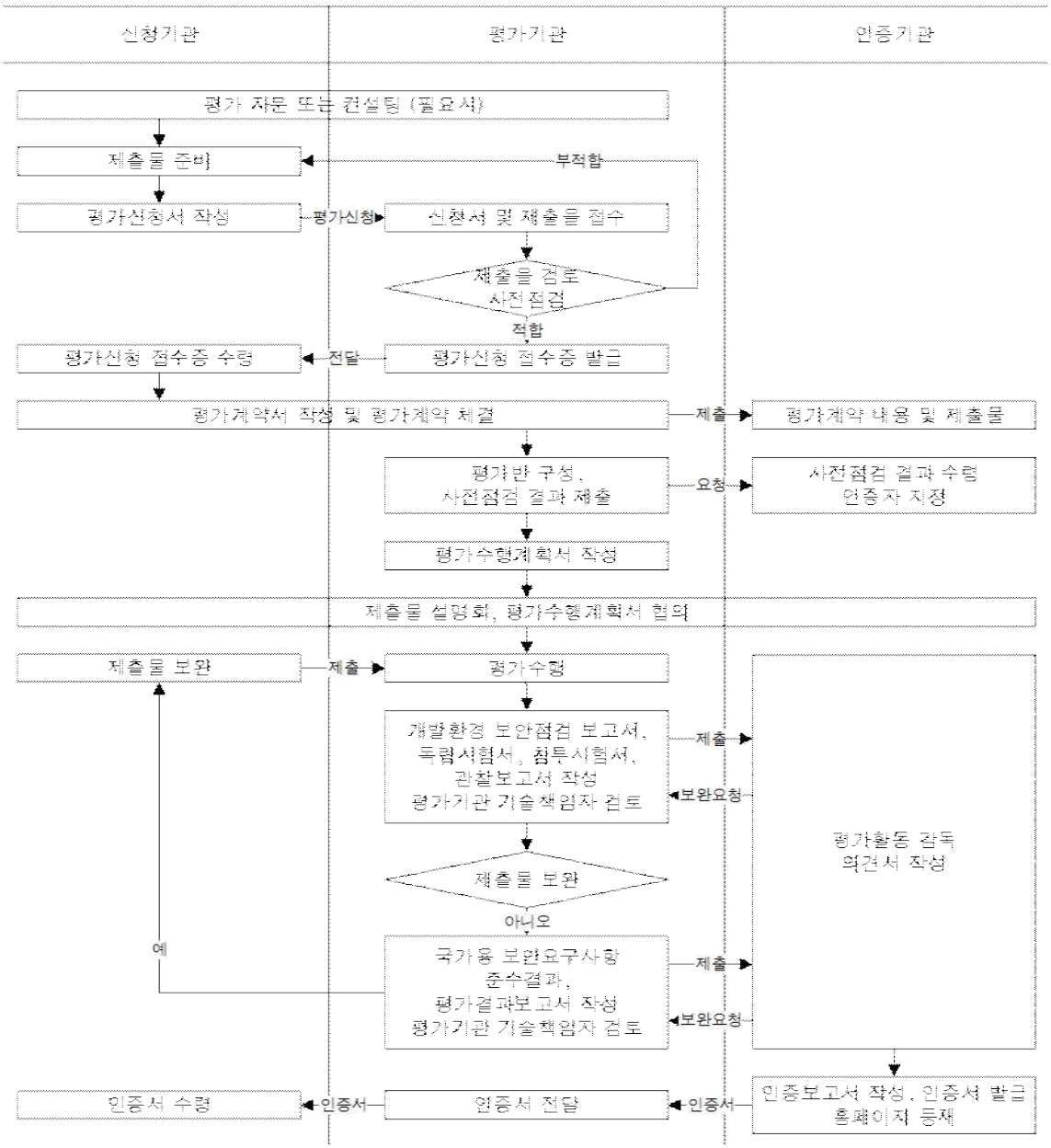
제1조(시행일) 이 절차는 2017년 6월 26일부터 시행한다.

제2조(준용) 이 절차에 규정되지 않은 사항은「정보보호제품 평가·인증 수행규정」에 따른다.

제3조(적용례) 2011년 2월 1일 이전에 인증된 제품의 인증서효력은 2014년 1월 31일까지 유효하다.

〔별표 1〕

정보보호제품 국내용 평가·인증 절차



〔별표 2〕

평가보증등급별 제출물

등 급	제출물
EAL2	1. 보안목표명세서 2. 준비절차서 3. 사용자운영 설명서 4. TOE 설계서 5. 형상관리문서 6. 배포절차서 7. 시험서 8. 취약성 분석서 9. 평가대상제품
EAL3	o EAL 2에서 요구하는 문서를 포함 1. 개발보안문서 2. 생명주기 정의문서
EAL4	o EAL 3에서 요구하는 문서를 포함 1. 구현의 표현 2. 개발도구 문서

〔별표 3〕

국내용 인증가능 정보보호제품 유형

제품 유형	용도
침입차단시스템	네트워크 유입 및 유출 트래픽 통제
침입방지시스템	네트워크 유해트래픽 침입탐지 및 자동차단 (침입탐지시스템 포함)
통합보안관리 제품	복수의 관리대상 시스템 중앙통제, 보안이벤트 통합모니터링 및 분석
웹 응용프로그램 침입차단 제품	웹기반 유해트래픽 침입탐지 및 자동차단
DDoS 대응장비	DDoS 공격 탐지 및 자동 차단
가상사설망 제품	IPSec 또는 SSL 방식 가상사설망
서버 접근통제 제품	서버 접근권한 통제 및 주요 파일 보안설정
DB 접근통제 제품	DB 접근통제 및 데이터 유출방지
네트워크 접근통제 제품	보안프로그램 설치 PC만 네트워크 접속 허용
인터넷전화 보안 제품	인터넷전화 관련 유해트래픽 탐지 및 침입차단
무선침입방지시스템	무선랜 환경에서 보안위협 침입탐지 및 침입차단
무선랜인증 제품	인증된 사용자만 무선랜 접속을 허용
스팸메일 차단시스템	스팸메일 유입 탐지 및 차단
네트워크 자료유출방지 제품	네트워크간 전송되는 트래픽을 통제하여 중요데이터의 외부유출 차단
호스트 자료유출방지 제품	호스트에 설치되어 매체제어 등을 통해 중요데이터의 외부유출 차단 (매체제어 제품 포함)
안티바이러스 제품	PC에 존재하는 악성코드 탐지 및 제거
패치관리시스템	중앙 서버에서 다수 PC에 대한 보안 패치 자동 수행
소프트웨어기반 보안USB	USB 메모리 접근 통제 및 분실 시 자동 삭제
가상화 제품	PC 또는 서버에서 실제영역과 가상영역에 대한 엄격한 영역분리 또는 역영분리 지원
망간 자료전송 제품	보안 수준이 서로 다른 영역간 데이터 및 정보흐름 통제
소스코드 보안약점 분석도구	소프트웨어 소스코드 분석 및 보안약점 식별
스마트폰 보안관리 제품	업무용 관리대상 스마트폰 중앙통제 및 보안관리

* 상기 제품 유형은 변동 가능함

[별지 제1호 서식]

(앞 면)

정보보호제품 국내용 평가신청서

<table>
<tr><td colspan="2">접 수 번 호
제 호</td><td colspan="3">평가신청서</td></tr>
<tr><td rowspan="7">신청기관</td><td>① 신청형태</td><td colspan="3">□ 단독신청 □ 공동신청</td></tr>
<tr><td>② 상 호</td><td></td><td>③ 구 분</td><td>□제조자 □판매자 □수입자</td></tr>
<tr><td>④ 주 소</td><td colspan="3">□□□□□</td></tr>
<tr><td>⑤ 대 표 자
성 명</td><td></td><td>사업자등록번호</td><td></td></tr>
<tr><td rowspan="3">⑥ 담 당 자</td><td rowspan="3"></td><td>부 서 명</td><td></td></tr>
<tr><td>전 화</td><td></td></tr>
<tr><td>팩 스</td><td></td></tr>
<tr><td rowspan="5">평 가 신 청
제 품</td><td>⑦ 평가기준</td><td></td><td>⑧ 적용
보안요구사항</td><td></td></tr>
<tr><td>⑨ 제품명</td><td></td><td>⑩ 제 품 분 류</td><td></td></tr>
<tr><td>⑪ 제품번호</td><td></td><td>⑫ 운 영 환 경</td><td></td></tr>
<tr><td>⑬ 개발국가</td><td></td><td>⑭ 개발자 명</td><td></td></tr>
<tr><td>⑮ 신청구분</td><td colspan="2">□최초평가 □재평가</td><td>⑯ 신 청 등 급</td><td></td></tr>
<tr><td>⑰ 인증번호</td><td colspan="2"></td><td></td><td></td></tr>
</table>

정보보호제품 국내용 평가·인증을 위한 세부 수행절차에 의거하여 상기와 같이 평가를 신청하며, 기재사항에 허위사실이 없음을 확인합니다.

년 월 일

신 청 인 (서명 또는 인)

<평가기관장> 귀하

(뒷 면)

평가신청서 작성요령

1. 해당하는 빈칸에 ☑ 와 같이 표기한다.
2. 각 항목의 작성요령은 다음과 같다.
   ① 평가신청 형태에 따라 표기를 하고 2인 이상 공동으로 신청할 때는 별지 제2호 서식의 공동신청기관 명부를 추가로 작성한다.
   ② 신청기관의 상호 또는 명칭을 기재한다.(공동신청의 경우에는 대표신청기관 상호 또는 명칭 기재)
   ③ 신청기관이 정보보호제품 제조자, 판매자 및 수입자인지를 구분하여 모든 해당항목에 표기한다.(공동신청의 경우에는 대표신청기관)
   ④ 신청기관의 주된 사업장 주소를 기재한다.(공동신청의 경우에는 대표신청기관)
   ⑤ 신청기관의 이름 및 사업자등록번호를 기재한다.(공동신청의 경우에는 대표신청기관)
   ⑥ 평가신청 업무 담당자의 성명, 부서명, 전화번호 등을 기재한다.
   ⑦ 국내용 제품 평가에 적용되는 평가기준의 버전을 기재한다.
   ⑧ 국내용 제품이 적용한 국가용 보안요구사항 명칭을 기재한다.
   ⑨ 평가신청제품의 명칭(모델명)과 버전번호를 기재한다.
   ⑩ 평가신청 제품의 형태를 기재한다.(예 : 침입차단시스템)
   ⑪ 국내용 제품의 제품번호를 기재한다.
   ⑫ 국내용 제품이 설치 및 운영되는 운영체제(명칭 및 버전번호) 등과 같은 운영환경을 기재한다.
   ⑬ 국내용 제품이 개발된 국가명을 기재한다.
   ⑭ 국내용 제품의 개발자 혹은 개발업체를 기재한다.
   ⑮ 다음의 평가신청 구분에 따라 표기한다.
      - 최초평가 : 처음으로 국내용 제품을 평가신청하는 경우
      - 재 평 가 : 인증제품의 보증에 주요한 영향을 주는 변경이 발생한 경우

⑯ 국내용 제품의 평가신청등급을 기재한다.

⑰ 재평가를 신청하는 경우 이전에 부여받은 인증서 번호를 기재한다.

〔별지 제2호 서식〕

공동신청기관 명부

신청기관	상　호		구　분	□ 제조자 □ 판매자 □ 수입자
	주　소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담 당 자		부 서 명	
			전　화	
			팩　스	
신청기관	상　호		구　분	□ 제조자 □ 판매자 □ 수입자
	주　소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담 당 자		부 서 명	
			전　화	
			팩　스	
신청기관	상　호		구　분	□ 제조자 □ 판매자 □ 수입자
	주　소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담 당 자		부 서 명	
			전　화	
			팩　스	
신청기관	상　호		구　분	□ 제조자 □ 판매자 □ 수입자
	주　소	□□□□□		
	대표자 성명	(인)	사업자등록번호	
	담 당 자		부 서 명	
			전　화	
			팩　스	

〔별지 제3호 서식〕

<접수번호>

평가수행계획서

<평가대상제품명>

년 월 일

<평가기관명>

1. 개요

o 일반적으로 다음의 사항을 포함한다.

- 평가대상제품명, 신청등급, 신청기관, 개발업체, 신청일, 계약일, 신청분류(최초평가/재평가), 검증필 암호모듈 탑재여부(모듈명, 제조사, 검증번호 포함), 국가용 암호알고리즘 적용여부 등
- 기타 추가적으로 포함되어야 할 사항

2. 준수선언

o 일반적으로 다음의 사항을 포함한다.

- 평가기준 식별, 보안요구사항 식별, 패키지 식별 등
- 기타 추가적으로 포함되어야 할 사항

3. 평가범위

o 일반적으로 다음의 사항을 포함한다.

- 보안목표명세서에 명세된 물리적 범위와 논리적 범위를 서술
- 기타 추가적으로 포함되어야 할 사항

4. 평가일정

o 일반적으로 다음의 사항을 포함한다.

- 평가반 구성, 평가 소요기간, 평가 세부 수행계획 등
- 기타 추가적으로 포함되어야 할 사항

5. 신청기관 일반현황

o 일반적으로 다음의 사항을 포함한다.

- 주소, 조직 구성, 주요 사업 등
- 기타 추가적으로 포함되어야 할 사항

〔별지 제4호 서식〕

<접수번호>

관찰보고서

<평가대상제품명>

년 월 일

<평가기관명>

1. 개요

o 일반적으로 다음의 사항을 포함한다.

- 평가신청 개요 : 접수번호, 평가대상제품명, 평가보증등급, 신청기관명 등
- 관찰보고서 개요 : 관찰보고서 식별정보, 보완요청 목록, 회의 일시, 평가자 이름, 신청기관 담당자 이름 등

2. 보완요청

o 보완요청 항목에는 일반적으로 다음의 사항을 포함한다.

- 컴포넌트 식별, 보완내용, 평가에 미치는 영향정도, 보완요청 이행 기관, 보완요청 이행 기한, 보완요청을 이행하지 않은 경우 평가에 미치는 영향 등
- 기타 추가적으로 포함되어야 할 사항

3. 서명

o 일반적으로 다음의 사항을 포함한다.

- 보완요청 사항 요약정보(보완요청 항목 번호, 작업단위, 평가에 미치는 영향정도, 보완요청 이행 기간) 등
- 인증기관, 평가기관, 신청기관의 서명 등

〔별지 제5호 서식〕

<접수번호>

관리 번호	

평가결과보고서

<평가대상제품명>

년 월 일

<평가기관명>

제 1 장 개요

o 일반적으로 다음의 사항을 포함한다.

- 정보보호제품 평가인증 관련 규정(지침, 수행규정 등)
- 평가결과보고서 개요
  · 평가결과보고서, TOE 식별, 보안목표명세서, 보안요구사항(보안규격), CC 버전, 평가보증등급, 신청구분 등 식별정보
- 신청기관명
- 평가기관명(평가자 이름 포함)
- 평가일정(평가신청접수, 평가계약, 제출물설명회, 평가착수, 평가종료)

※ '평가결과보고서 구성' 절 생략 가능

- 참조문서(관련 평가인증지시서, 최종 평가결과물, 최종 평가제출물)

제 2 장 평가대상제품 구조

o TOE 유형, 구성요소 운영환경 및 보안기능

- 제품 유형 개요(2-4 줄 수준)

o TOE 식별 및 구성요소

- 제품 및 구성요소 식별

o TOE 운영환경

- 운영환경
- 하드웨어 및 소프트웨어 요구사항(하부 플랫폼 최소 요구사항)

※ 'TOE 서브시스템 구조', 및 '물리적 범위' 생략 가능

o TOE 보안기능

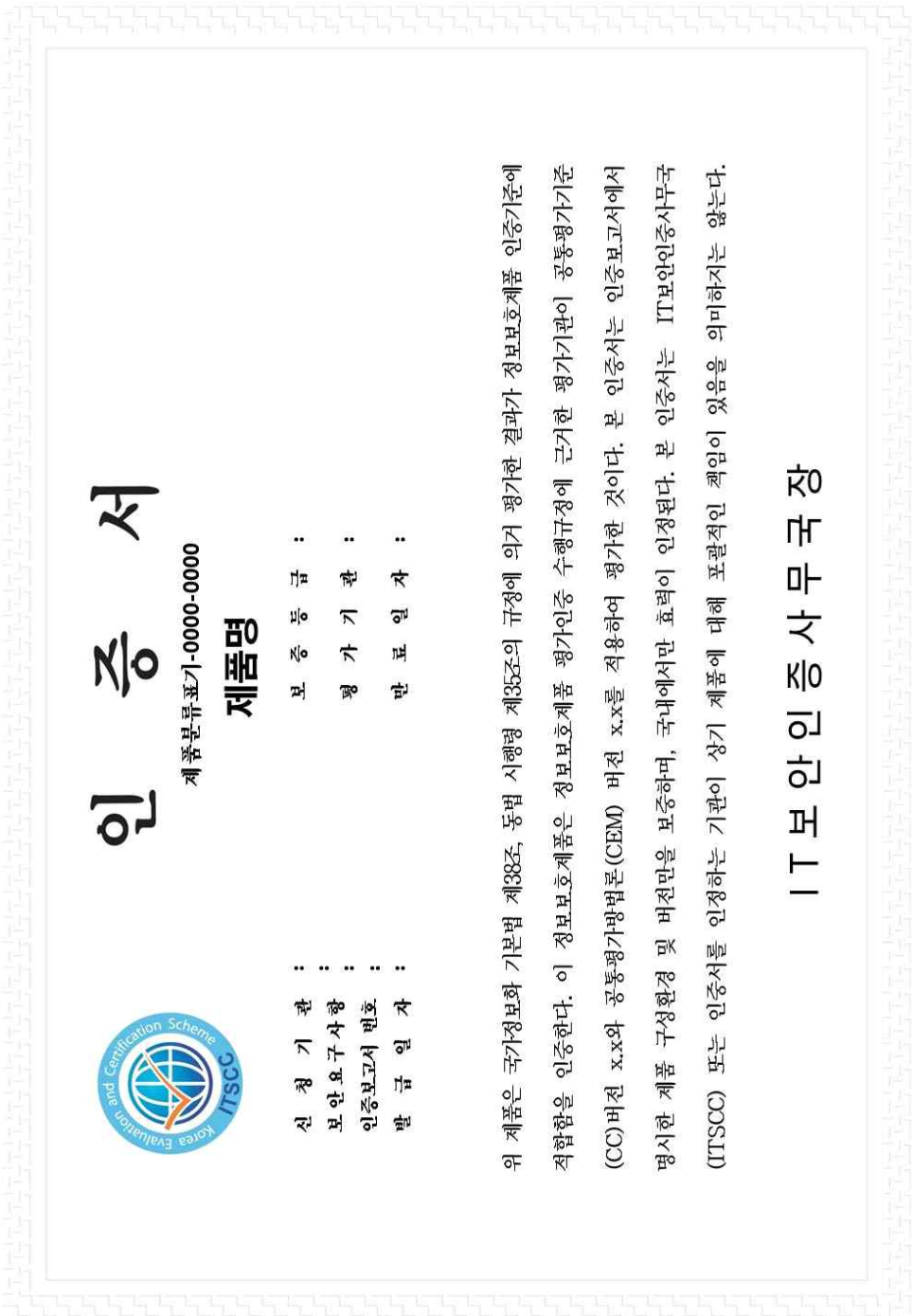
- 주요 보안기능

제 3 장 권고사항 및 특이사항

- 권고사항
- 특이사항 및 기타 추가적으로 포함되어야 할 사항
  (예, 특이사항, 잔여 취약점 등 명시)

[별지 제6호 서식]

정보보호제품 국내용 인증서



인 증 서

제품분류표기-0000-0000

제품명

신 청 기 관 :
보안요구사항 :
인증보고서 번호 :
발 급 일 자 :

보 증 등 급 :
평 가 기 관 :
만 료 일 자 :

위 제품은 국가정보화 기본법 제38조, 동법 시행령 제35조의 규정에 의거 평가한 결과가 정보보호제품 인증기준에 적합함을 인증한다. 이 정보보호제품은 정보보호제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC)버전 x.x와 공통평가방법론(CEM) 버전 x.x를 적용하여 평가한 것이다. 본 인증서는 인증보고서에 명시한 제품 구성환경 및 버전만을 보증하며, 국내에서만 효력이 인정된다. 본 인증서는 IT보안인증사무국(ITSCC) 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

IT보안인증사무국장

〔별지 제7호 서식〕

국내용 인증마크

1. 인증마크 도안

2. 인증번호는 다음과 같다.

   제품군 표기-일련번호-발급년도

3. 제품군 표기는 「정보보호제품 평가·인증 수행규정」별표 5와 같다.

4. 위의 인증마크는 사용자가 확인할 수 있도록 제품 또는 품질보증서 등에 부착하며, 인증기관과 사전협의를 통해 그 사용목적에 따라 동일한 비율로 확대하거나 축소하여 사용할 수 있다.

〔별지 제8호 서식〕

(앞 면)

<table>
<tr><td colspan="3">접수번호
제 호</td><td colspan="2">국내용 인증마크 사용신청서</td><td>처 리 기 간
15일</td></tr>
<tr><td rowspan="4">신청
기관</td><td>①상 호</td><td></td><td>② 구 분</td><td colspan="2">□ 제조자 □ 판매자 □ 수입자</td></tr>
<tr><td>③주 소</td><td colspan="4">□□□□□</td></tr>
<tr><td>④대표자
성명</td><td></td><td>사업자등록번호</td><td colspan="2"></td></tr>
<tr><td>⑤담당자</td><td></td><td>부 서 명</td><td colspan="2">전 화 :
E-Mail :</td></tr>
<tr><td colspan="2">⑥
제 품 분 류</td><td colspan="4"></td></tr>
<tr><td colspan="2">⑦
제 품 명</td><td colspan="4"></td></tr>
<tr><td colspan="2">⑧
운 영 체 제</td><td colspan="4"></td></tr>
<tr><td colspan="2">⑨
인 증 번 호</td><td colspan="4"></td></tr>
<tr><td colspan="2">⑩
평가보증등급</td><td colspan="4"></td></tr>
<tr><td colspan="2">⑪
신 청 수 량</td><td colspan="4"></td></tr>
<tr><td colspan="6">정보보호제품 국내용 평가·인증을 위한 세부 수행절차에 의거하여 상기와 같이 국내용 인증마크 사용을 신청하며, 기재사항에 허위사실이 없음을 확인합니다.

년 월 일

신 청 인 (서명 또는 인)

IT보안인증사무국장 귀하</td></tr>
</table>

(뒷 면)

국내용 인증마크 사용신청서 작성요령

1. 해당하는 빈칸에 ☑ 와 같이 표기한다.
2. 각 항목의 작성요령은 다음과 같다.
   ① 신청기관의 상호 또는 명칭을 기재한다.
   ② 신청기관이 정보보호제품 제조자, 판매자 및 수입자인지를 구분하여 모든 해당항목에 표기한다.
   ③ 신청기관의 주된 사업장 주소를 기재한다.
   ④ 신청기관의 이름 및 사업자등록번호를 기재한다.
   ⑤ 평가신청 업무담당자의 성명, 부서명, 전화번호 등을 기재한다.
   ⑥ 제품분류 또는 대상제품군(네트워크 정보보호제품, 정보보호 기반제품, 컴퓨팅 정보보호제품, 보호프로파일)을 기재한다.
   ⑦ 해당 정보보호제품의 제품명칭(모델명)과 버전번호를 기재한다.
   ⑧ 해당 정보보호제품의 운영체제 명칭과 버전번호를 기재한다.
   ⑨ 교부받은 인증번호를 기재한다.
   ⑩ 부여받은 해당 정보보호제품의 평가보증등급을 기재한다.
   ⑪ 교부받고자 하는 인증마크의 수량을 기재한다.

〔별지 제9호 서식〕

국내용 인증 정보보호제품
정보 공개 동의서

제 품 명 :

본인은 정보보호제품 국내용 평가·인증을 위한 세부 수행절차(제12조 제4항)에 의거, 同 제품 인증보고서에 영업비밀 등 중요자료가 포함되지 않아 인증기관 홈페이지에 공개를 동의합니다.

년 월 일

업체명 : 대표자 성명 : (서명)

IT보안인증사무국장 귀하

〔별지 제10호 서식〕

인증서효력연장 신청서

신청기관	상 호	
	대 표 자	
	담 당 자	전 화 : E-Mail :
인증제품	제 품 명	
	운 영 체 제	
	평가보증등급	
	인 증 번 호	

정보보호제품 국내용 평가·인증을 위한 세부 수행절차에 의거하여 상기와 같이 인증서효력연장을 신청합니다.

년 월 일

신청인 (서명 또는 인)

［별지 제11호 서식］

자체취약성분석서

1. 인증제품 개요

가. 작성자 정보 (인증서보유기관명, 작성일, 작성자 등)

나. 인증제품 (제품명, 버전, 인증일, 평가보증등급 등)

다. 이전 『변경승인』에 관련된 내용 (제품명, 버전, 변경승인일, 변경승인 내용 등)

2. 취약성 점검 내역

가. 최초 평가시 자체 취약성 점검 내역 (점검 항목명, 점검 내용 요약, 점검 결과 등)

나. 추가된 자체 취약성 점검 내역 (점검 항목명, 점검 내용 요약, 점검 결과 등)

다. 테스트 정보 (추가 점검 항목에 대한 시험 절차, 시험도구, Test Case 등)

라. 기타 정보 (취약성 점검 관련 기타 고려사항 명기)