「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 전부 개정(안)

과학기술정보통신부·행정안전부·방송통신위원회

1. 개정이유

과학기술정보통신부가 고시한「정보보호 관리체계 인증 등에 관한 고시」와 방송통신위원회와 행정안전부가 공동 고시한 「개인정보보호 관리체계 인증 등에 관한 고시」의 내용을 통합하여 중복운영에 따른 기업·기관부담 해소 및 행정비용을 절감하고 고도화·융합화되는 사이버 공격에 효과적으로 대응할 수 있는 환경을 마련하고자 함

2. 주요내용

가. 양 고시의 용어를 반영하여 '정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시'로 명칭 마련(안 제명)

나. 인증제도 전반에 관한 정책사항을 결정할 수 있도록 과기정통부·행안부·방통위가 참여하는 협의회 구성·운영(안 제4조~제5조)

다. 인증기관 및 심사기관의 지정 기준을 통합하고, 부처 공동으로 인증·심사기관을 지정할 수 있도록 절차 마련(안 제6조~제11조)

라. 기존 정보보호 관리체계 인증 및 개인정보보호 관리체계 인증 심사원 자격요건을 통합한 인증심사원 자격요건 마련(안 제12조~제16조, 안 별표3~별표4)

마. 정보보호 관리체계 인증 의무 이행기간을 기존 '매년 1월~12월'에서 '차년도 8.31까지'로 변경하고 '19년도 의무 대상자부터 적용(안 제19조, 안 부칙제2조)

바. 기존 정보보호 관리체계 인증기준(104개)와 개인정보보호 관리체계 인증기준(86개)을 통합하여 102개의 단일 인증기준으로 통합하되, 정보보호

관련 80개 인증기준으로 ‘정보보호 관리체계(ISMS) 인증’을 받을 수 있고, 개인정보 관련 22개 인증기준을 추가하면 ‘정보보호 및 개인정보보호 관리체계(ISMS-P) 인증’을 받을 수 있음(안 제23조, 안 별표7)

사. 인증심사에서 발견한 결함에 대해 심사종료 다음날부터 최대 100일(재조치 요구 60일 포함) 이내에 보완조치를 완료(안 제25조)

아. 고시는 개정 후 즉시 시행하되 고시 시행 후 6개월까지는 기존 인증기준으로도 심사를 받을 수 있게 유예기간 부여(안 부칙 제4조)

- 기존 인증 취득기업은 인증서 유효기간까지 기존 인증기준으로 사후심사

3. 참고사항

가. 관계법령 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법

나. 예산조치 : 별도조치 필요 없음

다. 기　　타 : 해당사항 없음

◉ **과학기술정보통신부　고시 제2018-80호**

◉ **행정안전부　　고시 제2018-71호**

◉ **방송통신위원회　　고시 제2018-14호**

과학기술정보통신부가 고시한「정보보호 관리체계 인증 등에 관한 고시」와 방송통신위원회와 행정안전부가 공동 고시한 「개인정보보호 관리체계 인증 등에 관한 고시」의 내용을 통합하여 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」로 공동으로 전부개정하여 고시합니다.

2018년 11월 7일

과학기술정보통신부장관·행정안전부장관·방송통신위원장

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

제1장 총칙

제1조(목적) 이 고시는「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법"이라 한다)」 제47조제3항·제4항, 같은 법 시행령 제47조부터 제53조의2까지의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과, 같은 법 제47조의3제2항, 같은 법 시행령 제54조의2의 규정에

따른 개인정보보호 관리체계 인증 및 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 인증의 통합 운영에 필요한 사항을 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 및 개인정보보호 관리체계 인증"이란 인증 신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
2. "정보보호 관리체계 인증"이란 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 것을 말한다.
3. "인증기관"이란 인증에 관한 업무를 수행할 수 있도록 정보통신망법 제47조제6항과 제47조의3제3항, 「개인정보 보호법 시행령」 제34조의6 제1항제2호 및 제2항에 따라 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회가 지정하는 기관을 말한다.
4. "심사기관"이란 인증심사 업무를 수행할 수 있도록 정보통신망법 제47조 제7항과 제47조의3제3항, 「개인정보 보호법 시행령」 제34조의6제1항제2호 및 제2항에 따라 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회가 지정하는 기관을 말한다.
5. "업무수행 요건·능력 심사"란 인증기관 또는 심사기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 심사하는 것을 말한다.
6. "인증심사"란 신청기관이 수립하여 운영하는 관리체계가 인증기준에 적합

한지의 여부를 인터넷진흥원·인증기관 또는 심사기관(이하 "심사수행기관"이라 한다)이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.

7. "인증위원회"란 인터넷진흥원 또는 인증기관의 장이 인증심사 결과 등을 심의·의결하기 위해 설치·운영하는 기구로서 위원장과 위원으로 구성된다.
8. "인증심사원"이란 인터넷진흥원으로부터 인증심사를 수행할 수 있는 자격을 부여받고 인증심사를 수행하는 자를 말한다.
9. "최초심사"란 처음으로 인증을 신청하거나 인증범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
10. "사후심사"란 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. "갱신심사"란 유효기간 만료로 유효기간 갱신을 위해 실시하는 인증심사를 말한다.

제3조(적용범위) 이 고시는 정보보호 및 개인정보보호 관리체계 인증, 정보보호 관리체계 인증에 공통으로 적용하되, 각 인증에 따로 적용되는 내용이 있는 경우 별도 조항으로 정한다.

제2장 정보보호 및 개인정보보호 관리체계 인증 협의회

제4조(협의회의 구성) ① 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 정보보호 및 개인정보보호 관리체계 인증 운영에 관한 정책사항을 협의하기 위하여 정보보호 및 개인정보보호 관리체계 인증 협의회(이하 "협의회"라 한다)를 운영한다.

② 협의회 위원은 과학기술정보통신부, 행정안전부 및 방송통신위원회 소속의 인증업무를 담당하는 부서의 장으로 한다.

③ 협의회 운영을 위하여 인터넷진흥원의 인증업무를 담당하는 부서의 장을 간사로 두며, 간사는 회의에 참석하여 발언할 수 있다.

제5조(협의회의 운영) ① 협의회는 정보보호 및 개인정보보호 관리체계 인증 제도 와 관련하여 다음 각 호의 사항을 협의한다.

1. 인증제도 연구 및 개선에 관한 사항

2. 인증제도 운영을 위한 제반사항 검토 및 품질관리에 관한 사항

3. 인증기관 및 심사기관의 지정·재지정 및 업무정지·지정 취소에 관한 사항

4. 인증기관 및 심사기관의 관리·감독에 관한 사항

5. 인증제도 운영에 따른 민원 처리 및 법적 분쟁에 관한 사항

6. 그 밖에 협의가 필요한 사항

② 협의회는 과학기술정보통신부장관, 행정안전부장관 또는 방송통신위원회의 요구가 있거나 협의안건이 발생한 경우 개최할 수 있다.

③ 인터넷진흥원은 협의회 개최 및 제1항 각 호에 따른 협의회 운영 업무를 지원할 수 있다.

④ 협의회는 필요하다고 인정하는 때에는 관계기관의 공무원 및 임·직원, 그 밖의 전문가를 협의회에 참석하게 하여 그 의견을 들을 수 있다.

⑤ 협의회는 협의회의 운영을 위한 별도의 규정을 정할 수 있다.

제3장 인증기관 및 심사기관

제6조(지정공고) ① 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 인증기관 또는 심사기관을 지정할 필요가 있는 때에는 협의회에서 지정대상 기관의 수, 업무의 범위, 신청방법 등을 미리 협의하고, 관보 또는 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관 또는 심사기관으로 지정받으려는 자는 다음 각 호의 서류를 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회에 제출하여야 한다.

1. 별지 제1호서식의 인증기관·심사기관 지정 신청서
2. 별지 제2호서식의 인증심사 업무를 수행하는 직원 보유현황과 이를 증명할 수 있는 서류
3. 별표 1의 업무수행 요건·능력 심사 제출서류

③ 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 인증기관 또는 심사기관의 지정, 재지정, 사후관리 등에 따른 업무를 인터넷진흥원에 위탁할 수 있다.

제7조(지정기준 및 지정절차) ① 인증기관 또는 심사기관의 업무수행 요건·능력 심사에 관한 세부기준은 별표 2와 같다.

② 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 제6조 제2항에 따라 인증기관 또는 심사기관의 지정 신청을 받은 때에는 제1항에 따른 업무수행 요건·능력을 심사한다.

③ 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 제2항에 따른 심사 결과를 바탕으로 협의하여 인증기관 또는 심사기관으로의 지정 여부를 최종 결정한다.

④ 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 인증기관으로 지정된 신청기관에 별지 제3호서식 정보보호 및 개인정보보호 관리체계 인증기관 지정서를, 심사기관으로 지정된 신청기관에 별지 제4호서식 정보보호 및 개인정보보호 관리체계 심사기관 지정서를 발급한다.

제8조(인증기관 및 심사기관의 사후관리) ① 인증기관과 심사기관은 매년 1월 31일까지 다음 각 호의 서류를 작성하여 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회에 제출하여야 한다.

1. 별지 제5호서식의 인증실적 보고서(해당 시)

2. 별지 제6호서식의 인증심사실적 보고서(해당 시)

② 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 필요한 경우 인증기관 또는 심사기관이 지정기준에 적합한지 여부의 확인을 위해 자료요청 또는 현장실사를 할 수 있다.

제9조(인증기관 및 심사기관의 재지정) ① 인증기관 및 심사기관 지정의 유효기간은 3년이며 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정을 신청을 할 수 있으며 제6조제2항 각 호의 서류를 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회에 제출하여야 한다. 이 경우 재지정의 신청에 대한 처리결과를 통지받을 때까지는 그 지정이 계속 유효한 것으로 본다.

② 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 제1항에 따른 재지정 신청을 받은 때에는 별표 2 업무수행 요건·능력 심사에 관한 세부기준에 따른 적합 여부를 심사하여 신청을 받은 날부터 3개월 이내에 그 결과를 신청기관에 통지하고, 인증기관 또는 심사기관으로 지정되는 신청

기관에 제7조제4항의 지정서를 발급하여야 한다.

③ 인증기관 또는 심사기관이 재지정을 신청하지 않고 유효기간이 경과한 때에는 인증기관 또는 심사기관의 효력은 상실된다.

제10조(공정성 및 독립성 확보) 인증기관 및 심사기관은 인증심사의 공정성 및 독립성 확보를 위해 다음 각 호의 행위가 발생되지 않도록 노력하여야 한다.

1. 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하는 행위
2. 정당한 사유 없이 인증절차, 인증기준 등의 일부를 생략하는 행위
3. 조직의 이익 등을 위해 인증심사 결과에 영향을 주는 행위
4. 그 밖에 인증심사의 공정성 및 독립성을 훼손할 수 있는 행위

제11조(인증기관 및 심사기관의 지정취소 등) ① 인증기관 및 심사기관이 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호나 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 인증기관 또는 심사기관의 지정을 받은 경우
2. 업무정지 기간 중에 인증 또는 인증심사를 한 경우
3. 정당한 사유 없이 인증 또는 인증심사를 하지 아니한 경우
4. 정보통신망법 제47조제11항을 위반하여 인증 또는 인증심사를 한 경우
5. 정보통신망법 제47조제12항에 따른 지정기준에 적합하지 아니하게 된 경우

② 지정취소 및 업무정지에 대해서는「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(이하 "정보통신망법 시행령"이라 한다)」제54조에 따른 지정취소 및 업무정지에 관한 행정처분의 기준을 따른다.

제4장 인증심사원

제12조(인증심사원의 자격 요건 등) 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며 등급별 자격 요건은 별표 3과 같다.

제13조(인증심사원 자격 신청) ① 인증심사원 자격을 신청하고자 하는 자는 별표 4의 인증심사원 자격 신청 요건을 갖추고 인터넷진흥원이 공고하는 신청기간 내에 별지 제7호 서식의 인증심사원 자격 신청서와 관련 서류를 제출하여야 한다.

② 인터넷진흥원은 제1항에 의해 제출한 신청서류가 자격 신청 요건에 적합한지를 검토하여야 한다.

③ 제2항에 따른 서류검토 결과 적합한 자는 인터넷진흥원이 시행하는 인증심사원 양성과정을 수료하여야 한다.

제14조(인증심사원 자격 발급 및 관리) ① 인터넷진흥원은 인증심사원 양성과정을 수료한 자에게 별지 제8호서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 발급하여야 한다.

② 인터넷진흥원은 인증심사원의 자격 증명서 발급, 심사원등급, 인증심사 업무경력 등을 관리하여야 한다.

제15조(인증심사원 자격 유지 및 갱신) ① 인증심사원의 자격 유효기간은 자격을

부여 받은 날부터 3년으로 한다.

② 인증심사원은 자격유지를 위해 자격 유효기간 만료 전까지 인터넷진흥원이 인정하는 보수교육을 수료하여야 한다.

③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 보수교육 시간 중 일부를 이수한 것으로 인정할 수 있다.

④ 인터넷진흥원은 인증정보를 제공하는 홈페이지에 제2항의 보수교육 운영에 관한 세부내용을 공지하여야 한다.

⑤ 인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 별지 제8호 서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.

제16조(인증심사원 자격 취소) ① 인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우 인증심사원의 자격을 취소할 수 있다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 부여 받은 경우
2. 제15조제2항에 따른 자격 유지 기준을 충족하지 못한 경우
3. 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않은 경우
4. 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우
5. 인증신청인으로부터 금전, 금품, 향응, 이익 등을 부당하게 수수하거나 요구한 경우

② 인터넷진흥원의 장은 제1항에 따른 자격 취소의 적합여부를 심의·의결

하기 위하여 자격심의위원회를 개최하여야 하며, 자격심의위원회는 제29조의 인증위원회 위원 3인 이상을 포함하여 구성한다.

③ 제1항에 따른 자격 취소에 대하여 인증심사원은 30일 이내에 이의신청을 할 수 있다. 이 경우 인터넷진흥원은 해당 인증심사원의 자격을 제2항의 절차에 따라 재심의하여 처리결과를 통지하여야 한다.

제5장 인증심사의 신청 및 수수료 납부

제17조(신청인의 사전 준비사항) ① 정보보호 및 개인정보보호 관리체계 인증을 취득하고자 하는 자(이하 "신청인"이라 한다)는 인증을 신청하기 전에 인증기준에 따른 정보보호 및 개인정보보호 관리체계 또는 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

② 신청인은 인증심사를 위하여 다음 각 호의 사항을 인증심사 실시 전에 준비하여야 한다.

1. 인증심사를 위한 문서 및 증적자료
2. 인증심사 수행에 필요한 장소·시설·장비·기자재 등의 확보
3. 그 밖에 인증심사를 원활하게 수행하기 위하여 심사수행기관이 요구하는 사항

제18조(인증 신청 등) ① 신청인은 다음 각 호의 인증을 선택하여 신청할 수 있다.

1. 정보보호 및 개인정보보호 관리체계 인증
2. 정보보호 관리체계 인증

② 신청인은 제1항의 인증 선택에 따른 별지 제9호서식의 정보보호 및 개인정보보호 관리체계 인증 신청서를 심사수행기관에 제출하여야 한다.

③ 신청인은 인증범위 및 일정 등을 심사수행기관과 사전 협의하여 신청하여야 한다.

④ 심사수행기관은 제17조에 따른 신청인의 인증심사 사전준비사항을 확인할 수 있으며, 신청인의 준비가 미흡한 경우에는 신청인에 이를 보완할 것을 요구할 수 있다.

⑤ 심사수행기관은 인증범위의 변경이 필요한 경우에 이를 신청인과 협의하여 변경할 수 있다.

제19조(정보보호 관리체계 인증 의무대상자) ① 정보보호 관리체계 인증 의무대상자(이하 "의무대상자"라 한다)란 정보통신망법 제47조제2항, 같은 법 시행령 제49조에 해당하는 자를 말한다.

② 제1항에 해당하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 정보통신망법 시행령 제49조제2항의 기준을 준용한다.

③ 의무대상자는 제18조제1항제2호의 정보보호 관리체계 인증을 받아야 한다. 이때 의무대상자가 같은 항 제1호의 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.

④ 의무대상자에 해당하는 자는 다음 해 8월31일까지 인증을 받아야 한다.

제20조(인증심사의 일부 생략 신청 등) ① 제18조제1항제2호의 정보보호 관리체계 인증을 신청한 자가 다음 각 호의 어느 하나에 해당하는 인증을 받거나 정보보호 조치를 취한 경우 별표 5의 인증심사 일부 생략의 범위 내에서

인증심사의 일부를 생략할 수 있다.

1. 국제인정협력기구에 가입된 인정기관이 인정한 인증기관으로부터 받은 ISO/IEC 27001 인증
2. 「정보통신기반 보호법」 제9조에 따른 주요정보통신기반시설의 취약점 분석·평가

② 제1항에 따라 정보보호 관리체계 인증심사의 일부를 생략하려는 경우에는 다음 각 호의 요건을 모두 충족하여야 한다.

1. 해당 국제표준 정보보호 인증 또는 정보보호 조치의 범위가 정보보호 관리체계 인증의 범위와 일치할 것
2. 정보보호 관리체계 인증 신청 및 심사 시에 해당 국제표준 정보보호 인증이나 정보보호 조치가 유효하게 유지되고 있을 것

③ 제1항에 따른 인증심사 일부 생략을 신청하고자하는 자는 별지 제10호 서식의 인증심사 일부 생략 신청서를 심사수행기관에 제출하여야 한다.

④ 심사수행기관은 별표 5의 인증심사 일부 생략의 범위를 생략하여 심사하고 인터넷진흥원 또는 인증기관이 인증을 부여할 때에는 그 사실을 인증서에 표기하여야한다.

제21조(수수료의 산정) ① 인증 수수료는 별표 6의 인증 수수료 산정 및 심사원 보수 기준을 적용하여 산정한다.

② 심사수행기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다.

③ 심사수행기관은 신청인이 다음 각 호에 해당하는 경우 수수료를 감면 또는 조정 할 수 있다.

1.「중소기업기본법」 제2조에 따른 소기업에 해당되는 경우

2. 제20조에 따른 인증심사 일부 생략 신청을 하는 경우

3. 그 밖에 신청인과 협의하여 수수료 조정이 필요하다고 판단되는 경우

제22조(수수료의 납부) 신청인은 최초심사, 사후심사 및 갱신심사 신청 시 인증수수료를 청구 받은 날부터 인증심사 시작일 이전까지 심사수행기관에 납부하여야 하며, 수수료를 납부하지 않은 경우 심사수행기관은 인증심사를 실시하지 아니할 수 있다.

제6장 인증심사의 기준과 방법

제23조(인증심사 기준) ① 인증기준은 별표 7과 같다. 다만, 제18조제1항제2호의 정보보호 관리체계 인증을 받는 경우 별표 7의 인증기준 중에서 "가. 관리체계 수립 및 운영", "나. 보호대책 요구사항"의 기준을 적용한다.

② 심사수행기관은 신청인과 협의를 통해 별표 7의 인증기준 내에서 인증범위, 업무특성 등을 고려하여 인증심사 항목을 조정할 수 있다.

제24조(인증심사팀 구성) ① 심사수행기관은 인증심사 일정이 확정된 때에는 인터넷진흥원에 심사원 모집을 요청하여 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 신청인의 인증범위, 사업유형, 기술의 다양성 등을 고려하여 심사팀원을 구성하고 심사팀장은 심사수행기관 소속의 심사원 이상으로 선정하여야 한다.

③ 인증심사원은 신청인의 정보보호 또는 개인정보보호 컨설팅에 참여하였거나 소속직원 등 신청인과 이해관계를 가지는 경우 사전에 소명하여야 하며, 심사수행기관은 해당 심사원을 인증심사팀의 구성원에서 배제하여야

한다.

제25조(인증심사 방법 및 보완조치) ① 인증심사는 신청인을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 별표 7의 인증기준에 적합한지에 대하여 정보보호 및 개인정보보호 관리체계 구축·운영 관련 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 및 개인정보 처리단계별 요구사항 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 심사수행기관은 인증심사에서 발견된 결함에 대해 심사종료 다음날부터 최대 100일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청인에게 요청할 수 있다.

⑤ 심사수행기관은 인증위원회 심의결과에 따라 인증위원회 종료 다음날부터 30일 이내에 신청인에게 추가 보완조치를 요구할 수 있다.

⑥ 심사수행기관은 보완조치 결과를 확인하기 위하여 필요한 때에는 현장확인을 할 수 있다.

제26조(심사중단) ① 심사수행기관은 다음 각 호의 사유가 발생한 경우에는 인증심사를 중단할 수 있다.

1. 신청인이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청인의 귀책사유로 인하여 인증심사팀장이 인증심사를 계속 진행하기가 곤란하다고 판단하는 경우

2. 신청인이 제출한 관련 자료 등을 검토한 결과 인증심사를 받을 준비가 되었다고 볼 수 없는 경우

3. 인증심사 후 제25조제4항에 따른 보완조치를 최대 100일(재조치 요구 60일 포함) 이내에 완료하지 않은 경우

4. 천재지변 및 경영환경 변화 등으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우

② 심사수행기관은 제1항에 따라 인증심사를 중단하는 때에는 그 사유를 신청인에 서면으로 통보하여야 한다.

③ 심사수행기관은 제1항의 인증심사 중단 사유가 해소되거나 제36조에 따른 이의신청 처리결과에 따라 인증심사를 재개하거나 종결할 수 있다.

제27조(사후관리) ① 인증을 취득한 자는 인증서 유효기간 중 연 1회 이상 심사수행기관에 사후심사를 신청하여야 한다.

② 사후심사는 제5장 및 제6장을 준용하여 진행한다.

③ 인증 취득한 범위와 관련하여 침해사고 또는 개인정보 유출사고가 발생한 경우 인터넷진흥원은 필요에 따라 인증관련 항목의 보안향상을 위한 필요한 지원 등을 할 수 있다.

제28조(인증의 갱신) ① 인증을 취득한 자는 인증서 유효기간 만료 3개월 전에 갱신심사를 신청하여야 한다.

② 갱신심사는 제5장 및 제6장을 준용하여 진행한다.

③ 인증을 취득한 자가 제1항에 따른 인증의 갱신을 신청하지 않고 인증의 유효기간이 경과한 때에는 인증의 효력은 상실된다.

제7장 인증위원회 구성과 운영

제29조(인증위원회의 구성) ① 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 제35조제1항에 따른 인증의 취소에 관한 사항
3. 제36조에 따른 이의신청에 관한 사항
4. 그 밖에 정보보호 및 개인정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 35인 이내의 위원으로 구성하되, 위원은 정보보호 및 개인정보보호 관련 분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

④ 인터넷진흥원 또는 인증기관의 장은 위원이 법령 또는 이 규정을 위반한 때에는 해당 위원을 해촉할 수 있다.

제30조(인증위원회의 운영) ① 인증위원회의 회의는 인터넷진흥원 또는 인증기관의 요구로 개최하되, 회의마다 위원장과 인증위원의 전문분야를 고려하여 6인 이상의 인증위원으로 구성한다. 단, 위원장이 부득이한 사유로 직무를 수행할 수 없는 경우 위원장이 사전에 지명한 위원이 위원장의 직무를 대행한다.

② 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다. 다만, 긴급한 경우나 부득

이한 사유가 있는 경우에는 그러하지 아니하다.

③ 인증위원회 위원장은 제29조제1항의 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

④ 인증위원회는 심의를 위하여 필요하다고 인정되는 경우에는 인증심사에 참여한 인증심사원 또는 관련 전문가로부터 그에 관한 의견을 들을 수 있다.

⑤ 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의·의결 결과를 제출받은 때에는 신청인에게 결과를 통보하여야 한다.

제31조(제척·기피·회피) ① 인증위원회 위원은 신청인과 다음 각 호의 사항 중 어느 하나에 해당하는 때에는 심의·의결에 관여할 수 없다.

1. 위원 본인과 직접적인 이해관계가 있는 사항
2. 위원 본인과 친족관계에 있거나 있었던 자와 관련된 사항
3. 위원이 되기 전에 감사·수사 또는 조사에 관여한 사항

② 위원에게 심의·의결의 공정을 기대하기 어려운 사정이 있는 경우 신청인은 기피신청을 할 수 있고, 위원회는 의결로 이를 결정한다.

③ 위원은 제척사유 또는 기피사유에 해당하는 경우에는 자기 스스로 심의·의결을 회피할 수 있다.

제8장 인증서의 발급·관리 및 홍보

제32조(인증서의 발급 등) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회에서 인증적합으로 판정된 경우 그 결과에 따라 신청인에게 별지 제11호서식의 정보보호 및 개인정보보호 관리체계 인증서 또는 별지 제12호서식의

정보보호 관리체계 인증서를 발급하여야 한다.

② 인증서 발급 시 인증번호는 별표 8의 인증의 표시를 따른다.

③ 제1항에 따른 인증서의 유효기간은 3년으로 한다.

제33조(인증서 관리 및 재발급) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제13호서식의 인증서 재발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제14호 서식의 인증서 변경 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제34조(인증의 표시 및 홍보) ① 「개인정보 보호법 시행령」 제34조의7 및 정보통신망법 시행령 제52조에 따른 인증의 표시는 별표 8과 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 인증범위 및 유효기간을 함께 표시하여야 한다.

③ 인터넷진흥원은 인증정보를 제공하는 홈페이지를 통해 인증현황을 공개하여야 한다.

제35조(인증의 취소) ① 인터넷진흥원 또는 인증기관은 다음 각 호의 사유를 발견한 때는 인증위원회 심의·의결을 거쳐 인증을 취소할 수 있다.

1. 거짓 혹은 부정한 방법으로 인증을 취득한 경우

2. 제23조에 따른 인증기준에 미달하게 된 경우

3. 인증을 취득한 자가 제27조제1항에 따른 사후심사 또는 제28조제1항에

따른 갱신심사를 받지 않았거나 제25조제4항에 따른 보완조치를 하지 않은 경우

4. 인증 받은 내용을 홍보하면서 제34조제2항에 따른 인증범위 및 유효기간을 허위로 표기하거나 누락한 경우
5. 인증을 취득한 자가 제27조 및 제28조에 따른 사후관리를 거부 또는 방해하는 경우
6. 개인정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

② 인터넷진흥원 또는 인증기관은 제1항에 따라 인증을 취소한 경우에 그 결과를 통지하고, 제32조에 따라 발급한 인증서를 회수한다.

제36조(이의신청) ① 신청인 또는 인증을 취득한 자가 인증심사 결과 또는 인증 취소처분에 관하여 이의가 있는 때에는 그 결과를 통보받은 날부터 15일 이내에 별지 제15호서식의 이의신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

② 인터넷진흥원 또는 인증기관은 제1항에 따른 이의신청이 이유가 있다고 인정되는 경우에는 인증위원회에 재심의를 요청할 수 있다.

③ 인터넷진흥원 또는 인증기관은 이의신청에 대한 처리결과를 신청인 또는 인증을 취득한 자에 통지하여야 한다.

제9장 인증업무 일반 등

제37조(비밀유지 등) ① 인터넷진흥원, 인증기관, 심사기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 정당한

권한 없이 또는 허용된 권한을 초과하여 업무상 지득한 비밀에 관한 정보를 누설하거나 이를 업무 목적 이외에 사용하여서는 아니 된다.

② 인터넷진흥원, 인증기관, 심사기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 인증에 관련하여 일체의 금전, 금품, 이익 등을 부당하게 수수하여서는 아니 된다.

제38조(업무 지침 등) 인터넷진흥원, 인증기관 또는 심사기관은 인증 또는 심사업무 수행을 위해 필요한 경우 법령의 범위 내에서 인증 또는 심사업무에 관한 지침을 마련하여 시행할 수 있다.

제39조(재검토 기한) 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는「행정규제기본법」 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2019년 1월 1일을 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙

제1조(시행일) 이 고시는 발령한 날부터 시행한다.

제2조(의무대상자에 관한 적용례) 제19조제4항의 개정규정은 이 고시 시행 후 의무대상자가 된 자부터 적용한다. 다만, 이 고시 시행 이전에 의무대상자가 된 자로서 최초의 인증신청을 이 고시 제23조의 인증기준으로 하는 경우에는 개정 규정을 적용한다.

제3조(인증심사원에 관한 경과조치) ① 이 고시 시행 이전에 「정보보호 관리

체계 인증 등에 관한 고시」 제11조 및 「개인정보보호 관리체계 인증 등에 관한 고시」 제9조에 따라 인터넷진흥원으로부터 인증심사원 자격을 받은 자는 고시 시행 후 6개월 또는 심사원 자격 유효기간 중 더 긴 기간까지 이 고시 시행이전 인증기준의 심사에 참여할 수 있다.

② 제1항의 인증심사원이 이 고시에 의한 인증기준의 심사에 참여하기 위해서는 고시 시행 후 6개월 또는 심사원 자격 유효기간 중 더 긴 기간 이내에 인터넷진흥원이 실시하는 심사원 자격전환 과정을 신청하고 자격전환 과정을 수료하여야 하며, 이 경우 이 고시에 의한 인증심사원으로 본다. 이때 자격전환 과정을 수료한 심사원은 이 고시 시행 이전 인증기준의 심사에 참여할 수 있다.

③ 인증심사원 자격전환 시 인증심사원 등급은 기존 인증심사 경력을 합산하여 적용하며 별표3의 자격요건을 따른다.

제4조(신청인에 관한 경과조치) 신청인은 희망하는 경우 고시 시행 후 6개월까지 이 고시에 의한 인증기준 대신 「정보보호 관리체계 인증 등에 관한 고시」 또는 「개인정보보호 관리체계 인증 등에 관한 고시」의 인증기준으로 인증심사를 받을 수 있으며, 고시 시행 이전의 인증기준으로 인증심사를 받은 자는 인증서의 유효기간까지 기존 인증기준으로 사후심사를 받을 수 있다.

제5조(인증기관 및 심사기관에 관한 경과조치) ① 이 고시 시행 이전에 과학기술정보통신부장관으로부터 지정받은 인증기관 및 심사기관은 지정서의 유효기간까지 부칙 제4조의 신청인에 대하여 이 고시 시행 이전의 인증기준으로 인증 또는 심사를 수행할 수 있다.

② 이 고시 시행 이전에 과학기술정보통신부장관으로부터 지정받은 인증기관 및 심사기관이 이 고시에 의한 인증기관 또는 심사기관으로 지정받은 경우 새로운 지정서의 유효기간까지 부칙 제4조의 신청인에 대하여 이 고시 시행 이전의 인증기준으로 인증 또는 심사를 수행할 수 있다.

[별표 1]

업무수행 요건 · 능력 심사 제출서류(제6조 관련)

구 분	제출서류
인증심사원 고용	1. 인증심사업무를 전담하는 심사원의 보유현황 2. 선임심사원 보유에 대한 증빙 서류
인증 · 심사의 공정성 · 독립성 확보	1. 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않음을 확인할 수 있는 기업설명자료, 직제규정, 사업수행 계획서 등 2. 인증신청인으로부터 독립성 확보 방안
재정 능력	1. 자본금 내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 2, 신용평가서 3. 운영자금 보유 내역 및 피해보상 대책
시설	사무공간·인증심사 서류 보관 장소 및 보안설비·시설 증빙서류
인증 및 심사실적 (재지정만 해당)	인증 및 심사실적에 대한 증빙서류
업무수행 요건 · 능력 심사를 위하여 필요한 서류	[별표2] 업무수행 요건 · 능력 심사를 위한 세부기준 충족을 증빙할 수 있는 서류 1. 조직 및 전문성 관련 증빙서류 2. 신뢰도 관련 증빙서류 3. 업무수행 관련 증빙서류 4. 시설 및 보안 관련 증빙서류

[별표 2]

업무수행 요건·능력 심사에 관한 세부기준

(제7조, 제9조 관련)

가. 업무수행 요건 심사 기준(필수)

평가 항목	세부평가 항목	세부 평가 기준 (인증기관 및 심사기관 모두 해당)
인력	인증심사원 고용	· 인증심사원 5명 이상 상시 고용 · 선임심사원 1명 이상 확보
공정성	객관성 · 공정성 · 독립성 확보	· 인증업무 또는 심사 업무의 독립성, 객관성, 공정성, 신뢰성을 확보할 수 있어야 하며 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 업무수행 능력 심사 기준

평가 항목	세부평가 항목	평가 지표	인증 기관 배점	심사 기관 배점	세부 평가 기준
1. 조직 및 전문성	전담조직	등급	5	5	o 인증/심사 업무를 수행하는 전담조직 유무 · 전담조직 보유 : 배점의 100% · 전담조직 없음 : 0점
	전담인력	비율	5	5	o 심사 업무를 수행하는 전담 심사원의 수 · 10명 이상 : 배점의 100% · 10명 미만 : 배점의 χ% ※ χ = (전담 심사원 수/10명) × 100
	전문성	비율	5	5	o 최근 3년간 전담 심사원의 인증심사 참여일 수의 합 · 200일 이상 : 배점의 100% · 200일 미만 : 배점의 χ% ※ χ = (총 참여일수/200일) × 100
		비율	5	5	o 업무 전문성 강화를 위한 최근 3년간 교육 시간 · 전담 심사원 모두 100시간 이상의 교육을 받은 경우 : 배점의 100% · 전담 심사원 모두 100시간 이상의 교육을 받지 않은 경우 : 배점의 χ% ※ χ = (100시간 이상 교육을 받은 전담 심사원의 수/총 전담 심사원의 수) × 100
2. 신뢰도	재정 능력	등급	5	5	o 신용평가등급 · AAA ~ A- : 배점의 100% · BBB+ ~ BBB- : 배점의 70%

					· BB+ ~ BB- : 배점의 50% · B+ ~ B- : 배점의 30% · CCC+ 이하 : 배점의 10%
		등급	3	3	o 자본금 보유 · 5억 이상 : 배점의 100% · 5억 미만 : 배점의 0%
	업무 지원 및 피해 보상 대책	비계량	2	2	o 운영자금 법인통장 보유 및 유지 수준 o 지정취소, 부도·해산, 업무상 과실 등에 따른 피해보상 관련 보험 가입 또는 이에 상응하는 대책 마련
3. 업무수행	업무지침	비계량	4	4	o 인증/심사 업무 수행 지침 보유 o 업무지침의 타당성 및 준수여부 - 인증/심사 업무를 수행하는 직원의 의무와 책임 - 품질관리, 운영관리, 인증/심사업무, 문서관리, 시설관리, 보안관리 절차 및 방법
	품질관리	비계량	16	18	o 인증/심사의 품질 보증 및 관리를 위한 정보공유, 교육, 세미나 등의 활동 o 피심사기관으로부터 공정성, 객관성, 신뢰성, 독립성 확보방안 및 이행 o 인증/심사업무 참여자 및 업무 담당자의 공정성, 객관성, 신뢰성, 독립성 확보방안 및 이행 o 관계 법령 및 내부절차 준수, 청렴 등에 대한 독립적인 내부감사 실시 및 결과에 대한 조치 o 인증/심사 결과에 대한 처리절차 준수 등에 대한 책임자 검토 o 인증/심사 업무 관련 불만 및 이의제기에 대한 대응 절차마련 및 이행
	운영관리	비계량	8	12	o 업무 수행 방법 및 절차 등의 투명성 및 타당성 o 신청 접수, 수수료 산정방법 및 부과 o 심사 이후 자문료, 출장비 등의 지급의 적절한 이행 o 인증취득 희망기업에 특정 기관으로 부적절한 방법으로 심사를 종용하는 등 부당행위 방지대책
	인증관리	비계량	12	-	o 인증의 독립성 · 객관성 · 공정성 확보를 위한 인증위원 구성 및 인증위원회 운영 o 인증위원회 개최 정족수, 상정안건의 검토, 의결 등의 운영절차 마련 및 이행 o 인증서 관리 절차 마련 및 이행 o (재지정만 해당)인증실적 및 인증 내역
	심사관리	비계량	12	18	o 심사팀 구성 원칙마련 및 이행 o 심사원의 의무와 책임 준수, 보안관리 및 감독 방안 및 이행 o 심사 수행절차 준수 o 심사결과보고, 인증위원회 상정 등 사후 절차 준수 o 인증심사 수행 시 문서 및 정보의 유출 방지를 위한 시스템 도입 및 이행 o (재지정만 해당)심사 실적 및 인증심사원 참여 내역
	문서관리	비계량	10	10	o 업무의 기록 및 문서에 관한 관리절차 마련 및 준수 o 업무 담당자간 파일 송수신 및 문서 공유시 안전한 방식을 사용

					o 업무 기록 및 문서에 권한이 없거나 불필요한 인원의 접근 방지 대책 및 이행
4. 시설 및 보안	시설 및 보안	비계량	4	4	o 독립된 사무공간 및 회의공간 o 인증 및 심사 기록물의 안전한 보관을 위한 장소 o 사무공간 출입의 신원확인 및 출입통제 보안설비 운영 o 문서 분실, 도난 등 예방을 위한 보안시설 마련
	시스템 및 보안	비계량	4	4	o 인증 및 심사 관리를 위한 시스템 운영 및 사무관련 시스템 보유 o 인증 및 심사정보의 침해사고, 유출사고를 대비한 보안 시스템 운영
5. 감점	자격 취소 사실	계량	감점	감점	o 지정공고일 기준으로 10년 이내에 과학기술정보통신부, 방송통신위원회 또는 행정안전부가 부여한 정보보호 또는 개인정보보호 관련 업무 수행자격이 취소된 사실이 있는 경우 ※취소 1회 당 : 감점 10점
합계			100	100	

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 비계량 각 세부평가 점수 부여기준은 배점에 평가등급(계수)를 곱하여 계산한다.

평가요소별 비계량 평가	평가등급(계수)
우수	1.0
보통	0.6
미흡	0.2
미 제출	점수없음(0)

[별표 3]

인증심사원 등급별 자격 요건(제12조 관련)

등급	자격 기준
심사원보	o 인증심사원 자격 신청 요건을 만족하는 자로서 인터넷진흥원이 수행하는 인증심사원 양성과정 통과하여 자격을 취득한 자
심사원	o 심사원보 자격 취득자로서 인증심사에 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자

※ 인터넷진흥원은 인증심사원의 인증심사 능력에 따라 매년 책임심사원을 지정할 수 있다.

[별표 4]

인증심사원 자격 신청 요건(제13조 관련)

4년제 대학졸업 이상 또는 이와 동등학력을 취득한 자로서 정보보호 및 개인정보보호 경력을 각 1년 이상 필수로 보유하고 정보보호, 개인정보보호 또는 정보기술 경력을 합하여 6년 이상을 보유

가. "동등학력" 이란 고등학교 졸업자는 4년 이상, 2년제 대학 졸업자는 2년 이상 업무경력을 말한다.

나. "정보기술 경력" 이란 공공기관, 기업체, 교육 및 연구기관 등에서 정보통신서비스, 정보통신기기, 소프트웨어 및 컴퓨터 관련 서비스 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 경력 또는 관련 법률자문 경력을 말한다.

다. "정보보호 경력" 이란 공공기관, 기업체, 교육 및 연구기관 등에서 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호, 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 경력 또는 관련 법률자문 경력을 말한다.

라. "개인정보보호 경력" 이란 공공기관, 기업체, 교육 및 연구기관 등에서 개인정보보호 업무 수행, 개인정보보호 컨설팅, 개인정보보호 관련 법률자문 등의 업무를 수행한 경력을 말한다.

마. 변호사법에 따른 변호사의 경우에는 6년의 개인정보보호 유관경력을 보유한 것으로 본다.

바. 동일기간에 두 가지 이상 업무가 중복되는 경우에 하나의 경력만 인정하며, 모든 해당 경력은 신청일 기준 최근 10년 이내의 경력에 한해 인정한다.

사. 아래의 학위 또는 자격을 취득한 경우 정보보호 또는 개인정보보호 경력을 대체할 수 있으며 중복으로 인정하지 않는다.

<경력인정 요건-중복 인정 불가>

구 분	경력 인정 요건	인정기간
정보보호 경력	o "정보보호" 관련 박사 학위 취득자	2년
	o "정보보호" 관련 석사 학위 취득자 o 정보보안기사 o 정보시스템감사통제협회(ISACA)의 정보시스템감사사(CISA) o 국제정보시스템보안자격협회(ISC²)의 정보시스템보호전문가(CISSP)	1년
개인정보보호 경력	o "개인정보보호" 관련 박사 학위 취득자	2년
	o "개인정보보호" 관련 석사 학위 취득자 o 개인정보 영향평가에 관한 고시 제6조에 따른 개인정보 영향평가 전문인력 o 개인정보관리사(CPPG)	1년
정보기술 경력	o "정보기술" 관련 박사 학위 취득자 o 정보관리기술사, 컴퓨터시스템응용기술사 o 정보시스템감리사	2년
	o "정보기술" 관련 석사 학위 취득자 o 정보시스템감리원 o 정보처리기사, 전자계산기조직응용기사	1년

[별표 5]

인증심사 일부 생략의 범위(제20조 관련)

분야		항목	
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리
		2.1.2	조직의 유지관리
		2.1.3	정보자산 관리
2.2.	인적 보안	2.2.1	주요 직무자 지정 및 관리
		2.2.2	직무 분리
		2.2.3	보안 서약
		2.2.4	인식제고 및 교육훈련
		2.2.5	퇴직 및 직무변경 관리
		2.2.6	보안 위반 시 조치
2.3.	외부자 보안	2.3.1	외부자 현황 관리
		2.3.2	외부자 계약 시 보안
		2.3.3	외부자 보안 이행 관리
		2.3.4	외부자 계약 변경 및 만료 시 보안
2.4.	물리 보안	2.4.1	보호구역 지정
		2.4.2	출입통제
		2.4.3	정보시스템 보호
		2.4.4	보호설비 운영
		2.4.5	보호구역 내 작업
		2.4.6	반출입 기기 통제
		2.4.7	업무 환경 보안
2.12.	재해복구	2.12.1	재해, 재난 대비 안전조치
		2.12.2	재해 복구 시험 및 개선

[별표 6]

인증 수수료 산정 및 심사원 보수 기준(제21조 관련)

1. 인증수수료 산정 기준

인증 수수료 = 직접인건비 + 제경비 + 기술료 + 직접경비

가. 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다.

나. 제경비는 최대 (직접인건비×120%) 로 산정한다.

다. 기술료는 최대 {(직접인건비+제경비)×40%} 로 산정한다.

라. 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다. 단, 신청인은 심사 현장 상황에 따라 직접경비를 인증 수수료와 별도로 지급할 수 있다.

2. 인증심사원 보수 및 출장비 지급기준

가. 인증심사원에 대한 보수는 소프트웨어산업진흥법 제22조제4항에 따른 소프트웨어기술자의 노임단가의 등급별 평균임금에서 심사원보는 초급기술자, 심사원은 고급기술자, 선임심사원은 특급기술자, 책임심사원은 기술사의 일평균임금을 참고하여 정할 수 있다.

나. 인증심사원이 국내·외에서 출장업무를 수행하는 경우 심사 수행기관의 업무 지침에 따른 정액여비로 별도 지급할 수 있다.

[별표 7]

인증기준(제23조 관련)

가. 관리체계 수립 및 운영

분야		항목		상세 내용
1.1.	관리체계 기반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
		1.1.2	최고책임자의 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
		1.1.3	조직 구성	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.
		1.1.4	범위 설정	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
		1.1.5	정책 수립	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.1.6	자원 할당	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
		1.2.2	현황 및 흐름분석	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
		1.2.3	위험 평가	조직의 대내외 환경분석을 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.
		1.2.4	보호대책 선정	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
1.3.	관리체계 운영	1.3.1	보호대책 구현	선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
		1.3.2	보호대책 공유	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.

		1.3.3	운영현황 관리	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
1.4.	관리체계 점검 및 개선	1.4.1	법적 요구사항 준수 검토	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
		1.4.2	관리체계 점검	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
		1.4.3	관리체계 개선	법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립 · 이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.

나. 보호대책 요구사항

분야		항목		상세 내용
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.
		2.1.2	조직의 유지관리	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.
		2.1.3	정보자산 관리	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
2.2.	인적 보안	2.2.1	주요 직무자 지정 및 관리	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.
		2.2.2	직무 분리	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.2.3	보안 서약	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
		2.2.4	인식제고 및 교육훈련	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
		2.2.5	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
		2.2.6	보안 위반 시 조치	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.
2.3.	외부자 보안	2.3.1	외부자 현황 관리	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
		2.3.2	외부자 계약 시 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.
		2.3.3	외부자 보안 이행 관리	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.
		2.3.4	외부자 계약 변경 및 만료 시 보안	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.

2.4.	물리 보안	2.4.1	보호구역 지정	물리적 · 환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역 · 제한구역 · 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립 · 이행하여야 한다.
		2.4.2	출입통제	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
		2.4.3	정보시스템 보호	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
		2.4.4	보호설비 운영	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온도 · 습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립 · 운영하여야 한다.
		2.4.5	보호구역 내 작업	보호구역 내에서의 비인가행위 및 권한 오 · 남용 등을 방지하기 위한 작업 절차를 수립 · 이행하고, 작업 기록을 주기적으로 검토하여야 한다.
		2.4.6	반출입 기기 통제	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립 · 이행하고 주기적으로 검토하여야 한다.
		2.4.7	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립 · 이행하여야 한다.
2.5.	인증 및 권한관리	2.5.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록 · 해지 및 접근권한 부여 · 변경 · 말소 절차를 수립 · 이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
		2.5.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립 · 이행하여야 한다.
		2.5.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립 · 이행하여야 한다.
		2.5.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립 · 이행하여야 한다.
		2.5.5	특수 계정 및 권한 관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.
		2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록 · 이용 · 삭제 및 접근권한의 부여 · 변경 · 삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
2.6.	접근통제	2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립 · 이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.

		2.6.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
		2.6.3	응용프로그램 접근	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
		2.6.4	데이터베이스 접근	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
		2.6.5	무선 네트워크 접근	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.
		2.6.6	원격접근 통제	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
		2.6.7	인터넷 접속 통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
2.7.	암호화 적용	2.7.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
		2.7.2	암호키 관리	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.
2.8.	정보시스템 도입 및 개발 보안	2.8.1	보안 요구사항 정의	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.
		2.8.2	보안 요구사항 검토 및 시험	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.
		2.8.3	시험과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
		2.8.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
		2.8.5	소스 프로그램 관리	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.
		2.8.6	운영환경 이관	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.

2.9.	시스템 및 서비스 운영관리	2.9.1	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립 · 이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
		2.9.2	성능 및 장애관리	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지 · 기록 · 분석 · 복구 · 보고 등의 절차를 수립 · 관리하여야 한다.
		2.9.3	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립 · 이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
		2.9.4	로그 및 접속기록 관리	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위 · 변조, 도난, 분실 되지 않도록 안전하게 보존 · 관리하여야 한다.
		2.9.5	로그 및 접속기록 점검	정보시스템의 정상적인 사용을 보장하고 사용자 오 · 남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.
		2.9.6	시간 동기화	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.
		2.9.7	정보자산의 재사용 및 폐기	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구 · 재생되지 않도록 안전한 재사용 및 폐기 절차를 수립 · 이행하여야 한다.
2.10.	시스템 및 서비스 보안관리	2.10.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립 · 이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
		2.10.2	클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유 · 노출되지 않도록 관리자 접근 및 보안설정 등에 대한 보호대책을 수립 · 이행하여야 한다.
		2.10.3	공개서버 보안	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집 · 저장 · 공개 절차 등 강화된 보호대책을 수립 · 이행하여야 한다.
		2.10.4	전자거래 및 핀테크 보안	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작 · 사기 등의 침해사고 예방을 위해 인증 · 암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
		2.10.5	정보전송 보안	타 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통해 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.
		2.10.6	업무용 단말기기 보안	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
		2.10.7	보조저장매체 관리	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립 · 이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.

		2.10.8	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.10.9	악성코드 통제	바이러스 · 웜 · 트로이목마 · 랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방 · 탐지 · 대응 등의 보호대책을 수립 · 이행하여야 한다.
2.11.	사고 예방 및 대응	2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내 · 외부 침해시도의 탐지 · 대응 · 분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
		2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
		2.11.3	이상행위 분석 및 모니터링	내 · 외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지 · 대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.
		2.11.4	사고 대응 훈련 및 개선	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.
		2.11.5	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.
2.12.	재해복구	2.12.1	재해 · 재난 대비 안전조치	자연재해, 통신 · 전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.
		2.12.2	재해 복구 시험 및 개선	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

다. 개인정보 처리 단계별 요구사항

분야		항목		상세 내용
3.1.	개인정보 수집 시 보호조치	3.1.1	개인정보 수집 제한	개인정보는 서비스 제공을 위하여 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.
		3.1.2	개인정보의 수집 동의	개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.
		3.1.3	주민등록번호 처리 제한	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
		3.1.4	민감정보 및 고유식별정보의 처리 제한	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체(이용자)의 별도 동의를 받아야 한다.
		3.1.5	간접수집 보호조치	정보주체(이용자) 이외로부터 개인정보를 수집하거나 제공받는 경우에는 업무에 필요한 최소한의 개인정보만 수집·이용하여야 하고 법령에 근거하거나 정보주체(이용자)의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
		3.1.6	영상정보처리기기 설치·운영	영상정보처리기기를 공개된 장소에 설치·운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
		3.1.7	홍보 및 마케팅 목적 활용 시 조치	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우에는 그 목적을 정보주체(이용자)가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.
3.2.	개인정보 보유 및 이용 시 보호조치	3.2.1	개인정보 현황관리	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
		3.2.2	개인정보 품질보장	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체(이용자)에게 관리절차를 제공하여야 한다.
		3.2.3	개인정보 표시제한 및 이용 시 보호조치	개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무상 반드시 필요하지 않은 개인정보는 삭제하거나 또는 식별할 수 없도록 조치하여야 한다.
		3.2.4	이용자 단말기 접근 보호	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.

		3.2.5	개인정보 목적 외 이용 및 제공	개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
3.3.	개인정보 제공 시 보호조치	3.3.1	개인정보 제3자 제공	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
		3.3.2	업무 위탁에 따른 정보주체 고지	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 정보주체(이용자)에게 알려야 하며, 필요한 경우 동의를 받아야 한다.
		3.3.3	영업의 양수 등에 따른 개인정보의 이전	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체(이용자) 통지 등 적절한 보호조치를 수립·이행하여야 한다.
		3.3.4	개인정보의 국외이전	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
3.4.	개인정보 파기 시 보호조치	3.4.1	개인정보의 파기	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
		3.4.2	처리목적 달성 후 보유 시 조치	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.
		3.4.3	휴면 이용자 관리	서비스를 일정기간 동안 이용하지 않는 휴면 이용자의 개인정보를 보호하기 위하여 관련 사항의 통지, 개인정보의 파기 또는 분리보관 등 적절한 보호조치를 이행하여야 한다.
3.5.	정보주체 권리보호	3.5.1	개인정보처리방침 공개	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보처리방침을 수립하고, 이를 정보주체(이용자)가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
		3.5.2	정보주체 권리보장	정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.
		3.5.3	이용내역 통지	개인정보의 이용내역 등 정보주체(이용자)에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.

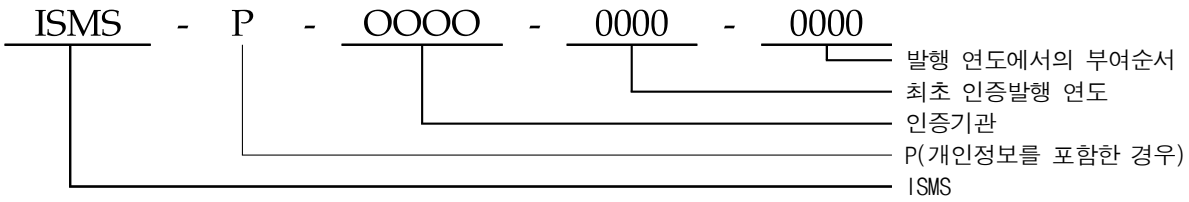
[별표 8]

인증의 표시(제32조, 제34조 관련)

1. 인증번호 부여

가. 인증번호는 유일성, 간결성, 관리의 용이성 등을 고려하여 최초심사, 갱신심사의 구분 없이 최초 발급순서별로 부여한다.

나. 인증번호는 아래와 같은 형식으로 부여한다.



2. 도안모형

정보보호 및 개인정보보호 관리체계 인증	정보보호 관리체계 인증
정보보호 및 개인정보보호 관리체계 인증 ISMS-P Personal information & Information Security Management System	정보보호 관리체계 인증 ISMS Information Security Management System

3. 인증 표시에 대한 유의사항

가. 인증 취득 사실의 홍보는 인증서를 발급받은 날부터 효력이 유지되는 동안에만 사용이 가능하다. 인증이 취소된 경우에는 인증에 대한 홍보, 인증서 사용을 중지하여야 한다.

나. 인증 표시를 사용하는 경우 유효기간, 인증범위를 함께 표시하여야 한다.

다. 인증을 취득한 자는 인증의 사실을 과장되거나 불명확한 표현을 사용하여 광고할 수 없다.

4. 인증 표시의 사용 방법

가. 인증 표시는 지정된 색상으로 사용할 수 있다. 또한 색상이 명확하게 나타날 수 있는 바탕색 위에 흑백으로 사용하거나 표시된 인쇄물의 주된 단일색상으로 사용 할 수 있다.

나. 인증 표시의 크기는 표시물 대상의 크기나 표시장소의 여건에 따라 조정할 수 있으며, 같은 비율로 축소 또는 확대하여 표시할 수 있다.

다. 일반문서, 편지의 상단, 송장, 홍보 책자 등에 인증 취득 사실의 내용을 홍보할 수 있다.

5. 인증명판 제작 시 유의사항

가. 소재는 가급적 동판으로 제작한다.

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다.

다. 도안 모형은 인증의 표지를 중앙에 둔다.

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다.

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호서식]

인증기관·심사기관 지정 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, [ ]에는 해당되는 곳에 √표를 합니다.

접수번호		접수일시	처리기간
신청인	업체명		사업자등록번호
	대표자		전화번호
	주소		
	전자우편 주소(e-mail)		
	총 직원 수	인증심사를 수행하는 직원 수	
신청구분	[ ] 신규	[ ] 재지정	
기관구분	[ ] 인증기관	[ ] 심사기관	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항, 제7항, 제47조의3제3항 및 같은 법 시행령 제53조의2, 「개인정보 보호법」 제32조2제5항 및 같은 법 시행령 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제6조에 따라 정보보호 및 개인정보보호 관리체계 인증기관 또는 심사기관 지정을 위와 같이 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

과학기술정보통신부장관 귀하 **행정안전부장관** 귀하 **방송통신위원회** 귀하

첨부서류 (각 3부)	1. 정관 또는 규약 2. 별지 제2호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관		처 리 기 관		처 리 기 관		처 리 기 관

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호서식]

인증심사 업무를 수행하는 직원 보유현황

신청인	업체명	
	대표자	
	전체 직원 수	인증심사 업무를 전담하는 직원의 수

번호	성명	생년월일	입사일	소속부서 및 업무		고용형태
		인증심사원 자격번호	최초자격취득일	심사원 등급 ※ 신청서 제출 시점	인증심사 참여 일수 ※ 최근 3년 이내	비고
		. . .	. . .			
			. . .		일	
		. . .	. . .			
			. . .		일	
		. . .	. . .			
			. . .		일	
		. . .	. . .			
			. . .		일	
		. . .	. . .			
			. . .		일	
		. . .	. . .			
			. . .		일	

유의사항

1. 「심사원등급」란에는 심사원보, 심사원, 선임심사원 여부를 기재한다.
2. 인증심사원 자격 보유 및 인증심사 경력을 증빙할 수 있는 서류를 함께 제출하여야 한다.
3. 비고에 학위, 자격 등에 대한 사항을 추가로 기재한 경우 학위 및 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.

210㎜×297㎜[(백상지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제3호서식]

(제1쪽)

정보보호 및 개인정보보호 관리체계 인증기관 지정서

등록번호 :　　유효기간 :

업 체 명 :　　대 표 자 :

업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항, 제47조의3제3항 및 같은 법 시행령 제53조의2, 「개인정보 보호법」 제32조2제5항 및 같은 법 시행령 제34조의6에 따라 위와 같이 정보보호 및 개인정보보호 관리체계 인증기관(위 인증업무에 한함)으로 지정합니다.

년　　월　　일

과학기술정보통신부장관 직인　　행정안전부장관 직인　　방송통신위원회 직인

210㎜×297㎜[백상지 (150g/㎡)]

CERTIFICATE OF DESIGNATION AS Certification Body of Personal information & Information Security Management System

Registry Number :
Name of Organization :
Scope of Certification work :

Period of Validity :
Name of Representative :

This is to certify that the abovementioned organization is designated Certification Body of Personal information & Information Security Management System in accordance with Article 47, Paragraph 6 and Article 47-3, Paragraph 3 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act and in accordance with Article 32-2, Paragraph 5 of 「Personal Information Protection Act」 and Article 34-6 of the Enforcement Decree of the same Act.

Date of Issuance:

서 명 또는 직 인	서 명 또는 직 인	서 명 또는 직 인
Minister, Ministry of Science and ICT	Minister of the Interior and Safety	Korea Communications Commission

210㎜×297㎜[백상지 (150g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호서식]

(제1쪽)

정보보호 및 개인정보보호 관리체계 심사기관 지정서

등록번호 :　　유효기간 :

업 체 명 :　　대 표 자 :

업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제7항, 제47조의3제3항 및 같은 법 시행령 제53조의2, 「개인정보 보호법」 제32조2제5항 및 같은 법 시행령 제34조의6에 따라 위와 같이 정보보호 및 개인정보보호 관리체계 심사기관(위 심사업무에 한함)으로 지정합니다.

년　　월　　일

과학기술정보통신부장관 직인　　행정안전부장관 직인　　방송통신위원회 직인

210㎜×297㎜[백상지 (150g/㎡)]

CERTIFICATE OF DESIGNATION AS Examination Institution for Personal information & Information Security Management System

Registry Number :

Period of Validity :

Name of Organization :

Name of Representative :

Address :

Scope of Examination work :

This is to certify that the abovementioned organization is designated Examination Institution of Personal information & Information Security Management System in accordance with Article 47, Paragraph 7 and Article 47-3, Paragraph 3 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act and in accordance with Article 32-2, Paragraph 5 of 「Personal Information Protection Act」 and Article 34-6 of the Enforcement Decree of the same Act.

Date of Issuance:

서 명 또는 직 인	서 명 또는 직 인	서 명 또는 직 인
Minister, Ministry of Science and ICT	Minister of the Interior and Safety	Korea Communications Commission

210㎜×297㎜[백상지 (150g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호서식]

인증실적 보고서

※ [ ]에는 해당되는 곳에 √표를 합니다.

인증기관	업체명	
	대표자	사업자등록번호
	인증기관 등록번호	인증기관 지정일(유효기간)
	인증업무의 범위	

구분	세부	실적
정보보호 및 개인정보보호 관리체계 인증 실적	신규 인증 건수	건
	인증 취소 건수	건
	인증 유지 건수	건
정보보호 관리체계 인증 실적	신규 인증 건수	건
	인증 취소 건수	건
	인증 유지 건수	건
인증기관 지정요건 내역 변동사항	[ ] 없음	[ ] 있음

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제53조의4, 「개인정보 보호법 시행령」 시행령 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제8조에 따라 정보보호 및 개인정보보호 관리체계 인증실적을 제출합니다.

년 월 일

신청인(대표자) (서명 또는 인)

과학기술정보통신부장관 귀하 **행정안전부장관** 귀하 **방송통신위원회** 귀하

첨부서류	1.인증실적 내역 2.인증기관 지정요건 내역 변동사항(해당되는 경우만 제출)

210㎜×297㎜[(백상지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호서식]

인증심사실적 보고서

※ [ ]에는 해당되는 곳에 √표를 합니다.

심사기관	업체명	
	대표자	사업자등록번호
	심사기관 등록번호	심사기관 지정일(유효기간)
	심사업무의 범위	

구분	세부	실적
정보보호 및 개인정보보호 관리체계 인증심사 실적	최초심사	건
	갱신심사	건
	사후심사	건
정보보호 관리체계 인증심사 실적	최초심사	건
	갱신심사	건
	사후심사	건
심사기관 지정요건 내역 변동사항	[ ] 없음	[ ] 있음

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제53조의4, 「개인정보 보호법 시행령」 시행령 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제8조에 따라 정보보호 및 개인정보보호 관리체계 인증심사실적을 제출합니다.

년 월 일

신청인(대표자) (서명 또는 인)

과학기술정보통신부장관 귀하 **행정안전부장관** 귀하 **방송통신위원회** 귀하

첨부서류	1. 인증심사실적 내역 2. 심사기관 지정요건 내역 변동사항(해당되는 경우만 제출)

210㎜×297㎜[(백상지(80g/㎡))]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호 서식]

인증심사원 자격 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, [ ]에는 해당되는 곳에 √표를 합니다.

<table>
<tr><td>접수번호</td><td colspan="2">접수일시</td><td colspan="2">처리기간</td></tr>
<tr><td rowspan="5">신청자
인적사항</td><td>성 명</td><td></td><td>생년월일</td><td></td><td rowspan="5">신청일부터 6개월 내에
촬영된 컬러사진
(3.5cm × 4.5cm)</td></tr>
<tr><td>소 속</td><td colspan="3"></td></tr>
<tr><td>주 소</td><td colspan="3">(우:)</td></tr>
<tr><td>휴대전화</td><td colspan="3"></td></tr>
<tr><td>이메일</td><td colspan="3"></td></tr>
<tr><td>학력사항</td><td>최종학력</td><td colspan="4">[ ] 고졸 [ ] 전문대졸 [ ] 대졸 [ ] 석사 [ ] 박사</td></tr>
<tr><td rowspan="6">경력사항
(※ 서류로 증명 가능한 내용만 기술)</td><td rowspan="4">경력 내역
(중복불가)</td><td colspan="4">[ ] 정보보호 경력 총 년 개월</td></tr>
<tr><td colspan="4">[ ] 개인정보보호 경력 총 년 개월</td></tr>
<tr><td colspan="4">[ ] 정보기술 경력 총 년 개월</td></tr>
<tr><td colspan="4">총 합 총 년 개월</td></tr>
<tr><td rowspan="2">경력인정
자격</td><td colspan="2">자격증 또는 학위명(전공 또는 논문명)</td><td>취득일자</td><td>수여기관</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>

정보보호 및 개인정보보호 관리체계 인증심사원 자격을 신청하기 위하여 이 신청서를 제출합니다. 본 신청서의 내용이 사실과 다르거나, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 별표4의 인증심사원 자격 신청 요건에 해당하지 아니할 때에는 합격 또는 자격을 취소하여도 이의를 제기하지 않겠습니다.

년 월 일

신청자 (서명 또는 인)

한국인터넷진흥원장 귀하

첨부서류	1. 자격 신청 세부내역서 2. 응시요건에 충족함을 증빙하는 서류 ① 학력증명서 ② 부서이동 및 수행업무 내역이 구체적으로 기재된 상세 경력증명서 또는 재직증명서 ③ 기술실적증명서(해당 시) ④ 자격증명서(해당 시) 3. 정보보호 서약서 4. 개인정보 수집 · 이용 동의서 등

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제8호 서식]

정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서

1. 발급번호 :

2. 성　　명 :

3. 생년월일 :

4. 유효기간 :

5. 등　　급 :

위 사람은 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제14조에 따른 정보보호 및 개인정보보호 관리체계 인증심사원임을 증명합니다.

년　　월　　일

한국인터넷진흥원장　　직인

210㎜×297㎜[백상지 (150g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호서식]

정보보호 및 개인정보보호 관리체계 인증 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, [ ]에는 해당되는 곳에 √표를 합니다.

접수번호	접수일시	처리기간

신청인	업체명		사업자등록번호
	대표자		전화번호
	주소		
	전자우편(e-mail)		
정보보호 및 개인정보보호 관리체계 인증	심사구분	[ ]최초심사 [ ]사후심사(차)	[ ]갱신심사
	인증범위		
	범위 내 개인정보		
정보보호 관리체계 인증	심사구분	[ ]최초심사 [ ]사후심사(차)	[ ]갱신심사
	인증범위		

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 제47조의3 제1항, 같은 법 시행령 제47조, 「개인정보 보호법」 제32조의2에 따라 위와 같이 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

ooooo(심사수행기관명)의 장 귀하

첨부서류	정보보호 및 개인정보보호 관리체계 명세서 1부

처 리 절 차

신청서 작성	→	접수 및 예비점검	→	수수료 납부	→	인증심사	→	인증위원회 심의	→	인증서발급
신청인		심사수행기관		신청인		심사수행기관		인증기관		처 리 기 관

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호서식]

인증심사 일부 생략 신청서

접수번호	접수일시	처리기간

신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
ISO/IEC 27001	인증번호 :	인증기관 :
	인증의 범위 :	
	인증유효기간 : . . ~ . .	
	최근 인증심사 수행기간 : . . ~ . .	
	보완조치 완료일 :	
「정보통신기반 보호법」 제9조에 따른 취약점의 분석·평가	기반시설 지정번호(공문번호) :	
	취약점 분석 · 평가 수행범위 :	
	취약점 분석 · 평가 수행기간 : . . ~ . .	
	수행주체 :	

「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제20조에 따라 위와 같이 정보보호 관리체계 인증 일부 심사 생략을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

ooooo(심사수행기관명)의 장 귀하

첨부서류	1. 정보보호 관리체계 인증 일부 심사 생략 명세서 1부 2. 인증심사 일부기준 생략을 증명할 수 있는 서류

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제11호서식]

(제1쪽)

정보보호 및 개인정보보호 관리체계 인증서

1. 인증번호 :

2. 업체명 :

3. 대표자 :

4. 인증의 범위 :

5. 유효기간 :

6. 심사수행기관 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 제47조의3 제1항, 같은 법 시행령 제47조, 「개인정보 보호법」 제32조의2에 따라 위와 같이 정보보호 및 개인정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원장
또는 인증기관의 장

직인

210㎜×297㎜[백상지 (150g/㎡)]

CERTIFICATE
OF
Personal information & Information Security Management System

1. Certificate Number :

2. Name of Organization :

3. Name of Representative :

4. Scope of Certification :

5. Period of Validity :

6. Examination Institution :

This is to certify that the abovementioned organization is compliant to the assessment standard for Personal information & Information Security Management System certification in accordance with Article 47, Paragraph 1 and Article 47-3, Paragraph 1 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act and in accordance with Article 32-2 of 「Personal Information Protection Act」

Date of Issuance :

서 명 또는 직 인

한국인터넷진흥원장 또는 인증기관의 장 영문

210㎜×297㎜[백상지 (150g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제12호서식]

(제1쪽)

정보보호 관리체계 인증서

1. 인증번호 :

2. 업체명 :

3. 대표자 :

4. 인증의 범위 :

※ 심사 생략 범위 :

5. 유효기간 :

6. 심사수행기관 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원장
또는 인증기관의 장

직인

210㎜×297㎜[백상지 (150g/㎡)]

CERTIFICATE
OF
Information Security Management System

1. Certificate Number :

2. Name of Organization :

3. Name of Representative :

4. Scope of Certification :

※ Scope of omitted certification examination :

5. Period of Validity :

6. Examination Institution :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

서 명 또는 직 인

한국인터넷진흥원장 또는 인증기관의 장 영문

210㎜×297㎜[백상지 (150g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식]

인증서 재발급 신청서

접수번호	접수일시	처리기간

신청인	업체명		사업자등록번호
	대표자		전화번호
	주소		
	전자우편(e-mail)		
인증 정보	인증번호		
	인증범위		
재발급 사유			

위와 같이 인증서의 재발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 인증기관의 장 귀하

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제14호서식]

인증서 변경 신청서

접수번호	접수일시	처리기간

신청인	업체명		사업자등록번호
	대표자		전화번호
	주소		
	전자우편(e-mail)		
인증정보	인증번호		
	인증범위		
변경 내용	변경전	(국문)	
		(영문)	
	변경후	(국문)	
		(영문)	
변경사유			

위와 같이 인증서의 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 인증기관의 장 귀하

첨부서류	인증서 내용의 변경이 필요함을 증명할 수 있는 서류

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]

■「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제15호서식]

이의신청서

접수번호	접수일시	처리기간

신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	

통지사항	통지를 받은 날	
	통지된 사항	
이의신청 대상		
이의신청 사유		

위와 같이 이의신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 인증기관의 장 귀하

첨부서류	이의신청 내용을 확인할 수 있는 증빙 자료

210㎜×297㎜[(백상지(80g/㎡)또는 중질지(80g/㎡)]