정보보호 및 개인정보보호 관리체계 인증업무지침

제정 2013. 6 . 27.
개정 2013. 9. 1.
개정 2014. 7. 17.
전부개정 2015. 9. 10.
전부개정 2017. 4. 13.
전부개정 2018. 12. 28.
개정 2021. 4. 30.
개정 2022. 12. 23.
개정 2023. 6. 1.
개정 2023. 9. 26.

제1장 총칙

제1조(목적) 이 지침은 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에 따른 정보보호 및 개인정보보호 관리체계 인증 업무를 운영하는데 필요한 사항과 「정보보호 관리등급 부여에 관한 고시」에 따른 정보보호 관리등급 부여 업무 수행에 필요한 사항을 규정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어는 각 호와 같이 정의한다.

1. “신청인”이란 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(이하 “고시”라 한다)」 또는「정보보호 관리등급 부여에 관한 고시」에 따라 인증 또는 등급을 취득하고자 신청한 자를 말한다.
2. “중결함”이란 신청인의 정보보호 및 개인정보보호 관리체계가 인증심사기준에 규정된 요구사항을 충족하지 못하는 사항이 발견되고 발견된 문제점이 정보보호 및 개인정보보호 관리체계 운영에 심각한 영향을 미치는 사항을 말한다.
3. “결함”이란 신청인의 정보보호 및 개인정보보호 관리체계가 인증심사기준에 규정된 요구사항을 충족하지 못하는 사항이 발견되고 있으나 발견된 문제점이 정보보호 및 개인정보보호 관리체계 운영에 심각한 영향을 미치지 않는 사항을 말한다.
4. “인증위원”이란 인증위원회를 구성하는 위원을 말한다.
5. “보궐위원”이란 인증위원회 결원이 생겼을 경우 결원을 보충하기 위해 위촉하는 인증위원을 말한다.
6. “자격검정”이란 인증심사원 자격을 부여하기 위하여 실시하는 일련의 과정으로 서류검토, 필기전형, 실기전형을 포함한다.
7. “시험위원”이란 출제위원, 검증위원, 채점위원 등을 통칭하여 말한다.<개정 2022. 12. 23.>

8. “감독위원”이란 본부감독, 고사장감독, 복도감독 등을 통칭하여 말한다.<신설 2022. 12. 23.>
9. “현장참관”이란 인증기관 소속 직원이 심사현장에 참여하여 직접 심사에 관여하지 않고 인증심사의 절차, 방법, 내용 등의 적절성을 확인하는 과정을 통칭하여 말한다.<신설 2023. 9. 26.>

제2장 인증제도 운영

제3조(협의회 지원) ① 한국인터넷진흥원의 인증업무를 담당하는 부서의 장은 과학기술정보통신부 및 개인정보 보호위원회가 운영하는 정보보호 및 개인정보보호 관리체계 인증 협의회에 간사로 참여한다.

② 한국인터넷진흥원은 인증제도 연구 및 개선에 관한사항, 인증제도 운영을 위한 제반사항 등을 검토하여 정기적으로 협의회 안건으로 상정한다.

제4조(인증·심사기관 관리) ① 한국인터넷진흥원은 심사기관의 사후심사 결과를 확인하여 인증기준에 적합하다고 판단되면 인증유지 공문을 인증을 취득한 자에 발송해야 한다. 이를 위해 심사기관에게 인증심사 결과 자료의 제출을 요구할 수 있다.

② 한국인터넷진흥원은 인증현황관리, 인증심사원 자격관리, 인증위원회 운영 등을 위해 인증·심사기관에게 관련 자료의 제출을 요구할 수 있다.

③ 한국인터넷진흥원은 인증·심사기관 지정기준의 충족 여부 심사, 자료제출 요구 또는 현장심사에 관한 업무를 수행할 수 있다.

제4조의2(인증심사 현장참관) ① 한국인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 경우 현장참관을 시행할 수 있다.

1. 인증을 취득한 자가 정보보호 및 개인정보 관련 침해사고가 발생한 경우
2. 인증심사의 공정성 및 독립성이 훼손될 우려가 있는 경우
3. 그 밖에 한국인터넷진흥원이 현장참관이 필요하다고 판단하는 경우

② 한국인터넷진흥원은 제1항에 따른 현장참관을 시행할 때에는 현장참관 사유, 일시, 내용 등을 구체적으로 명시하여 서면(전자문서를 포함한다)으로 알려야 한다. 이 경우 신청인 및 심사수행기관은 특별한 사유가 없으면 현장참관에 응하여야 한다.

③ 한국인터넷진흥원은 현장참관 시 발견된 문제점을 신청인 및 심사수행기관에 조치할 것을 권고할 수 있다.

[본조 신설 2023. 9. 26.]

제3장 인증심사

제5조(인증심사 신청) ① 신청인은 다음 각 호의 인증을 선택하여 신청할 수 있다.

1. 정보보호 및 개인정보보호 관리체계 인증(이하 “ISMS-P 인증”이라 한다)
2. 정보보호 관리체계 인증(이하 “ISMS 인증”이라 한다)
3. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조에 따른 신고 목적의 예비인증(이하 “ISMS 예비인증”이라 한다)<개정 2022. 12. 23.>

② 인증을 신청하고자 할 경우 다음 각 호의 서류를 한국인터넷진흥원에 제출하여야 한다.

1. 고시 별지 제9호 서식에 따른 인증신청서
2. 별지 제1호 서식의 정보보호 및 개인정보보호 관리체계(ISMS-P) 운영현황(단, 제1항제3호의 경우, 별지 제1-2호 서식의 정보보호 관리체계(ISMS) 예비인증 운영현황)<개정 2022. 12. 23.>
3. 별지 제2호 서식의 정보보호 및 개인정보보호 관리체계 명세서
4. 법인사업자등록증 또는 고유번호증, 법인등기부등본
5. 관련 고시에 따른 수수료 감면 또는 조정 대상인 경우 이를 증빙할 수 있는 서류

③ 한국인터넷진흥원은 신청인이 제출한 서류의 기재사항이 미비하거나 첨부 자료가 누락되었을 경우 신청인에게 보완을 요청할 수 있다.

④ 신청인은 한국인터넷진흥원의 보완요청을 받은 날로부터 10일 이내에 신청서류를 보완하여야 하며, 이를 기한 내에 이행하지 않을 경우 인증심사 신청을 포기한 것으로 본다.

제6조(인증심사 일부 생략 신청) ① 신청인이 ISMS 인증의 일부 생략을 신청하고자 할 경우 추가적으로 다음 각 호의 서류를 한국인터넷진흥원에 제출하여야 한다.

1. ISO/IEC 27001 인증 : 적용성보고서, 범위정의서, 정보보호 조치 결과서, 인증서(인증유지 공문) 등
2. 「정보통신기반 보호법」 제9조에 따른 취약점의 분석·평가 : 주요정보통신기반시설 보호대책서, 조치결과서 등

② 한국인터넷진흥원은 인증심사 일부 생략 대상 및 적절성을 판단하기 위해 추가 증명서류를 요청할 수 있다.

제7조(예비점검) ① 한국인터넷진흥원은 신청인의 심사 준비상태를 서면검토 또는 현장 방문하여 확인할 수 있다.

② 한국인터넷진흥원은 신청인의 준비가 미흡하여 인증심사를 진행할 수 없는 경우 이에 대한 보완조치를 요청하고 인증심사를 연기할 수 있다.

제8조(인증 수수료) ① 인증 수수료는 다음 각 호의 비용을 포함한다.<개정 2022. 12. 23.>

1. 인증심사계획 송부, 예비점검, 인증심사, 이행점검, 인증위원회 개최, 인증서 발급 및 관리에 소요되는 비용<개정 2022. 00. 00.>
2. 교통비, 숙박비, 일비, 식비 등 인증심사 업무에 소요되는 직접적인 비용<개정 2022. 12. 23.>

② 신청인이 규정에 따라 수수료를 납부하지 않은 경우 한국인터넷진흥원은 인증절차를 중지할 수 있다.

③ 한국인터넷진흥원은 신청인이 다음 각 호에 해당하는 경우 인증수수료를 경감할 수 있다.

1. 「중소기업기본법」에 따른 소기업
2. 고시 제20조에 따라 인증심사의 일부 생략을 신청한 경우
3. 「정보보호산업의 진흥에 관한 법률」 제13조제1항에 따라 정보보호 공시제도를 이행하는 경우 <개정 2022. 12. 23.>
4. 그 밖에 한국인터넷진흥원장이 수수료 경감의 필요성이 있다고 인정하는 경우

제9조(인증심사팀 구성) ① 인증심사팀은 한국인터넷진흥원에 소속된 심사팀장과 인증심사원으로 구성한다.
② 인증심사팀 구성 시 다음 각 호 해당하는 인증심사원은 제외하여야 한다.
1. 신청인에 소속(근무)되어 있거나 과거 3년 동안 소속된 경력이 있는 자
2. 신청인의 보안컨설팅, 위탁업무 등 관련 업무를 과거 3년 동안 수행한 경력이 있는 자
3. 그 밖에 신청인과 이해관계가 있는 자

제10조(인증심사팀의 역할) ① 심사팀장은 다음 각 호에 해당하는 역할을 수행하여야 한다.
1. 인증심사 계획 수립, 심사 총괄 및 결과보고
2. 인증심사원(심사팀원) 심사업무 분장
3. 인증심사 결함사항에 대한 보완조치 확인
4. 인증심사 활동에 대한 인증심사원(심사팀원) 평가
5. 인증심사 결과보고서 작성
6. 인증위원회 개최 시 인증위원회 인증심사 결과보고
7. 신청인의 정보보호 사고 시, 사고 관련 현황 파악 및 사고 보고서 작성
② 심사팀원은 다음 각 호에 해당하는 역할을 수행하여야 한다.
1. 할당된 심사업무에 대한 심사계획 수립 및 심사 수행
2. 인증심사 결함보고서 작성 및 제출
3. 심사팀장 지원 및 협력

제11조(인증심사원 자문비 및 출장비) ① 한국인터넷진흥원은 인증심사원에게 [별표 1] 인증심사원 자문비 지급 기준에 따라 자문비를 지급한다.
② 인증심사원이 국내에서 인증심사 업무를 수행하는 경우 고시 별표 6에 따라 교통비, 식비, 일비, 숙박비에 대하여 정액여비로 지급하고, 그 금액은 [별표 3]을 참고하여 지급한다. 단, 국외에서 인증심사 업무를 수행하는 경우 한국인터넷진흥원「출장규칙」 별표 제2호를 참고하여 지급한다. <개정 2022. 12. 23.>

제12조(인증심사) ① 인증심사원은 임의로 취약점 점검을 수행할 수 없으며 심사팀장과 협의하여 취약점 점검이 필요하다고 판단되는 경우 신청인과 사전협의를 거쳐 수행할 수 있다.
② 인증심사팀은 인증심사를 통하여 인증심사기준에 부적합한 사항을 발견한 경우 별지 제3호 서식 결함보고서를 작성한다.

③ 한국인터넷진흥원은 결함보고서에 기술한 결함에 대해 별지 제4호 서식 보완조치 요청서를 작성하여 신청인에게 보완조치를 요청한다.

제13조(인증심사 중단) ① 한국인터넷진흥원은 다음 각 호의 사유가 발생한 경우에는 인증심사를 중단할 수 있다.

1. 신청인이 고의로 인증심사업무를 지연 또는 방해하는 등 신청인의 귀책사유로 인하여 인증심사를 계속 진행하기가 곤란하다고 인정되는 경우
2. 신청인이 의무대상 기준의 인증범위를 누락하여 인증심사를 진행하기가 곤란한 경우
3. 사후심사 또는 갱신심사 중 이전 심사 대비 인증범위에 큰 영향을 주는 변경사항이 발견되어 인증범위를 재설정해야 하는 경우
4. 천재지변 및 경영환경 변화 등으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우
5. 인증신청, 서면 및 현장심사, 보완조치 등 일련의 인증심사과정 중에 인증제도의 신뢰성을 훼손할 수 있는 사회적 물의를 일으키거나 중대한 정보보호 침해사고 및 개인정보 유출사고가 발생한 경우
6. 신청인의 보완조치가 완료되지 않을 경우

② 인증심사가 중단된 경우 신청인은 별지 제5호 서식 인증심사 중단 확인서를 작성하여 한국인터넷진흥원에 제출하여야 한다.

제14조(보완조치) ① 신청인은 보완조치 요청을 받은 날로부터 40일 이내에 보완조치를 수행하고 별지 제6호 서식 보완조치 내역서를 작성하여 보완조치 완료 공문과 함께 한국인터넷진흥원에 제출하여야 한다.

② 40일 이내에 보완조치가 완료되지 않은 경우 신청인은 보완조치가 완료된 결함사항은 보완조치 내역서, 보완조치가 완료되지 않은 결함사항은 별지 제7호 서식 보완조치 요약서를 작성하여 보완조치 연장 공문과 함께 한국인터넷진흥원에 제출하여야 한다. 이 경우, 심사팀장은 보완조치 연장 사유가 타당하다고 판단한 경우 추가 60일의 보완조치 기간을 부여할 수 있으며 60일 이내에 보완조치가 완료되어야 한다.

③ 심사팀장은 신청인이 제출한 보완조치 내역에 대하여 현장 확인이 필요하다고 판단될 경우 현장을 방문하여 결과를 확인할 수 있다.

④ 제1항과 제2항의 보완조치 완료라 함은 신청인이 ISMS 인증의 경우 정보보호최고책임자, ISMS-P 인증의 경우 정보보호최고책임자 및 개인정보보호책임자, 심사팀장의 서명을 포함한 보완조치 완료확인서(별지 제8호 서식)의 제출이 완료된 것을 말한다.

제15조(결과보고) 심사팀장은 결함에 대한 보완조치 내역을 확인하고 이에 대한 인증심사 결과보고서를 작성하여 심사종료일 다음날부터 산정하여 130일 이내 한국인터넷진흥원에 제출하여야 한다.

제16조(사후관리) ① 인증을 취득한 자는 인증서 부여일로부터 매 1년이 되는 시점까지 사후심사를 완료하여야 하며 특별한 사유가 없는 경우 이전심사로부터 6개월 이후 시점부터 받을 수 있다.

사후심사 이후 인증유지 여부가 결정되기 전까지는 인증이 유지되는 것으로 인정한다.
② 인증을 취득한 자가 유효기간 연장을 위해서는 유효기간 만료일 3개월 이전에 인증심사를 신청하고 유효기간 이전까지 갱신심사를 완료하여야 한다. 이때 유효기간 만료일 이후부터 인증위원회 통과 전까지는 인증이 유효하지 않은 것으로 본다.
③ 인증을 취득한 자에 중대한 정보보호 침해사고가 발생하거나 관리체계 운영에 심각한 문제가 있어서, 한국인터넷진흥원이 필요하다고 판단하는 경우 정기적 사후심사 이외 별도의 사후심사를 할 수 있다.

제17조(인증서 관리) 한국인터넷진흥원은 발급한 인증서의 인증번호, 인증범위, 유효기간 등을 관리하고 홈페이지에 게시한다.

제18조(인증심사 세부사항) 인증심사에 대한 세부사항은 인증심사업무 매뉴얼에서 규정한다.

제4장 인증심사원 관리

제19조(자격 취득 절차) ① 인증심사원 자격을 취득하려는 자는 한국인터넷진흥원이 시행하는 인증심사원 자격검정을 통과하여야 한다.
② 인증심사원 자격검정은 서류검토, 필기전형, 실기전형 순으로 실시하고 앞 순서의 과정을 통과하지 못한 자는 다음 순서의 전형에 참여할 수 없다.

제19조의2(자격검정 문제출제 및 관리) ① 한국인터넷진흥원은 필기전형 및 실기전형을 위해 시험위원 및 감독위원을 위촉할 수 있다. 단, 시험위원은 인증심사원 자격을 보유하여야 한다.
② 시험문제는 자격검정 시행 시마다 한국인터넷진흥원이 지정한 장소에서 내부직원의 관리에 따라 시험위원이 출제, 선정, 검증하는 것을 원칙으로 한다.
③ 필기전형 및 실기전형에 사용된 시험문제지는 일괄 회수하여 조속한 시일 내에 파기하여야 한다. 단, 시험문제는 1년간, 답안지 등 채점관련 자료는 최종합격자 발표일로부터 최대 2년간 보관한다. <신설 2022. 12. 23.>

제20조(자격 응시 요건) ① 자격검정 신청자는 고시 별표 4의 요건을 갖추어야 응시가 가능하다.
② 자격검정 응시자는 신청일 기준 인증심사원 자격 신청 요건을 충족하여야 한다.
③ 인증심사원 자격을 기보유한 자는 인증심사원 자격에 응시할 수 없다.

제21조(원서접수 및 서류검토) ① 자격검정 응시자는 자격신청서와 관련 서류를 구비하여 한국인터넷진흥원에 제출하여야 한다.
② 한국인터넷진흥원은 자격 응시자의 신청서류를 검토하고, 제33조에 따른 자격심의 위원회를 통해

자격요건을 충족하는지 확인하여야 한다.<개정 2023. 6. 1.>
③ 서류검토 결과 자격요건을 충족하는 경우에만 필기전형 응시가 가능하다.

제22조(필기전형) ① 한국인터넷진흥원은 필기전형 접수기간을 사전에 공지하여야 한다.
② 필기전형 결과는 해당 연도와 다음 연도까지 유효하다.
③ <삭제 2022. 12. 23.>
④ 시험위원은 업무 수행과정에서 취득한 사실에 대한 비밀을 유출 또는 공개하지 아니한다.
⑤ 필기시험의 문제 및 정답은 공개하지 않는 것을 원칙으로 한다.

제23조(실기전형) ① 실기전형은 실무교육과 평가시험으로 구성된다. 단, 필요한 경우 실무교육은 원격으로 실시할 수 있다.
② 실기전형은 해당 연도와 직전연도 필기전형 합격자만 응시 가능하다.
③ 한국인터넷진흥원은 시험위원이 답안지의 응시자 인적사항을 알 수 없도록 조치하여야 하며 시험위원은 세부항목별 채점기준 및 배점에 따라 채점하여야 한다.
④ 평가시험의 문제 및 정답은 공개하지 않는 것을 원칙으로 한다.

제24조(최종합격자 발표) 한국인터넷진흥원은 실무교육과 평가시험의 결과에 따라 최종합격자를 선정하고 그 결과를 개별 통지한다.

제25조(부정행위자에 대한 조치) 한국인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 자에 대하여 자격검정을 무효처리하며, 해당 응시자는 그 처분이 있는 날부터 3년간 인증심사원 자격검정에 응시할 수 없다.
1. 자격검정 신청서류 및 관련 증빙자료를 허위로 제출한 경우
2. 수험표 등에 문제 또는 정답을 옮겨 적는 행위를 한 경우
3. 시험 또는 실무교육과정에서 녹취 또는 촬영(동영상, 사진 포함)하는 경우
4. 필기 또는 실기 시험 내용의 일부 또는 전부를 누설·유출한 경우
5. 본인이 아닌 자가 시험 응시 또는 교육을 받은 경우
6. 그 밖에 부정한 행위를 한 경우로서 검정과정을 무효화하는 것이 타당하다고 인정되는 경우

제26조(자격검정 회계규정) 한국인터넷진흥원은 외부 시험위원 및 감독위원에게 [별표 2]에 따라 대가를 지급하고, 내부 직원이 감독위원으로 참여할 경우 [별표 2]를 준용하여 대가를 지급할 수 있다. <개정 2022. 12. 23.>

제27조(인증심사원 자격증 발급 및 관리) ① 한국인터넷진흥원은 인증심사원 자격 검정을 최종 합격한 응시자에게 인증심사원 자격증을 발급한다.
② 한국인터넷진흥원은 인증심사원의 자격 증명서 발급, 등급변경 사실과 인증심사 업무경력 등을 기록하여 관리하여야 한다.

③ 한국인터넷진흥원은 인증심사원이 심사경력 확인을 요청하는 경우 인증심사 경력 확인서를 발급할 수 있다.

제28조(인증심사원 등급) ① 인증심사원은 고시 별표 3의 요건에 따라 심사원보, 심사원, 선임심사원으로 구분한다.

② 인터넷진흥원은 매년 1월 1일 기준으로 전년도 1년 동안 다음의 요건을 모두 만족하는 경우 책임심사원으로 임명할 수 있다.

1. 전년도 1년 동안 심사원 등급으로서 인증심사에 4회 이상 참여하고 심사일수의 합이 20일 이상
2. 전년도 1년 동안 최초 또는 갱신심사 1회 이상 참여
3. 전년도 1년 동안 정보보호 및 개인정보보호 관리체계 인증심사 2회 이상 참여
4. 전년도 1년 동안 인증심사 수행 결과에 대한 적격성 평가 충족

③ 책임심사원은 1년 동안 임시적으로 활동하는 등급으로 별지 제9호 서식 책임심사원 확인서를 발급하며 자격증 등에 공식적인 등급으로 표시할 수 없다.

④ 인증심사원 자격을 갱신하지 않고 유효기간이 만료되면, 책임심사원 등급도 함께 종료된다.

제29조(인증심사원 자격유지) ① 인증심사원은 자격유지를 위해 자격 유효기간 만료 전까지 한국인터넷진흥원이 인정하는 보수교육을 42시간 이상 수료하고 평가시험에 응시하여야 한다.<개정 2022. 12. 23.>

② 보수교육은 필수교육 1일(7시간)과 선택교육(심사대체과정) 5일(35시간)으로 나누어 운영하며 자격 유효기간 내 인증심사 1일 참여시마다 선택교육 5시간을 이수한 것으로 인정한다.

③ 한국인터넷진흥원은 보수교육 운영에 관한 변경이 있을 경우 보수교육 운영 세부내용을 인증정보를 제공하는 홈페이지에 공지하여야 한다.

④ 한국인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 고시 별지 제8호서식의 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.

⑤ 제1항에도 불구하고 인증심사원은 자격 유효기간 만료 전까지 평가시험에 통과하여야 한다. 단, 평가시험에 통과하지 못하여도 자격은 유지되지만 인증심사는 참여할 수 없다. <신설 2022. 12. 23.>

제30조(인증심사원 적격성 평가) ① 인증심사 팀장과 심사원은 심사종료 후 심사에 참여한 인증심사팀에 대해 별지 제10호 서식에 따라 다면 평가서를 작성하여 한국인터넷진흥원에 제출하여야 한다. <개정 2022. 12. 23.>

② 한국인터넷진흥원은 책임심사원 선정을 위해 매년 12월에서 1월 사이에 인증심사원 적격성 평가를 실시한다.

③ 제2항의 적격성 평가는 다면 평가서, 심사결과보고서, 심사일지, 신청기관 담당자 등의 의견을 수렴하여 종합적으로 결정한다. <개정 2022. 12. 23.>

제31조(인증심사원 자격정지 및 취소) ① 인증심사원의 자격정지 또는 취소의 사유가 발생한 경우 자격정지 또는 취소여부를 인증심사원 자격 심의를 거쳐 결정한 후 해당 인증심사원에게 통보하여야 한다.

② 한국인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우 인증심사원의 자격을 정지할 수 있다.

1. 신청인의 소속직원으로 근무 또는 신청인에 자문·기술지원 등을 제공 후 3년 이내에 신청인

의 인증심사원으로 참여한 경우
2. 사실을 은폐하거나 허위로 보고서를 작성한 경우
3. 인증심사원이 인증심사 업무와 관련하여 고의 또는 중대한 과실로 손해를 끼치는 경우
4. 그 밖에 인증심사 업무를 성실히 수행하지 않거나 품위를 손상시켜 공익을 해한 경우

③ 한국인터넷진흥원은 고시 제16조제1항에 해당하는 사유를 발견한 경우 인증심사원의 자격을 취소할 수 있다.

④ 제2항에 따라 인증심사원 자격정지기간은 3년의 범위 내에서 한국인터넷진흥원장이 정한다.

⑤ 제3항에 따라 인증심사원 자격이 취소된 자는 자격이 취소된 날부터 3년 이내에는 인증심사원의 자격을 취득할 수 없다.

제32조(인증심사원의 의무) ① 인증심사원은 다음 각 호의 의무 사항을 준수하여야 한다.
1. 인증심사원은 객관적이고 공정한 인증심사를 수행한다.
2. 인증심사원으로서 성실한 직무수행 및 품위유지를 한다.
3. 인증심사와 관련된 부당한 금전, 금품 등의 수수를 금지한다.
4. 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청인의 동의 없이 외부에 누설하여서는 아니 된다.
5. 인증심사 수행 부적합 조건에 해당하면서 인증심사에 참여해서는 아니 된다.
6. 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력으로부터 배제되어야 한다.

② 인증심사원은 인증심사 참여 시 별지 제11호 서식의 업무 수행 행동 강령과 별지 제12호 서식의 보안서약서에 서명하여야 한다.

제33조(인증심사원 자격심의 위원회) 한국인터넷진흥원은 인증심사원의 자격의 검증, 정지, 취소 및 등급의 변경을 심의하기 위하여 3명 이상의 인증위원을 포함한 자격심의위원회를 구성하여 운영할 수 있다.

제34조(인증심사원 자격관리 세부사항) 인증심사원 자격관리에 대한 세부사항은 인증심사원 자격관리 매뉴얼에서 규정한다.

제5장 인증위원회 운영

제35조(인증위원회 구성) ① 인증위원은 정보보호 또는 개인정보보호 분야에 학식과 경험이 있는 전문가를 대상으로 35명 이하의 인원으로 구성한다.<개정 2023. 6. 1.>

② 한국인터넷진흥원장은 인증위원 위촉 시 별지 제13호 서식 인증위원 위촉장을 수여한다.

③ 인증위원회는 위원장, 위원, 간사를 두며 간사는 인증제도 담당 사업팀장이 담당한다.

제36조(인증위원 의무) 인증위원은 다음 각 호의 윤리 및 보안 의무를 준수하여야 한다.
1. 인증위원은 객관적이고 공정하게 인증심사 결과를 심의하고, 인증부여를 의결한다.

2. 인증위원은 성실한 직무수행 및 품위를 유지한다.
3. 인증위원은 인증 심의와 관련하여 부당한 금전, 금품 등을 수수하지 않는다.
4. 인증위원은 인증 심의과정에서 취득한 정보를 외부에 누설하지 않는다.
5. 인증위원은 인증 심의와 관련하여 상업적, 재정적 등 기타 모든 압력을 배제하여야 한다.
6. 인증위원은 위원회에 불참하는 사례가 없도록 최선의 노력을 하여야 한다.
7. 인증위원은 상기 사항 준수에 대해 별지 제14호 서식 인증위원 윤리 서약서 및 별지 제15호 서식 인증위원 정보보호 서약서를 작성하여 한국인터넷진흥원에 제출한다.

제37조(보궐위원 위촉 및 위촉 취소) ① 다음 각 호의 이유로 인증위원에 결원이 생겼을 때에는 보궐위원을 위촉할 수 있다.
1. 인증위원회 활동과정에서 금품수수, 이해관계인으로부터 청탁, 부당한 영향력을 행사한 위원이 그 사실이 확인되어 위촉이 취소된 경우
2. 인증위원의 사임, 퇴직, 이직, 해임, 업무 변경 등의 사유로 위촉이 취소된 경우

② 한국인터넷진흥원은 인증위원이 연속 3회 이상 특별한 사유 없이 위원회에 불참한 경우 위촉을 취소할 수 있다.

제38조(인증위원 임기) ① 인증위원의 임기는 3년으로 하고 재구성을 통해 연임할 수 있다.
② 보궐위원의 임기는 전임자의 잔여기간으로 한다.

제39조(인증위원회 개최) ① 한국인터넷진흥원은 인증심사팀의 인증심사결과 심의·의결 요구 또는 인증위원회 개최가 필요하다고 인정되는 경우 인증위원회를 개최한다.

② 한국인터넷진흥원은 인증위원회를 소집하고자 할 경우 일시, 장소, 안건 및 기타 관련사항을 회의 소집 5일전까지 각 위원에게 통보한다. 다만, 긴급한 사유 등으로 인해 인증위원회를 개최할 수 없거나 의결 안건이 경미하다고 판단할 경우 인증위원회는 서면 또는 원격으로 심의·의결할 수 있다.

제40조(인증위원회 개최·의결 정족수) ① 인증위원회는 위원장 1명과 전문분야를 고려한 6명 이상의 인증위원으로 구성된다. 단, 위원장이 부득이한 사유로 직무를 수행할 수 없을 경우 사전에 지명한 위원이 위원장의 직무를 대행한다.

② 출석한 인증위원의 2/3 이상 심의안건에 대해 찬성으로 가결한다.

③ 인증위원회 심의·의결 결과 가부동수인 경우에는 위원장이 결정한다.

제41조(제척·기피·회피) ① 다음 각 호에 해당하는 인증위원은 심의·의결에서 제척한다.
1. 신청인과 직접적인 이해관계가 있는 경우
2. 신청인의 전·현직 임직원과 친족 관계인 경우
3. 신청인과 법률상 특수 관계 등으로 직접적인 이해관계가 있는 경우
4. 인증위원이 되기 전에 감사·수사 또는 조사에 관여한 경우

② 직접적인 이해관계 등으로 공정한 심의·의결을 기대하기 어려운 경우 해당 인증위원을 위원장에게 기피신청 할 수 있다.
③ 인증위원은 제척사유 또는 기피사유에 해당하는 경우 자기 스스로 그 사항의 심의·의결을 회피할 수 있다.

제42조(인증위원의 역할) 인증위원은 다음 각 호의 역할을 수행한다.
1. 최초 및 갱신 인증심사결과 심의·의결
2. 인증 취소 상정 건에 대한 심의·의결
3. 기타 인증위원회의 심의·의결이 필요한 사항

제43조(인증위원회 세부사항) 인증위원회 운영에 대한 세부사항은 인증위원회 운영 매뉴얼에서 규정한다.

제6장 정보보호 관리등급 운영

제44조(정보보호 관리등급) 정보보호 관리체계 인증을 취득한 자는 정보보호 관리등급을 신청할 수 있다.

제45조(정보보호 관리등급 부여 세부사항) 정보보호 관리등급 부여에 관한 세부사항은 정보보호 관리등급 운영 매뉴얼에서 규정한다.

제7장 기타 사항

제46조(매뉴얼 제·개정) ① 한국인터넷진흥원의 관리체계 인증업무를 수행하는 부서에서는 인증업무 수행을 위해 필요한 매뉴얼을 마련하여 시행할 수 있다.
② 각 매뉴얼에 대한 제·개정은 한국인터넷진흥원의 관리체계 인증업무를 수행하는 부서의 장이 승인한다.
③ 각 매뉴얼은 승인일로부터 효력이 발생하며, 필요시 관리체계 인증업무를 수행하는 부서의 장이 효력 발생일을 지정하여 시행할 수 있다.

부 칙<2018. 12. 28.>

제1조(시행일) 이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.
제2조(적용례) 제35조에 따른 인증위원회는 2019년 8월부터 적용한다.
제3조(타 지침의 폐지) 정보보호 관리체계 및 개인정보보호 관리체계 인증업무 지침은 폐지한다.

부 칙<2021. 4. 30.>

제1조(시행일) 이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2022. 12. 23.>

제1조(시행일) 이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2023. 6. 1.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2023. 9. 26.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

[별표 1] 인증심사원 자문비 지급 기준

1. 인증심사원에 대한 보수는 고시 별표 6에 따라 2018년 소프트웨어기술자의 일일 평균임금을 참고하여 다음과 같이 적용한다.

인증심사원 등급	1일 자문료
심사원보	200,000원
심사원	300,000원
선임심사원	350,000원
책임심사원	450,000원

2. 인증심사원이 한국인터넷진흥원, 인증기관, 심사기관의 직원 또는 관계부처 공무원인 경우에는 별도의 심사비를 지급하지 않는다.

3. 인증심사원 중 공무원인 경우에는「예산 및 기금운용계획 집행지침」의 '위원회 참석비'를 따른다.

[별표 2] 시험위원 및 감독위원 대가 지급기준 <개정 2022. 12. 23.>

구분		지급 상한액	비고
시험위원	출제위원	300,000원	· 1인 문제출제회의 참여 1회당 기준 임 · ISMS-P 인증심사원 중 심사원 등급 이상으로 위촉함
	검증위원	400,000원	1인 문제검증회의 참여 1회당 기준 임
	채점위원	400,000원	1인 문제채점회의 참여 1회당 기준 임
감독위원		150,000원	1인 시험과목당 기준 임

※ 단, 내부직원이 휴무일에 감독위원으로 참여 시, 상기 지급기준에 준하여 비용 지급 가능(이 경우, 초과근무수당 신청은 불가)

[별표 3] 직접경비 청구 기준 <개정 2023. 6. 1.>

1. 인증심사원에 대한 직접경비는「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」별표 6에 따라 다음과 같이 적용한다.

기준점	구분	청구 기준(정액)			
		교통비	숙박비	일비	식비
광화문을 공통기준으로 정함 ※ 도로원표(도로법 시행령 제50조 2항)	근무지 내	-	-	20,000원	-
	근무지 외	왕복 KTX 기준	55,000원	25,000원	25,000원

※ 심사수행기관이 서울에 집중되어 있어 서울의 중심인 광화문(도로원표)을 공통 기준으로 정함

2. 구분의 근무지 내는 서울특별시와 한국인터넷진흥원이 정하여 홈페이지에 공지하는 지역을 말한다.

3. 인증심사원이 한국인터넷진흥원 직원인 경우, 한국인터넷진흥원「출장규칙」을 따른다.

[별지 제1호 서식] 정보보호 및 개인정보보호 관리체계(ISMS-P) 운영현황

아래는 정보보호 및 개인정보보호 관리체계(**ISMS, ISMS-P**) 인증 신청 기업·기관을 대상으로 운영현황과 제도개선 사항을 파악하고자 질문으로 구성하였으니 답변하여 주시기 바랍니다.

1. 귀 사(기관)에서 운영하는 전체 서비스 관련 회원 및 일일 평균 이용자수에 대해 각각 기입해 주십시오.

(B2B 포함)

회원 수(명)		일일 평균 이용자수(명)	

2. 귀 사(기관)의 정보보호 및 개인정보보호 조직 운영방식은 무엇입니까? ( )

1) 전담조직[1] 2) 겸임조직 3) 기타방식 (※ 간단히 내용 작성)

3. 귀 사(기관)의 정보보호 및 개인정보보호 등을 포함한 인력 규모는 어느 정도입니까?

(단위 : 명)

회사內 전체 인력	IT 인력	정보보호 전담인력	개인정보보호 전담인력

4. 귀 사(기관)는 최근 1년 이내에 정보보호 또는 개인정보보호 인력을 신규 채용하였습니까?

1) 아니오 2) 예 (명)

5. 귀 사(기관)의 정보보호 및 개인정보보호 예산 규모는 어느 정도입니까?

(단위 : %)

전체예산 대비 IT 예산	IT 예산 대비 정보보호 예산	IT 예산 대비 개인정보보호 예산

6. 귀 사(기관)가 정보보호 관련 인증, 점검, 평가를 수행하기 위해 1년 동안 전체 소요되는 총 인력 및 기간은 어느 정도입니까?

소요 인력(명)		소요 기간(일)	

7. 귀 사(기관)는 관리체계(ISMS, ISMS-P) 구축 시, 인력구성은 어떻게 되었나요?

1) 자체 인력만 2) 외부 인력만 3) 자체 인력과 외부 인력

---

1) **정보보호 전담조직** : 정보보호(개인정보보호 포함) 관련 업무만을 수행하는 조직(인력)
※ 타 업무를 수행하며 정보보호 관련 업무를 겸직하는 경우는 제외

8. 귀 사(기관)가 관리체계(ISMS, ISMS-P) 구축·운영을 위해 소요된 비용은 어느 정도입니까?

1) 외부 컨설팅 비용 (※ 해당 범위에 V표시)

해당 없음	~ 3천만 원 미만	3천만 원 이상 ~ 5천만 원 미만	5천만 원 이상 ~ 1억 원 미만	1억 원 이상 ~ 2억 원 미만	2억 원 이상

2) 정보시스템 또는 정보보호시스템 구매 비용(H/W, S/W) : (약 백만 원)

9. 귀 사(기관)는 홈페이지 등을 통해 정보보호 활동 내역 공개하고 있습니까? (O, X **)**

10. ISMS, ISMS-P, 기존 인증(ISMS, PIMS) 이외에 귀 사(기관)에서 받았거나 유지하고 있는 타 인증・점검・평가는 무엇입니까?

1) 개인정보보호 수준진단 2) 개인정보 영향평가 3) ISO27001 4) 주요 정보통신 기반시설 대상

5) 기타 (, ,)

11. ISMS, ISMS-P 인증을 취득 또는 준비하면서 가장 크게 개선된 사항은 무엇입니까? (1, 3, **)**

1) 정보보호 관련 계획 추진 및 예산 확보가 쉬워짐
2) 정보보호에 대한 경영진의 이해가 높아짐
3) 정보보호 전담하는 조직이 새로 구성됨
4) 기관 직원들의 정보보호 관련 인식이 확대됨
5) 침해사고에 대한 위험도가 낮아짐
6) 정보보호 우수기업 마케팅 활용에 따른 고객의 신뢰성이 높아짐
7) 기타 (※ 간단히 내용 작성)

12. 귀 사(기관)가 ISMS, ISMS-P 인증을 도입하면서 기대하는 효과는 무엇입니까? (1, 3, **)**

1) 정보통신망법에 따른 의무 요건 충족
2) 사내 정보보호 수준 강화
3) 정보보호 조직의 역할과 권한 확대
4) ISMS 인증 취득으로 인한 고객 신뢰성 확보
5) 기타 (※ 간단히 내용 작성)

13. ISMS, ISMS-P 인증제도와 관련하여 의견

[별지 제1-2호 서식] 정보보호 및 개인정보보호 관리체계(ISMS-P) 예비인증 운영현황 <개정 2022. 12. 23.>

아래는 정보보호 관리체계(**ISMS**) 예비인증 신청 기업·기관을 대상으로 운영현황과 제도개선 사항을 파악하고자 질문으로 구성하였으니 답변하여 주시기 바랍니다.

1. 귀 사(기관)에서 ISMS 예비인증을 신청하는 인증범위의 가상자산 서비스 업무를 선택해 주십시오.

구분	선택(O)
1) 가상자산을 매도, 매수하는 행위	
2) 가상자산을 다른 가상자산과 교환하는 행위	
3) 가상자산을 이전하는 행위 중 대통령령으로 정하는 행위	
4) 가상자산을 보관 또는 관리하는 행위	
5) 1) 및 2)의 행위를 중개, 알선하거나 대행하는 행위	
6) 그 밖에 가상자산과 관련하여 자금세탁행위와 공중협박자금조달행위에 이용될 가능성이 높은 것으로서 대통령령으로 정하는 행위	

※ 특정 금융거래정보의 보고 및 이용 등에 관한 법률 제2조제1호하목 중 선택하되 복수 기재 가능

2. 귀 사(기관)에서 운영하는 전체 서비스 관련 회원 및 일일 평균 이용자수에 대해 각각 기입해 주십시오. (B2B 포함)

회원수(명)		일일 평균 이용자수(명)	

3. 귀 사(기관)의 정보보호 및 개인정보보호 조직 운영방식은 무엇입니까? ( )

1) 전담조직[2] 2) 겸임조직 3) 기타방식 (※ 간단히 내용 작성)

4. 귀 사(기관)의 정보보호 및 개인정보보호 등을 포함한 인력 규모는 어느 정도입니까?

(단위 : 명)

회사內 전체 인력	IT 인력	정보보호 전담인력	개인정보보호 전담인력

5. 귀 사(기관)는 최근 1년 이내에 정보보호 또는 개인정보보호 인력을 신규 채용하였습니까?

1) 아니오 2) 예 (명)

6. 귀 사(기관)의 정보보호 및 개인정보보호 예산 규모는 어느 정도입니까?

(단위 : %)

전체예산 대비 IT 예산	IT예산 대비 정보보호 예산	IT예산 대비 개인정보보호 예산

2) **정보보호 전담조직** : 정보보호(개인정보보호 포함) 관련 업무만을 수행하는 조직(인력)
※ 타 업무를 수행하며 정보보호 관련 업무를 겸직하는 경우는 제외

7. 귀 사(기관)가 정보보호 관련 인증, 점검, 평가를 수행하기 위해 1년 동안 전체 소요되는 총 인력 및 기간은 어느 정도입니까?

소요 인력(명)		소요 기간(일)	

8. 귀 사(기관)는 정보보호 관리체계(ISMS) 예비인증 구축 시, 인력구성을 어떻게 하였습니까?

1) 자체 인력만 2) 외부 인력만 3) 자체 인력과 외부 인력

9. 귀 사(기관)가 정보보호 관리체계(ISMS) 예비인증 구축·운영을 위해 소요한 비용은 어느 정도입니까?

1) 외부 컨설팅 비용 (※ 해당 범위에 V표시)

해당없음	~ 3천만원 미만	3천만원 이상 ~ 5천만원 미만	5천만원 이상 ~ 1억원 미만	1억원 이상 ~ 2억원 미만	2억원 이상

2) 정보시스템 또는 정보보호시스템 구매 비용(H/W, S/W) : (약 백만원)

10. 귀 사(기관)는 홈페이지 등을 통해 정보보호 활동 내역 공개하고 있습니까? (O, X)

11. 정보보호 관리체계(ISMS) 예비인증 이외에 귀 사(기관)에서 받았거나 유지하고 있는 타 인증・점검・평가는 무엇입니까?

1) 개인정보보호 수준진단 2) 개인정보 영향평가 3) ISO27001 4) 주요 정보통신 기반시설 대상
5) 기타 **(, ,)**

12. 정보보호 관리체계(ISMS) 예비인증을 취득 또는 준비하면서 가장 크게 개선된 사항은 무엇입니까? (1, 3,)

1) 정보보호 관련 계획 추진 및 예산 확보가 쉬워짐
2) 정보보호에 대한 경영진의 이해가 높아짐
3) 정보보호 전담하는 조직이 새로 구성됨
4) 기관 직원들의 정보보호 관련 인식이 확대됨
5) 침해사고에 대한 위험도가 낮아짐
6) 정보보호 우수기업 마케팅 활용에 따른 고객의 신뢰성이 높아짐
7) 기타 (※ 간단히 내용 작성)

13. 귀 사(기관)가 정보보호 관리체계(ISMS) 예비인증을 도입하면서 기대하는 효과는 무엇입니까? (1, 3)

1) 정보통신망법에 따른 의무 요건 충족
2) 사내 정보보호 수준 강화
3) 정보보호 조직의 역할과 권한 확대
4) ISMS 인증 취득으로 인한 고객 신뢰성 확보
5) 가상자산 사업자 신고요건 만족
6) 기타 (※ 간단히 내용 작성)

[별지 제2호 서식] 정보보호 및 개인정보보호 관리체계(ISMS-P) 명세서

Ⅰ 개요

	구분			인증범위명		
인증범위 개요	Ⅰ	ISMS	최초	쇼핑몰		
	Ⅱ	ISMS	사후1	쇼핑몰 개인정보처리 시스템		
	Ⅲ	ISMS	사후2	ISP		
	Ⅳ	ISMS-P	갱신	IDC		
인증심사 희망일	1순위: 4월2주(04.08-)			2순위: 5월2주(05.13-)	3순위: 6월2주(06.10-)	
담당자 연락처	부 서 :			성 명 :		
	전화번호 :			이 메 일 :		
관리체계 운영기간	__년 __개월 (○○○○년 ○월 ~ ○○○○년 ○월)					

	구분		범위 내 서비스 수	범위 내 개인정보	인원수 (중복 인원수)	정보시스템 수 (중복 시스템 수)	개인정보 위탁업체 수 (ISMS-P만 작성)
인증범위 대상	Ⅰ	ISMS	*○○개 서비스*	*○○만 건*	10,000명 (3,000명)	9,000대 (1,000대)	*○○개*
	Ⅱ	ISMS	*○○개 서비스*	*○○만 건*	5,000명 (3,000명)	3,000대 (1,000대)	*○○개*
	Ⅲ	ISMS	*○○개 서비스*	*○○만 건*	50,000명 (3,000명)	30,000대 (1,000대)	*○○개*
	Ⅳ	ISMS-P					*○○개*

※ 인증범위內 대상(인원, 정보시스템) 수에는 중복 포함하여 작성
※ 정보시스템에는 서버(웹서버, DB서버 등), 네트워크 장비(라우터, L4이상 스위치 등), 보안장비(방화벽, IDS, IPS, DDos 대응시스템, 웹방화벽 등) 등을 포함하며 범위내의 임대장비도 포함
※ 가상화로 운영하는 경우, 서버수 산정은 OS기준으로 산정
※ 동일 네트워크 구간내 이중화인 경우 중복 제외(네트워크 존 및 OS 세부 버전, 모델 등이 완전히 동일하게 구성된 경우만 해당)

물리적 위치	심사장 위치	
	범위 내 사업장 수	

	구분	수행일자
관리체계 수립·운영	현황 및 흐름분석 완료일	
	위험평가 완료일	
	보호대책 구현 완료일	
	관리체계 점검 완료일	

	구분	문서명	최종 업데이트일
내부정책	정책	*외 00종*	
	시행문서	*외 00종*	

[별지 제3호 서식] 결함보고서

결 함 보 고 서

기록일자	년 월 일			신 청 인		
인증범위	구분		결함유형	인증범위명		기관 확인자
	Ⅰ	ISMS	결함	OOO 쇼핑몰 운영		홍길동 팀장(인)
	Ⅱ	ISMS-P	중결함	OOO 회원관리 서비스		홍길동 부장(인)
	Ⅲ	ISMS	-	ISP		홍길동 팀장(인)
	Ⅳ	ISMS	-	IDC		홍길동 차장(인)
심사원명	홍 길 동 (인)					
관계부서	인터뷰 대상 부서 목록					

관련조항	**(관리체계) 1.2.3. 위험평가** ※ (관리체계) / (보호대책) / (개인정보) 중 작성
관련 근거	◇ **(인증기준)** 조직의 대내외 환경 분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다. ◇ **(법령)** 정보통신망법 제22조(OOO) (2020.12.10.) ※ 필요 시 작성 필요 시 간단히 요약 ◇ **(내부규정)** 계정관리지침 제6조(계정 관리 절차) (2020.7.26.) ※ 필요 시 작성 필요 시 간단히 요약
운영현황 및 결함내역	**(공통결함)** ※ 중복 인증범위에 대해서 작성 ◇ **(운영현황) 인증범위內 OOO 서비스에 대하여 ~~~ 운영하고 있음** o OOO 계정을 ~~~~ 관리하고 있음 o XXX 로그를 ~~~~ 수집·저장하고 있음 ◇ **(결함내역) OOO 서비스에 대하여 ~~~ 문제점이 발견됨** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~
	(Ⅰ. OOO 쇼핑몰 운영) ※ 해당 인증범위명 작성 ◇ **(운영현황) 인증범위內 OOO 서비스에 대하여 ~~~ 운영하고 있음** o OOO 시스템, 개인정보처리시스템 등 ~~~에 대한 위험평가를 수행함 o XXX 로그시스템에 대한 위험평가에 대한 결과를 ~~~ 보고하고 있음

	◇ **(결함내역) OOO 에 대하여 ~~~ 문제점이 발견됨** o OOO 서비스 시 XXX 공용 계정, ~~~ 등에 대한 위험평가가 누락되었음 - - o ~~~~~~~~ - - ◇ **(조치사항) OOO 에 대하여 ~~~~ 하도록 하여야 함**
	(Ⅱ. OOO 회원관리 서비스) ※ 해당 인증범위명 작성 ◇ **(운영현황) OOO 서비스에 대하여 ~~~ 위험평가 계획을 수립하고 있음** o OOO 계정에 대한 ~~~~ 위험평가 계획에 따라 위험을 평가하고 있음 o XXX 로그에 대한 ~~~~ 위험평가를 수행하여 ~~~를 하고 있음 ◇ **(결함내역) OOO 위험평가 시 ~~~ 문제점이 발견됨** o OOO 위험평가 항목에서 ~~~~ 누락되어 ~~~ 함 - - o ~~~~~ - - ◇ **(조치사항) OOO 에 대하여 ~~~~ 하도록 하여야 함**
	(Ⅲ. 인증범위명) **※ 필요 시 행 추가하여 작성**
	(Ⅳ. 인증범위명) **※ 필요 시 행 추가하여 작성**
근거목록	o OOO 계정관리 시스템 o OOO시스템 로그

[별지 제4호 서식] 보완조치 요청서

보 완 조 치 요 청 서

신 청 인				
인증범위	구 분			인증범위명
	Ⅰ	ISMS	최초	쇼핑몰
	Ⅱ	ISMS	사후1	IDC
	Ⅲ	ISMS	사후2	ISP
	Ⅳ	ISMS-P	갱신	쇼핑몰 개인정보처리시스템
인증기준	□ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표7 (과학기술정보통신부 고시 제2020-37호, 개인정보보호위원회 고시 제2020-13호)			

□ Ⅰ 인증범위명	중결함	건
	결 함	건
□ Ⅱ 인증범위명	중결함	건
	결 함	건
□ Ⅲ 인증범위명	중결함	건
	결 함	건
□ Ⅳ 인증범위명	중결함	건
	결 함	건

※ 건별 결함보고서 별도 첨부

위와 같이 인증심사 결함에 대한 보완조치요청사항을 통보하오니 40일 이내(년 월 일까지)에 보완조치를 완료하여 주시기 바랍니다.

*심사종료일 다음날부터 산정하여 40일 기준

년 월 일

한국인터넷진흥원 심사팀장 (인)

위 내용과 건별 결함보고서를 충분히 확인하였으며 기한 내 보완조치를 완료하겠습니다.

년 월 일

정보보호최고책임자 (인) 개인정보보호책임자 (인)

1. 보완조치완료사항이 미흡한 경우 심사팀장은 재조치를 요구할 수 있으며 신청인은 재조치 요구사항을 반영한 보완조치 내역서를 제출하여야 합니다.
2. 기한까지 보완조치 완료가 불가한 경우, 보완조치 연장공문을 보완조치요약서, 보완조치내역서 첨부하여 제출하여야 하며 최대 60일 연장신청을 할 수 있습니다.

※ **보완조치 기간까지 보완조치결과에 대한 이행점검 및 심사팀장의 서명이 완료되어야 하며, 완료되지 않을 경우, 해당 인증심사는 자동취소**가 됩니다.

3. 이 인증심사는 샘플링 심사기법에 의하여 수행된 것으로 발견되지 않은 결함이 존재할 수 있습니다.
4. 이 보고서의 내용은 비밀로 취급되며 신청인의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법률로 정한 경우 예외로 합니다.

[별지 제5호 서식] 인증심사 중단 확인서

인증심사 중단 확인서

신 청 인				
인증범위	구 분			인증범위명
	Ⅰ	ISMS	최초	쇼핑몰
	Ⅱ	ISMS	사후1	IDC
	Ⅲ	ISMS	사후2	ISP
	Ⅳ	ISMS-P	갱신	쇼핑몰 개인정보처리시스템
인증기준	□ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표7 (과학기술정보통신부 고시 제2020-37호, 개인정보보호위원회 고시 제2020-13호)			

□ 인증심사 중단 사유

위와 같은 사유로 인하여 인증심사를 중단하오니, 심사중단 사유를 보완 후 인증심사를 재신청하시기 바랍니다.

년 월 일

한국인터넷진흥원 심사팀장 (인)

위 내용을 확인하였으며, 인증심사 준비가 완료된 후 인증심사를 재신청하겠습니다.

년 월 일

정보보호최고책임자 (인) 개인정보보호책임자 (인)

1. 심사원 자문비 등 심사 중단전까지 소요된 모든 비용에 대한 책임은 신청인에 있으며, 신청인은 계약서에 따라 한국인터넷진흥원과 재계약을 진행해야 합니다.
2. 인증범위 변경으로 인한 심사중단인 경우에는 재신청시 최초심사로 진행합니다.
3. 인증 유효기간까지 심사를 재신청하지 않은 경우, 관계 법령에 따라 인증이 취소될 수 있습니다.
4. 이 보고서의 내용은 비밀로 취급되며 신청인의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법률로 정한 경우 예외로 합니다.

[별지 제6호 서식] 보완조치 내역서

보 완 조 치 내 역 서

신청기관					
인증범위	구분		결함유형	인증범위명	기관 확인자
	Ⅰ	ISMS	결함	OOO 쇼핑몰 운영	홍길동 팀장(인)
	Ⅱ	ISMS-P	중결함	OOO 회원관리 서비스	홍길동 부장(인)
	Ⅲ	ISMS	-	ISP	홍길동 팀장(인)
	Ⅳ	ISMS	-	IDC	홍길동 차장(인)
보완조치 결과확인	확인자(심사팀장)			홍 길 동 (인)	확인일 / 년 월 일

관련조항	(보호대책) 2.5.1 사용자 계정 관리
보완조치 및 재발방지대책	**(공통사항)** ※ 중복 인증범위 결함이 있는 경우 공통 보완조치 내역 작성 **◇ (결함내역) OOO 서비스에 대하여 ~~~ 문제점이 발견됨** o OOO 계정을 ~~~~ 관리하고 있음 o XXX 로그를 ~~~~ 수집·저장하고 있음 **◇ (조치내역) OOO 서비스에 대하여 ~~~를 다음과 같이 조치함** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~ **◇ (재발방지대책) OOO 서비스에 대하여 ~~~ 하도록 함** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~ *※ 보완내역을 상세하게 작성하고 필요 시 증적(실행 화면, 문서, 사진 등)를 첨부, 여러 페이지 작성 가능* *※ 관련 문서 또는 시스템이 있는 경우 작성*
	(Ⅰ. OOO 쇼핑몰 운영) ※ 인증범위명 작성 **◇ (결함내역) OOO 서비스에 대하여 ~~~ 문제점이 발견됨** o OOO 계정을 ~~~~ 관리하고 있음 o XXX 로그를 ~~~~ 수집·저장하고 있음 **◇ (조치내역) OOO 서비스에 대하여 ~~~를 다음과 같이 조치함** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~

	◇ **(재발방지대책) OOO 서비스에 대하여 ~~~ 하도록 함** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~ *※ 보완내역을 상세하게 작성하고 필요 시 증적(실행 화면, 문서, 사진 등)를 첨부, 여러 페이지 작성 가능* *※ 관련 문서 또는 시스템이 있는 경우 작성*
	(Ⅱ. OOO 회원관리 서비스) ※ 해당 인증범위명 작성 ◇ **(결함내역) OOO 서비스에 대하여 ~~~ 문제점이 발견됨** o OOO 계정을 ~~~~ 관리하고 있음 o XXX 로그를 ~~~~ 수집·저장하고 있음 ◇ **(조치내역) OOO 서비스에 대하여 ~~~를 다음과 같이 조치함** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~ ◇ **(재발방지대책) OOO 서비스에 대하여 ~~~ 하도록 함** o OOO 서비스 시 XXX 계정을 공용으로 사용하고 있어 ~~~ 함 o ~~~~~ *※ 보완내역을 상세하게 작성하고 필요 시 증적(실행 화면, 문서, 사진 등)를 첨부, 여러 페이지 작성 가능* *※ 관련 문서 또는 시스템이 있는 경우 작성*
	(Ⅲ. 인증범위명) **※ 필요 시 행 추가하여 작성**
	(Ⅳ. 인증범위명) **※ 필요 시 행 추가하여 작성**
근거목록	o OOO 계정관리 시스템 o OOO시스템 로그

[별지 제7호 서식] 보완조치 요약서

보 완 조 치 요 약 서

신 청 인				
인증범위	구 분			인증범위명
	Ⅰ	*ISMS*	*최초*	*쇼핑몰*
	Ⅱ	*ISMS*	*사후1*	*IDC*
	Ⅲ	*ISMS*	*사후2*	*ISP*
	Ⅳ	*ISMS-P*	*갱신*	*쇼핑몰 개인정보처리시스템*

□ 보완조치 내역

(1) 완료 내역
- 총 결함 O건 중 O건 완료

	결함	건
□ *Ⅰ 인증범위명*	완료	건
	미완료	건
	결함	**건**
□ *Ⅱ 인증범위명*	완료	건
	미완료	건
	결함	**건**
□ *Ⅲ 인증범위명*	완료	건
	미완료	건
	결함	**건**
□ *Ⅳ 인증범위명*	완료	건
	미완료	건

(2) 미완료 상세내역

기준 항목	미완료 내역	완료예정일
(관) 1.2.3 위험 평가	*Ⅰ 인증범위명* ※ 인증범위명 기준으로 별도 작성 o 위험 식별 및 평가 수행*(예시)* - 누락자산 현행화 : 완료 - 위험 식별 및 취약점 점검 : 진행중(~0000.00.00) - 도출된 결과를 통한 대책수립 : 예정(~0000.00.00) *Ⅲ 성춘향 커뮤니티 서비스운영* ※ 인증범위명 기준으로 별도 작성 o 위험 식별 및 평가 수행*(예시)* - 누락자산 현행화 : 완료 - 위험 식별 및 취약점 점검 : 진행중(~0000.00.00) - 도출된 결과를 통한 대책수립 : 예정(~0000.00.00)	0000.00.00

2.5.5 특수 계정 및 권한 관리	*Ⅲ 성춘향 커뮤니티 서비스운영* ※ 인증범위명 기준으로 별도 작성 o 계정 관리 - DB접근제어 솔루션: 완료*(예시)* - VPN 솔루션: 완료 - IPS: O대中 O대 완료(0000.00.00까지 완료 예정)	0000.00.00

※ 위의 표는 **보완조치 미완료 통제항목**에 대한 진행상황 및 구체적인 일정계획 작성

[별지 제8호 서식] 보완조치 완료확인서

보 완 조 치 완 료 확 인 서

신 청 인				
인증범위	구 분			인증범위명
	Ⅰ	ISMS	최초	쇼핑몰
	Ⅱ	ISMS	사후1	IDC
	Ⅲ	ISMS	사후2	ISP
	Ⅳ	ISMS-P	갱신	쇼핑몰 개인정보처리시스템
인증기준	□ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표7 (과학기술정보통신부 고시 제2020-37호, 개인정보보호위원회 고시 제2020-13호)			

□ Ⅰ 인증범위명	결함내역	건
	보완조치	건
□ Ⅱ 인증범위명	결함내역	건
	보완조치	건
□ Ⅲ 인증범위명	결함내역	건
	보완조치	건
□ Ⅳ 인증범위명	결함내역	건
	보완조치	건

※ 건별 보완조치내역서 별도 첨부

인증심사 결함 사항에 대한 보완조치 내역을 제출합니다.

년 월 일

정보보호최고책임자 (인) 개인정보보호책임자 (인)

인증심사 결함사항에 대해 보완조치가 완료되었음을 확인하였습니다.

년 월 일

한국인터넷진흥원 심사팀장 (인)

1. 이 인증심사는 샘플링 심사기법에 의하여 수행된 것으로 발견되지 않은 결함이 존재할 수 있습니다.
2. 이 보고서의 내용은 비밀로 취급되며 신청인의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법률로 정한 경우 예외로 합니다.

[별지 제9호 서식] 책임심사원 확인서

책임심사원 확인서

1. 자격번호 :
2. 성 명 :
3. 활동기간 : 0000년 1월 1일 ~ 12월 31일

위 사람은 위 활동기간 동안 정보보호 및 개인정보보호 관리체계 인증심사 책임심사원임을 확인합니다. 단, 인증심사원 자격을 갱신하지 않고 심사원 자격 유효기간이 만료되면, 책임심사원 등급도 함께 종료됩니다.

년 월 일

한국인터넷진흥원장 직인

[별지 제10호 서식] 인증심사팀 다면 평가서<개정 2022. 12. 23.>

인증심사팀 다면 평가서

기업명		심사	ISMS ISMS-P	유형	최초 사후 갱신

평 가 항 목		평 가 방 법	배점		A	B
공통	**인증기준 이해력**	분야 전문성, 자료요구 및 인터뷰 내용과 통제항목과의 연관성 등	매우우수 우수 보통 미흡 매우미흡	100점 90점 80점 70점 60점		
	결함 및 관찰사항 판단 능력	양식작성, 문맥오류, 보고서의 논리력 및 전달력, 기한 내 작성 등				
	피심사자와의 의사소통 능력	인터뷰 언행, 자료요구 및 현장심사 태도 등				
심사팀장	**심사팀 통솔 능력**	정보수집력, 결함에 따른 조치방안의 적절성 등				
	명확한 근거 제시 능력	심사팀 내 의견제시, 심사참여 적극성, 심사준비, 시간준수, 복장, 보안의식 등				
심사원	**심사보고서 작성능력**	정보수집력, 결함에 따른 조치방안의 적절성 등				
	협업 및 심사태도	심사팀 내 의견제시, 심사참여 적극성, 심사준비, 시간준수, 복장, 보안의식 등				
이슈사항	**인증심사 업무 관련 이해관계인으로부터 받은 이의제기**	타당성이 인정된 민원 접수 건				
심사원 추천 여부(기술분야)						
심사원 추천 여부(전반)						
평가점수					0	0

평가소견	
평가일자/평가자	0000.00.00. /성명 : (인)

[별지 제11호 서식] 업무 수행 행동 강령

업무 수행 행동 강령

☐ 대상 : (신청기관) (심사구분) 인증 (최초/사후/갱신) 심사
☐ 수행 기간 : 년 월 일 ~ 년 월 일

우리는 한국인터넷진흥원(KISA)의 인증심사 업무를 수행함에 있어, 깨끗하고 투명한 사회의 실현을 위하여 다음 사항들을 실천하겠습니다.

Ⅰ. 우리는 법과 원칙의 철저한 준수야말로 부패방지의 바른 길이라 생각하며, 관계 법령과 규정이 정하는 절차에 따라 업무를 정확하고 공정하게 수행하겠습니다.

Ⅰ. 우리는 작은 부패에도 관대하지 않을 것이며, 부정한 방법과 부패한 수단에 의존하여 자신과 타인의 이익을 도모하지 않겠습니다.

Ⅰ. 우리는 혈연·지연·학연보다는 합리성과 공정성을 기준으로 판단하고 행동하겠습니다.

Ⅰ. 우리는 부정부패와 관련될 수 있는 어떠한 금품이나 선물, 향응이나 접대 등을 요구하지도 않고 받지도 않겠으며, 이를 위반할 때에는 관계 법령과 규정에 따라 엄중히 책임지겠습니다.

Ⅰ. 우리는 업무상 지득한 각종 정보를 불법적으로 유출·은폐·왜곡·조작하여 공공의 피해를 주거나 자신과 타인의 이익을 도모하는 '정보부패'를 저지르지 않겠습니다.

Ⅰ. 우리는 업무 수행과 관련한 불편, 불만, 개선의견 등을 적극 수렴하겠습니다. 이를 위하여 본 업무 관련 보직자와의 핫라인을 운영하고 있으며 연락자의 인적사항 등은 철저하게 보호하겠습니다.

- KISA oooo단 단장 ooo, ooooo@kisa.or.kr, 00-000-0000

- KISA oooo팀 팀장 ooo, ooooo@kisa.or.kr, 00-000-0000

년 월 일

(심사구분) 심사팀장 *(심사팀장)* 외 *(심사원 수)*명 일동

	(인)		(인)
	(인)		(인)
	(인)		(인)

[별지 제12호 서식] 보안서약서<개정 2022. 12. 23.>

보 안 서 약 서

심사구분	□ ISMS-P (최초 / 사후1차 / 사후2차 / 갱신)
	□ ISMS (최초 / 사후1차 / 사후2차 / 갱신)
기관명	
심사기간	년 월 일 ~ 년 월 일

본인은 위 신청기관에 대한 한국인터넷진흥원에서 수행하는 정보보호 및 개인정보보호 관리체계 인증업무를 수행함에 있어 관련 법령을 성실히 준수합니다.

또한, 인증업무 수행과정에서 취득한 사실과 신청인의 제출물을 인증업무 수행 이외의 용도로 사용하거나 유출 또는 공개하지 아니할 것이며 위의 사항을 위반할 경우 심사자격 취소 및 관련 법규에 따라 형사처벌 등 어떠한 처벌도 감수할 것을 서약합니다.

소 속 :

성 명 : **(서명)**

년 월 일

가. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

제66조(비밀유지 등) 다음 각 호의 어느 하나에 해당하는 업무에 종사하는 자 또는 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

2. 제47조에 따른 정보보호 관리체계 인증 업무

제72조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 **3천만원 이하**의 벌금에 처한다.

5. 제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자

나. 정보통신기반 보호법 제27조(비밀유지의무) 및 제29조(벌칙)

다. 국가보안법 제4조 제1항 제5호(국가기밀 누설 등)

[별지 제13호 서식] 인증위원 위촉장

제 호

인증위원 위촉장

소 속 :

성 명 :

기 간 :

귀하를 한국인터넷진흥원 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증위원으로 위촉합니다.

년 월 일

한국인터넷진흥원장 직인

[별지 제14호 서식] 인증위원 윤리 서약서

인증위원 윤리 서약서

□ 대상 활동 : 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증위원회 활동

□ 위촉 기간 : 년 월 일 - 년 월 일

우리는 정보보호 및 개인정보보호 관리체계 인증위원으로 활동함에 있어, 깨끗하고 투명한 사회의 실현을 위하여 다음 사항들을 실천하겠습니다.

1. 우리는 법과 원칙의 철저한 준수야말로 부패방지의 바른 길이라 생각하며, 관계 법령과 규정이 정하는 절차에 따라 업무를 정확하고 공정하게 수행하겠습니다.

1. 우리는 작은 부패에도 관대하지 않을 것이며, 부정한 방법과 부패한 수단에 의존하여 자신과 타인의 이익을 도모하지 않겠습니다.

1. 우리는 혈연.지연.학연 보다는 합리성과 공정성을 기준으로 판단하고 행동하겠습니다.

1. 우리는 부정부패와 관련될 수 있는 어떠한 금품이나 선물, 향응이나 접대 등을 요구하지도 않고 받지도 않겠으며, 이를 위반할 때에는 관계 법령과 규정에 따라 엄중히 책임지겠습니다.

1. 우리는 업무상 지득한 각종 정보를 불법적으로 유출.은폐.왜곡.조작하여 공공의 피해를 주거나 자신과 타인의 이익을 도모하는 '정보부패'를 저지르지 않겠습니다.

년 월 일

인증위원회 위원장 외 위원 O명 일동

_____

_____

_____

_____

[별지 제15호 서식] 인증위원 정보보호 서약서

인증위원 정보보호 서약서

□ 위촉 기간 : 년 월 일 - 년 월 일

본인은 위 기간 동안 한국인터넷진흥원의 정보보호 및 개인정보보호 관리체계 인증위원회 위원으로서 인증업무를 수행함에 있어 관련 법령을 성실히 준수하고 수행과정에서 취득한 사실에 대한 비밀을 유출 또는 공개하지 아니할 것이며 위의 사항을 위반할 경우 관련 법규에 따라 어떠한 처벌도 감수할 것을 서약합니다.

소속 :

성명 : (서명)

가. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

제66조(비밀유지 등) 다음 각 호의 어느 하나에 해당하는 업무에 종사하는 자 또는 종사하였던 자는 **그 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용하여서는 아니 된다**. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

2. 제47조에 따른 정보보호 관리체계 인증업무

제72조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 **3년 이하의 징역 또는 3천만원 이하의 벌금**에 처한다.

5. 제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자

나. 정보통신기반 보호법 제27조(비밀유지의무) 및 제29조(벌칙)

다. 국가보안법 제4조 제1항 제5호(국가기밀 누설 등)

라. 형법 제127조(공무상 비밀의 누설)

마. 군형법 제80조(군사기밀 누설)

바. 군사기밀 보호법 제12조(누설) 및 제13조(업무상 군사기밀 누설)

[별지 제16호 서식] 현장참관 결과서<신설 2023. 9. 26.>

분야	대상	구분	점검항목	검토의견	결과
자원관리	심사팀장	리더십	o 심사원의 의무, 책임 및 권한에 대한 명확한 업무분장(R&R)을 하였는가?	*o 확 인 사 항 ~~~ ※ 증빙자료 ~*	*양호*
		심사역량	o 심사 스킬 및 지식 뿐 아니라 특정 기술 영역의 심사를 위한 역량을 보유하고 있는가?	*o 확 인 사 항 ~~~ ※ 증빙자료 ~*	*미흡*
		의사소통	o 심사원의 심사과정, 보고서 작성, 기업 담당자 인터뷰 및 피드백이 적절히 이루어지고 있는지 파악하고 있는가?		
		이슈해결	o 신청기관 또는 심사팀 내의 이슈발생 시 적절한 의견교환 및 협의를 통해 원활히 해결하는가?		
	심사원	심사역량	o 심사스킬 및 지식뿐 아니라 특정 기술 영역의 심사를 위한 역량을 보유하고 있는가?		
		인증이해	o 심사 프로세스, 인증 요구사항에 대해 명확히 이해하고 있는가?		
		비밀유지	o 외부출처(민원신청자, 규제기관 등)을 통해 입수된 신청기관의 정보를 심사과정에서 기밀로 취급하고 관리하는가? o 타기업 정보 등 유사기밀을 심사팀 또는 신청기관 등 타인에게 발설하거나 외부에 공개되지 않도록 유의하는가?		
		의사소통	o 심사 중 신청기관 담당자 및 타심사원과 의사소통이 원활히 진행되었는가? o 심사팀 및 신청기관 상호간 의견상충 시 합의점 도출에 필요한 적합한 노력을 취하였는가?		
		보고서 작성	o 심사 시 발견사항, 근거자료, 인터뷰 수행 이력 등을 적절하게 기록하였는가? o 결함보고서의 형식, 내용, 결함의 판단근거 등이 명확하고 알기쉽게 작성되었는가?		
프로세스관리	심사팀 전체	심사절차	o 심사는 정해진 계획에 따라 적절한 절차와 일정대로 진행되었는가? o 당초 계획에 포함되지 않은 비상상황, 추가일정 등에 적절히 대처하였는가?		
		결함 및 조치대응	o 심사 종료 시, 발견된 결함에 대한 적절한 판단근거를 제시하고 구체적인 개선방안을 권고하였는가?		
		시작·종료	o 시작회의 시, 전반적인 심사계획의 공유		

분야	대상	구분	점검항목	검토의견	결과
		회의	및 종료회의 시, 심사결과에 대한 총평 등을 통해 신청기관이 쉽게 이해할 수 있도록 회의를 진행하였는가?		
일정 관리	심사 팀장	사전준비	o 신청기관의 인증범위, 조직, 법적 요구사항 등 주요사항에 대해 신청서, 홈페이지 등을 통해 사전에 충분히 숙지하고 심사에 참여하였는가?		
		심사계획	o 신청기관과 사전에 충분한 협의를 거쳐 적절한 심사범위, 일정, 인증기준 등 계획을 수립하여 진행하였는가? 또한, 심사계획을 신청기관과 사전에 공유하였는가?		
		복수심사장	o 복수 심사장소에 대해 샘플링하여 심사를 진행하는 경우, 전체적으로 적절한 심사일정을 보장할 수 있도록 계획하였는가?		
사후 관리	심사팀 전체	지속성	o 전년도 결함사항에 대한 후속조치 활동이 지속적으로 이루어지는 지 검토하였는가?		
		변경관리	o 전년도와 현재의 인증범위 비교를 통해 조직내 중요한 변경사항(시스템 구성 또는 조직의 변화 등) 발생여부에 대해 검토하였는가?		
		사고대응	o 지난 1년간 침해사고 발생여부, 사고조치 여부, 후속조치의 적절성 등에 대하여 세부적으로 확인하였는가?		
심사 대응	신청 기관	심사대응	o 적절한 사유없이 심사를 지연시키거나 심사절차를 위반하지 않았는가?		
		자료제출	o 심사팀에서 요구하는 심사에 필수적으로 확인이 필요한 자료 등을 적시에 제출하였는가?		
		인증이해	o 심사 사전·사후 절차 준수, 인증범위·대상, 인증기준 등 심사 전반에 대해 충분히 숙지하고 대응하였는가?		
		의사소통	o 심사가 원활히 진행될 수 있도록 심사에 협조하고 소통하려고 노력하였는가?		